MARCELO AUGUSTO LEOCADIO

CÓDIGOS MDS COM A MÉTRICA POSET

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

VIÇOSA
MINAS GERAIS - BRASIL
2012

Ficha catalográfica preparada pela Seção de Catalogação e Classificação da Biblioteca Central da UFV

T
L576c
2012

Leocadio, Marcelo Augusto, 1981-
Códigos MDS com a métrica poset / Marcelo Augusto Leocadio. – Viçosa, MG, 2012.
viii, 73f. : il. ; 29cm.

Orientador: Allan de Oliveira Moura.
Dissertação (mestrado) - Universidade Federal de Viçosa.
Referências bibliográficas: f. 72-73.

1. Geometria. 2. Códigos corretores de erros (Teoria da informação). I. Universidade Federal de Viçosa. Departamento de Matemática. Programa de Pós-Graduação em Matemática. II. Título.

CDD 22. ed. 516

MARCELO AUGUSTO LEOCADIO

CÓDIGOS MDS COM A MÉTRICA POSET

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

APROVADA: 30 de julho de 2012.

Marcelo Firer	Rogério Carvalho Picanço
Marinês Guerreiro Co-orientadora	Simone Maria de Moraes

Allan de Oliveira Moura
Orientador

"Enquanto eu tiver perguntas e não houver respostas... continuarei a escrever."

Clarice Linspector.

Agradecimentos

Primeiramente aos meus pais, Antonio e Vera, por sempre me estimularem a continuar meus estudos, mesmo nos momentos de maiores dificuldades.

A minha irmã Viviane, que apesar de estar tão longe, sempre me apoiou incondicionalmente e me fez acreditar que a gente é capaz de chegar aonde quer.

Ao grande amigo, Lucas, que me acompanhou em quase todos os momentos de Viçosa. Fosse nos dias quentes de estudo, ou nas noites geladas de Leão.

A todos os amigos de DMA nesses anos, Lucas, Isaque, Prego, Guemael, Fredão, Gilbertão. E todos os outros que me ajudaram de alguma forma, Mariana, Julio, Pablo, Paquitão, Inaiá, Tainã, dentre muitos outros.

As professoras Marines e Simone, por estarem sempre ao meu lado me ajudando a crescer, tanto profissionalmente quanto pessoalmente. Me aconselhando quando necessário e acreditando no meu potencial.

Aos companheiros de república, Túlio e Gustavo, por aguentar meu humor durante a fase final desse trabalho e me propiciarem varias gargalhadas.

A FAPEMIG pelo apoio financeiro.

Ao professor Abílio.

E ao meu orientador Allan Oliveira Moura, por direcionar meu estudo e toda paciência comigo durante neste trabalho, que de alguma forma me ajudará a crescer ainda mais.

Resumo

LEOCADIO, Marcelo Augusto, M.Sc., Universidade Federal de Viçosa, Julho, 2012. **Códigos MDS com a métrica poset**. Orientador: Allan Oliveira Moura. Co-Orientadora: Marinês Guerreiro. Co-Orientador: Abílio Lemos Cardoso Junior.

Uma generalização da métrica de Hamming é a métrica poset. Nesse fazemos um estudo detalhado dos espaços poset, hierarquia de $\mathbb{P}$-pesos e a $\mathbb{P}$-distribuição de pesos, dando ênfase aos códigos poset não degenerados. Verificamos a relação de dualidade poset entre as hierarquias de um código e seu dual. Definimos ainda dois novos parâmetros para a classe de códigos dualmente não degenerados no ambiente poset. Como consequência enunciamos o Teorema da Minimalidade, o Teorema da Variância e mostramos a Identidade de Minimalidades no espaço poset.

Abstract

LEOCADIO, Marcelo Augusto, M.Sc., Universidade Federal de Viçosa, Julho, 2012. **MDS codes with the poset metric**. Adviser: Allan Oliveira Moura. Co-adviser: Marinês Guerreiro. Co-adviser: Abílio Lemos Cardoso Junior.

A poset metric is the generalization of the Hamming metric. In this work we make a detailed study of poset spaces, hierarchy of $I\!P$-weights and $I\!P$-distribution of weights, emphasizing the non-degenerate poset codes. We verify the duality relation between the hierarchy weights of poset code and its dual. In the sequel two new parameters are defined to a class of poset codes non-degenerate with dual code is too non-degenerate in the environment. As a result enunciated in the Minimality Theorem, the Variance Theorem and the Minimality Identity in the poset spaces.

Lista de Figuras

Sumário

Introdução

Com o trabalho [Sha48] intitulado *A Mathematical Theory of Communication* C.E. Shannon dos laboratórios Bell formalizou a Teoria da Informação em 1948. A partir da década de 70 essa teoria começou a interessar também aos engenheiros, com os avanços nas pesquisas espaciais e computacionais. Os códigos corretores de erros são utilizados sempre que se deseja transmitir ou armazenar dados com confiabilidade, como por exemplo as comunicações via satélite e o armazenamento de dados em um disco magnético.

Um exemplo de código corretor de erros e um código de robô. Considere que este se desloca sobre um tabuleiro quadriculado, nas direções Norte, Sul, Leste e Oeste, de acordo com os comandos codificados como elementos do conjunto $\{0,1\}\mathtt{x}\{0,1\}$. Assim temos

$$\begin{array}{llll} Leste & \longmapsto 00 & Norte & \longmapsto 10 \\ Oeste & \longmapsto 01 & Sul & \longmapsto 11 \end{array}$$

O código definido acima é chamado como um *código fonte*. Suponhamos que ocorra uma erro na transmissão de uma mensagem e que a palavra 00 seja enviada, mas a palavra recebida seja 01, fazendo com que o robô se movimente na direção oeste em vez de leste. Devemos então recodificar as palavras do código e introduzir redundâncias que permitam detectar e corrigir erros.

Podemos, por exemplo, modificar o código da seguinte maneira

$$\begin{array}{ll} 00 & \longmapsto 00000 \\ 01 & \longmapsto 01011 \\ 10 & \longmapsto 10110 \\ 11 & \longmapsto 11101 \end{array}$$

Após a recodificação temos as duas primeiras posições sendo o código da fonte, enquanto as outras três são as redundâncias introduzidas. Através dessa recodificação, temos um novo código chamado *código de canal*.

Observe que, neste caso, se um erro for cometido na transmissão da palavra 10110, de forma que a palavra recebida seja 11110, sabemos que a palavra do código mais próxima da recebida(a que tem menor número de coordenadas distintas) é 10110, que é exatamente a palavra transmitida.

Um sistema de comunicação utilizado para transmissão da informação segue o esquema abaixo.

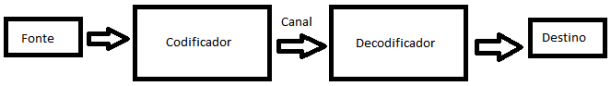

Figura 1: Sistema de Comunicação

O canal de envio da informação pode ser de radiofrequência, canal de micro-ondas, cabo, circuito integrado digital, fita magnética, HSDPA (3G) e etc. Mais detalhadamente.

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

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

Um *canal* é um meio físico pelo qual, o sinal obtido do codificador é enviado para o dispositivo 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, um computador, um celular, em que a mensagem está sendo encaminhada.

Num sistema de comunicação consideramos um conjunto finito A, chamado alfabeto, que são os dígitos. Um *código* é um subconjunto C de A^n e n é um número natural. Uma *palavra-código* é um elemento do código, contida na fonte. 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.

O estudo dos Códigos Corretores de Erros consiste em transformar o código da fonte em código de canal, detectar e corrigir os possíveis erros na recepção das mensagens e decodificar o código de canal em código da fonte.

Trabalharemos apenas com canais, possuindo as seguintes propriedades:

- Todos os símbolos têm a mesma probabilidade (pequena) de serem recebidos errados.

- Se um símbolo é recebido errado, a probabilidade de ser qualquer um dos outros é a mesma.

- Canal sem memória.

Shannon, em [Sha48], 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 valores muito grandes. Como a demonstração feita por Shannon não é construtiva, originou-se o interesse em construções de bons códigos.

As codificações mais utilizadas utilizam duas métricas principais, de Hamming [Ham50] e a de Lee [$HP03$].

O problema de decodificar um sinal y, enviado pelo codificador através do canal como um sinal x, consiste em maximizar a probabilidade de y ser enviado, dado que, x foi recebido, isto é, escolher uma palavra-código y que é mais provável de ser recebida como 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 feita por Niederreider [Nie91]. A partir de um tipo de conjunto parcialmente ordenado, ele definiu um nova classe de métricas, generalizando o problema clássico da teoria de códigos. Esse foi um dos primeiros estudos utilizando outra métrica além das usuais.

Mais tarde em [BGL95], Brualdi, Graves e Lawrence determinaram um modelo geral para essas métricas, obtendo a métrica ponderada por ordem parcial, originando os espaços poset. A métrica de Hamming e a métrica construída por Niederreider são casos particulares de métrica ponderada por ordem parcial.

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 t limitada de dígitos da informação.

Em [Wei91], Wei definiu o peso generalizado de Hamming de um subespaço como o número de coordenadas desse subespaço que não se anulam. Para cada dimensão temos um peso mínimo generalizado, o conjunto desses pesos é chamado de hierarquia do subespaço. Wei derivou algumas propriedades dessa hierarquia, e uma das mais interessantes relações é um certo tipo de Identidade de MacWilliams da hierarquia. Existe uma relação entre a hierarquia do código e a hierarquia do seu código dual. Esta relação entre as hierarquias é conhecida como Dualidade, que é utilizada para calcular os pesos generalizados de um código.

No trabalho [MF10], Moura e Firer generalizaram o conceito de Dualidade para métricas ponderadas. Em [Wei91], Wei utilizou-se da Dualidade para mostrar que

um código satisfaz a condição cadeia se, e somente se, o seu código dual a satisfaz também. Assim, como Wei, Moura e Firer mostraram a Dualidade sobre os códigos ponderados e obtiveram que um código ponderado satisfaz a condição cadeia se, e somente se, o seu código dual satisfaz a condição cadeia.

Nesse trabalho buscamos compreender os principais conceitos e problemas da teoria de códigos, desde os conceitos apresentados por Shannon em [Sha48] e Hamming, em [Ham50], até a relação de dualidade no espaço poset demonstrada, em [MF10], por Moura e Firer.

No Capítulo 1, fazemos uma introdução sobre a teoria de códigos clássica, utilizando a métrica de Hamming. Descrevemos a equivalência de códigos através de isometrias do espaço $\mathbb{F}_q^n$. Depois fazemos uma abordagem sobre códigos lineares, onde definimos o peso mínimo de um elemento, peso mínimo de um código e matriz geradora de um código. Definimos também o código dual de um código C, e a condição necessária para um código ser MDS. Finalizamos o capítulo dando exemplos de alguns códigos clássicos.

No Capítulo 2, apresentamos os códigos ponderados por uma ordem parcial e algumas de suas propriedades. Introduzimos o capítulo com definição de um poset seguida de alguns exemplos de poset's clássicos. Mostramos que qualquer conjunto bem ordenado pode ser rotulado naturalmente. A partir daí, damos ênfase aos códigos ponderados por ordens parciais, onde o poset determina o peso das palavras do código C.

No Capítulo 3, estudamos o peso generalizado de Hamming para espaços poset, essa uma generalização do peso de um elemento para subespaços, apresentado por Wei em [Wei91] e seus principais resultados como o Teorema da Monotonicidade e o Teorema da Dualidade. Estudamos também os multiconjuntos e suas relações com códigos. Apresentamos também algumas propriedades relacionadas os pesos generalizados e aos códigos poset. Estudamos também o Teorema da Dualidade para o caso poset, demonstrado por Moura e Firer em [MF10] .

No capítulo 4, para códigos não degenerados, apresentamos o conceito de minimalidade $\mathbb{P}$-MDS e o teorema da minimalidade $\mathbb{P}$-MDS. Wei, em [Wei91], definiu o conceito de código r-MDS, dessa forma, com a métrica poset, em [LLB08], Panek, Lazzarotto e Bando demonstraram alguns resultados, como o teorema da monotonicidade para o caso poset. A partir daí, o conceito de minimalidade surge da tentativa de responder se há alguma relação de dualidade de um código em um código $(\mathbb{P}, r)$-MDS e seu dual ser $(\widetilde{\mathbb{P}}, s(r))$-MDS. Assim demonstramos o Teorema da Minimalidade $\mathbb{P}$-MDS, que relaciona a minimalidade $\mathbb{P}$-MDS de um $\mathbb{P}$-código C com o peso mínimo de seu dual. Estes derivados do Teorema da Dualidade para o caso poset, apresentado por Moura e Firer em [MF10] e dos conceitos apresentados por Wei, em [Wei91].

Finalizamos esse trabalho estudando uma classe de códigos, onde C e seu dual

são não-degenerados. Nesse contexto podemos aplicar o Teorema da Minimalidade $\mathbb{P}$-MDS em C e em seu dual. Dessa forma definimos o conceito de variância $\mathbb{P}$-MDS de C, que mede a variação entre as minimalidades dos dois códigos. Em seguida demonstramos o Teorema da Variância $\mathbb{P}$-MDS de C, deste, deriva-se a Identidade de Minimalidades, que mostra que o peso mínimo, a dimensão e as minimalidades de um código e de seu dual estão inteiramente ligadas.

Capítulo 1

Códigos Corretores de Erros

1.1 Introdução

Nesse capítulo faremos uma introdução sobre a teoria clássica de códigos corretores de erros, utilizando a métrica definida por Hamming em [Ham50]. Os primeiros códigos corretores de erros foram criados por Hamming em [Ham50]. Esses códigos utilizavam um processo de verificação bit a bit. Logo mais, introduziram-se as redundância por blocos de informação, em um processo de verificação de de correção de erros. Com a modernização das tecnologias e uso em alta escala tornou-se necessário o desenvolvimento de codificadores mais eficientes com o objetivo de melhorar o aproveitamento do canal de transmissão de informações.

Como referência para esse capítulo sugerimos, [HV02], [Sha48].

1.2 Códigos e Métrica de Hamming

Em teoria de códigos corretores de erros consideramos um **alfabeto** A, que consiste em um conjunto finito. Nosso alfabeto será dado por um corpo finito, $\mathbb{F}_q$, onde $|\ \mathbb{F}_q\ |$ é a cardinalidade do corpo. A relevância de se trabalhar com corpos finitos é a presença de uma boa estrutura algébrica, assim nos permitindo fazer operações com os vetores do espaço.

Definição 1.2.1. *Dados n um número natural e um corpo finito de cardinalidade q, $\mathbb{F}_q$, definimos o espaço $\mathbb{F}_q^n$ como sendo formado pelas n-uplas com entradas em $\mathbb{F}_q$, ou seja*

$$\mathbb{F}_q^n = \{x_1 x_2 \dots x_n; x_i \in \mathbb{F}_q\}.$$

Definição 1.2.2. *Seja $\mathbb{F}_q$ um alfabeto. Um **código corretor de erros** C, ou simplesmente um **código**, é um subconjunto próprio do espaço vetorial $\mathbb{F}_q^n$. Os elementos do código são chamados de palavras-código, ou simplesmente, palavras.*

Afim de comparar as palavras do código, Hamming, em [Ham50], definiu uma distância dentro do espaço $\mathbb{F}_q^n$.

Definição 1.2.3. *Sejam* $\mathbf{u} = u_1u_2\dots u_n, \mathbf{v} = v_1v_2\dots v_n \in \mathbb{F}_q^n$. *A* ***distância de Hamming*** *entre* $\mathbf{u}$ *e* $\mathbf{v}$ *é dada por*

$$d(\mathbf{u},\mathbf{v}) = |\{i : u_i \neq v_i, 1 \leq i \leq n\}|$$

Exemplo: Em $\{0,1\}^3$ temos

$$d(\mathbf{001},\mathbf{111}) = 2$$
$$d(\mathbf{000},\mathbf{111}) = 3$$
$$d(\mathbf{100},\mathbf{110}) = 1$$

Proposição 1.2.4. [*HV02*] *Dados* $\mathbf{u},\mathbf{v}$ *e* $\mathbf{w} \in \mathbb{F}_q^n$, *valem as seguintes propriedades:*

(i) Positividade: $d(\mathbf{u},\mathbf{v}) \geq 0$, *valendo a igualdade se, e somente se,* $\mathbf{u} = \mathbf{v}$.
(ii) Simetria: $d(\mathbf{u},\mathbf{v}) = d(\mathbf{v},\mathbf{u})$.
(iii) Desigualdade Triangular: $d(\mathbf{u},\mathbf{v}) \leq d(\mathbf{u},\mathbf{w}) + d(\mathbf{w},\mathbf{v})$.

Demonstração. (*i*) Positividade.

Dados $\mathbf{u},\mathbf{v} \in \mathbb{F}_q^n$, temos que $d(\mathbf{u},\mathbf{v}) \geq 0$, pois, por definição, é a cardinalidade de um conjunto e $d(\mathbf{u},\mathbf{v}) = 0$ somente quando $x_i = y_i$, para todo $1 \leq i \leq n$.

(*ii*) Simetria.

Dados $\mathbf{u},\mathbf{v} \in \mathbb{F}_q^n$, temos $d(\mathbf{u},\mathbf{v}) = d(\mathbf{v},\mathbf{u})$ pois, $u_i = v_i$ se, e somente se, $v_i = u_i$, para todo $1 \leq i \leq n$.

(*iii*) Desigualdade triângular.

Sejam $\mathbf{u},\mathbf{v}$ e $\mathbf{w} \in \mathbb{F}_q^n$. Quando a contribuição para a distância de Hamming das i-ésimas coordenadas de $\mathbf{u}$ e $\mathbf{v}$ é nula, qualquer contribuição das i-ésimas coordenadas em $d(\mathbf{u},\mathbf{w})$ e $d(\mathbf{w},\mathbf{v})$ tornará a desigualdade verdadeira.

Vamos analisar a contribuição não-nula. Nesse caso, temos $u_i \neq v_i$ e portanto, não podemos ter $u_i = w_i$ e $w_i = v_i$. Consequentemente, $d(\mathbf{u},\mathbf{w}) + d(\mathbf{w},\mathbf{v})$ é maior ou igual a 1, que é igual a contribuição das i-ésimas coordenadas de $\mathbf{u}$ e $\mathbf{v}$.

□

Definição 1.2.5. *Dados* $\mathbf{a} \in \mathbb{F}_q^n$ *e* $t > 0$ *um número real, define-se a* ***bola*** *e a* ***esfera*** *de centro* $\mathbf{a}$ *e raio* t *respectivamente,*

$$D(\mathbf{a}, t) = \{\mathbf{u} \in I\!F_q^n; d(\mathbf{u}, \mathbf{a}) \leq t\},$$
$$S(\mathbf{a}, t) = \{\mathbf{u} \in I\!F_q^n; d(\mathbf{u}, \mathbf{a}) = t\}.$$

Lema 1.2.6. *[HV02] Para todo $\mathbf{a} \in I\!F_q^n$ e todo número real $r > 0$, temos*

$$|D(\mathbf{a}, r)| = \sum_{i=0}^{r} \left(\begin{array}{c} n \\ i \end{array} \right) (q-1)^i.$$

Demonstração. Sejam $\mathbf{a} \in I\!F_q^n$ e $r \in I\!R^*$. O número de elementos de uma esfera $S(\mathbf{a}, i)$ é

$$|S(\mathbf{a}, i)| = \left(\begin{array}{c} n \\ i \end{array} \right) (q-1)^i,$$

pois em cada coordenada da palavra $\mathbf{c}$ temos $(q-1)$ elementos de $I\!F_q^n$ distintos, podendo variar nas i coordenadas da palavra, justificando assim, a potência i. Mas como $\mathbf{c}$ tem tamanho n, pois pertence a $I\!F_q^n$, e as i entradas distintas podem percorrer em qualquer coordenada de $\mathbf{c}$, obtemos a combinação $\left(\begin{array}{c} n \\ i \end{array} \right)$.

Ainda temos que

$$S(\mathbf{a}, i) \cap S(\mathbf{a}, j) = \emptyset, \text{ se } i \neq j \text{ e } \bigcup_{i=0}^{r} S(\mathbf{a}, i) = D(\mathbf{a}, i).$$

Portanto, pelo princípio de contagem, obtemos

$$|D(\mathbf{a}, r)| = \sum_{i=0}^{r} \mid S(\mathbf{a}, i) \mid = \sum_{i=0}^{r} \left(\begin{array}{c} n \\ i \end{array} \right) (q-1)^i.$$

□

Observe que a cardinalidade de $D(\mathbf{a}, r)$ depende somente de n, q e r, pois d é invariante por translações.

Definição 1.2.7. *Seja C um código. A **distância mínima** de C é o número*

$$d = min\{d(\mathbf{u}, \mathbf{v}) : \mathbf{u}, \mathbf{v} \in C \ \ e \ \ \mathbf{u} \neq \mathbf{v}\}.$$

Sendo M o número de elementos de C, temos que calcular $\left(\begin{array}{c} M \\ 2 \end{array} \right)$ distâncias para calcular d, o que tem um custo computacional elevado. Entretanto, podemos calcular essa distância mínima de um modo mais fácil em códigos com alguma estrutura algébrica adicional que veremos mais adiante.

Dado um código C com distância mínima d, define-se

$$\kappa = \left[\ \frac{d-1}{2} \ \right],$$

onde $[t]$ representa a parte inteira de um número real t.

Lema 1.2.8. *[HV02] Seja C um código com distância mínima d. Se $\mathbf{c}$ e $\mathbf{c}'$ são palavras distintas de C, então*

$$D(\mathbf{c}, \kappa) \cap D(\mathbf{c}', \kappa) = \emptyset$$

Demonstração. Sejam $\mathbf{c}, \mathbf{c}' \in \mathbb{F}_q^n$ e κ como definido acima. Suponha, por absurdo, que exista $\mathbf{x} \in \mathbb{F}_q^n$, de forma que $\mathbf{x} \in D(\mathbf{c}, \kappa)$ e $\mathbf{x} \in D(\mathbf{c}', \kappa)$. Logo teríamos $d(\mathbf{x}, \mathbf{c}) \leq \kappa$ e $d(\mathbf{x}, \mathbf{c}') \leq \kappa$. Com isso, temos

$$d(\mathbf{c}, \mathbf{c}') \leq d(\mathbf{c}, \mathbf{x}) + d(\mathbf{x}, \mathbf{c}') \leq 2\kappa.$$

Portanto, $d(\mathbf{c}, \mathbf{c}') \leq 2\kappa \leq d - 1$, o que é um absurdo, pois $d(\mathbf{c}, \mathbf{c}') \geq d$.
□

Teorema 1.2.9. *[HV02] Seja C um código com distância mínima d, então C pode corrigir até $\kappa = \left[\frac{d-1}{2}\right]$ erros e detectar até $d-1$ erros.*

Demonstração. Se ao transmitirmos uma palavra $\mathbf{c}$ do código cometermos t erros com $t \leq \kappa$, recebendo a palavra r, então $d(\mathbf{r}, \mathbf{c}) = t \leq \kappa$; enquanto que, pelo Lema 1.2.8, a distância de r a qualquer outra palavra do código é menor que κ. Isso determina $\mathbf{c}$ univocamente a partir de r, corrigindo a palavra recebida e substituindo-a por $\mathbf{c}$.

Por outro lado, dada uma palavra do código, podemos introduzir até $d-1$ erros sem encontrar outra palavra do código, e assim podemos detectar até $d-1$ erros.
□

Definição 1.2.10. *Sejam $C \subset \mathbb{F}_q^n$ um código com distância mínima d e $\kappa = \left[\frac{d-1}{2}\right]$. O código C será dito **perfeito** se a união disjunta das bolas centradas nas palavras do código forma todo espaço $\mathbb{F}_q^n$, ou seja, se*

$$\bigcup_{\mathbf{c} \in C} D(\boldsymbol{c}, \kappa) = \mathbb{F}_q^n.$$

Usando o Teorema 1.2.9 podemos traçar uma estratégia para detecção e correção de erros.

Quando o receptor recebe uma palavra $\mathbf{r}$, verifica-se uma das seguintes situações:

i) A palavra recebida $\mathbf{r}$ encontra-se num disco de raio κ em torno de uma palavra $\mathbf{c}$ do código (essa palavra é única, pelo Teorema 1.2.9). Substitua a palavra $\mathbf{r}$ pela palavra $\mathbf{c}$.

ii) A palavra recebida $\mathbf{r}$ não se encontra em nenhum disco de raio κ em torno de uma palavra $\mathbf{c}$ do código. Nesse caso, não é possível decodificar $\mathbf{r}$ com boa margem de segurança.

Observe que nem sempre essa estratégia é segura, pois em i) poderíamos ter cometido mais do que κ erros afastando $\mathbf{r}$ da palavra transmitida e aproximando-a de outra palavra do código. Observe também que ii) não ocorre em códigos perfeitos.

1.2.1 Equivalência de Códigos

Definição 1.2.11. *Uma função $F : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$ é uma **isometria** de $\mathbb{F}_q^n$ se esta preserva a distância de Hamming, ou seja,*

$$d(\mathbf{F}(\mathbf{x}), \mathbf{F}(\mathbf{y})) = d(\mathbf{x}, \mathbf{y}); \text{ para todos } \mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$$

Nas proposições abaixo exibiremos propriedades das isometrias para a métrica de Hamming.

Proposição 1.2.12. [*MF10, Corolário* 1.8] *Seja T o conjunto de todas as isometrias de $\mathbb{F}_q^n$, então T é um grupo.*

Proposição 1.2.13. [*HV02*] *Toda isometria de $\mathbb{F}_q^n$ é uma bijeção de $\mathbb{F}_q^n$.*

Demonstração. Seja $F : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$ uma isometria. Suponha que, para $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$ tenhamos $F(\mathbf{x}) = F(\mathbf{y})$. Logo, $d(\mathbf{x}, \mathbf{y}) = \mathbf{d}(\mathbf{F}(\mathbf{x}), \mathbf{F}(\mathbf{y})) = \mathbf{0}$, o que implica $\mathbf{x} = \mathbf{y}$. Com isso, F é injetora e, como toda aplicação injetora de um conjunto finito nele próprio é sobrejetora, então F é uma bijeção.

□

Proposição 1.2.14. [*HV02*] *i) A função identidade de $\mathbb{F}_q^n$ é uma isometria.*
ii) Se F é uma isometria de $\mathbb{F}_q^n$, então F^{-1} é uma isometria de $\mathbb{F}_q^n$.
iii) Se F e G são isometrias de $\mathbb{F}_q^n$, então $F \circ G$ é uma isometria de $\mathbb{F}_q^n$.

Demonstração. i) Seja F a função identidade de $\mathbb{F}_q^n$. Dessa forma, para $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$, temos $F(\mathbf{x}) = \mathbf{x}$ e $F(\mathbf{y}) = \mathbf{y}$, e portanto,

$$d(F(\mathbf{x}), F(\mathbf{y})) = d(\mathbf{x}, \mathbf{y}).$$

ii) Se $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$ e F é uma isometria de $\mathbb{F}_q^n$, pela Proposição 1.2.13, existe a função inversa F^{-1} de F. Como F é uma isometria, segue que

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

o que prova que F^{-1} é uma isometria.

iii) Sejam $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$, usando o fato que F e G são isometrias, temos,

$$d(F(G(\mathbf{x})), F(G(\mathbf{y}))) = d(G(\mathbf{x}), G(\mathbf{y})) = d(\mathbf{x}, \mathbf{y}).$$

Portanto, $F \circ G$ é uma isometria.

□

Definição 1.2.15. *Dados 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 $F(C) = C'$.*

Segue da Proposição 1.2.13 que a equivalência de códigos é uma relação de equivalência.

Exemplo: Se π é uma bijeção do conjunto $\{1, \ldots, n\}$ nele próprio, também chamada de permutação de $\{1, \ldots, n\}$, a aplicação permutação de coordenadas

$$\begin{array}{rccc} T_\pi : & \mathbb{F}_q^n & \longrightarrow & \mathbb{F}_q^n \\ & a_1 a_2 \ldots a_n & \mapsto & a_{\pi(1)} a_{\pi(2)} \ldots a_{\pi(n)} \end{array}$$

é uma isometria.

Vamos utilizar as isometrias induzidas por permutações para caracterizar as isometrias lineares de $\mathbb{F}_q^n$.

Lema 1.2.16. [*HV02*] *Dada uma isometria F de $\mathbb{F}_q^n$ com $n \geq 2$ e, dados elementos $a_1, \ldots, a_{n-1} \in \mathbb{F}_q$, existem $a'_1, \ldots, a'_{n-1} \in \mathbb{F}_q$, uma bijeção $f_n : \mathbb{F}_q \longrightarrow \mathbb{F}_q$ e uma permutação σ de $\{1, \ldots, n\}$ tais que*

$$(T_\sigma \circ F)(a_1 a_2 \ldots a_{n-1} x) = (a'_1 a'_2 \ldots a'_{n-1} f_n(x)), \quad \textit{para todo} \quad x \in \mathbb{F}_q.$$

Lema 1.2.17. [*HV02*] *Seja G uma isometria de $\mathbb{F}_q^n$ e sejam $a_1, \ldots, a_{n-1}, a'_1, \ldots, a'_{n-1}$ elementos fixos de $\mathbb{F}_q$. Suponhamos que exista uma bijeção $f : \mathbb{F}_q \longrightarrow \mathbb{F}_q$ tal que*

$$G(a_1 a_2 \ldots a_{n-1} x) = (a'_1 \ldots a'_{n-1} f(x)), \quad \textit{para todo} \quad x \in \mathbb{F}_q.$$

Então, existe uma isometria H de $\mathbb{F}_q^{n-1}$ tal que

$$G(x_1 \ldots x_{n-1} x_n) = (H(x_1 \ldots x_{n-1}), f(x)), \forall (x_1, \ldots, x_n) \in \mathbb{F}_q^n.$$

Teorema 1.2.18. *[HV02] Seja $F : \mathbb{F}_q^n \to \mathbb{F}_q^n$ uma isometria, então existem uma permutação π de $\{1, \ldots, n\}$ e bijeções f_i de $\mathbb{F}_q$, para $i = 1, \ldots, n$, tais que*

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

Demonstração. Faremos a demonstração utilizando indução sobre n.

Se $n = 1$, e F é uma isometria de $\mathbb{F}_q$, então temos que F é bijeção. Dessa forma, como a função identidade é uma permutação, podemos escrever $F = I_d \circ F$.

Suponhamos $n > 1$ e que o resultado seja válido para $n - 1$.

Sejam $a_1, \ldots, a_{n-1} \in \mathbb{F}_q$. Pelo Lema 1.2.16, existem $a'_1, \ldots, a'_{n-1} \in \mathbb{F}_q$, uma bijeção $f_n : \mathbb{F}_q \longrightarrow \mathbb{F}_q$ e uma permutação σ de $\{1, \ldots, n\}$ tais que

$$(T_\sigma \circ F)(a_1 \ldots a_{n-1}x) = (a'_1 \ldots a'_{n-1} f_n(x)), \quad \text{para todo} \quad x \in \mathbb{F}_q.$$

Pelo Lema 1.2.17, existe uma isometria H de $\mathbb{F}_q^{n-1}$ tal que

$$(T_\sigma \circ F)(x_1 \ldots x_n) = (H(x_1 \ldots x_{n-1}), f_n(x_n)). \tag{1.1}$$

Pela hipótese de indução existem permutações τ^{-1} de $1, \ldots, n-1$ e bijeções $f_1, \ldots, f_{n-1}$ de $\mathbb{F}_q$ tais que

$$H = (T_{\tau'})' \circ (T_{f_1}^1)' \circ \cdots \circ (T_{f_{n-1}}^{n-1})', \tag{1.2}$$

onde

$$\begin{array}{rccc} (T_{\tau'})' : & \mathbb{F}_q^{n-1} & \longrightarrow & \mathbb{F}_q^{n-1} \\ & x_1 \ldots x_{n-1} & \mapsto & x_{\tau'(1)} \ldots x_{\tau'(n-1)} \end{array}$$

e, para $i = 1, \ldots, n-1$,

$$\begin{array}{rccc} (T_{f_i}^i)' : & \mathbb{F}_q^{n-1} & \longrightarrow & \mathbb{F}_q^{n-1} \\ & x_1 \ldots x_{n-1}) & \mapsto & x_1 \ldots f_i(x_i) \ldots x_{n-1} \end{array}.$$

Definamos a permutação τ de $\{1, \ldots, n\}$ da seguinte forma

$$\tau(i) = \begin{cases} \tau', & \text{se} \quad 1 \leq i \leq n-1 \\ n, & \text{se} \quad i = n \end{cases}$$

e ponhamos

$$\begin{array}{rccc} T_\sigma : & \mathbb{F}_q^n & \longrightarrow & \mathbb{F}_q^n \\ & (x_1 \ldots x_n) & \mapsto & (x_{\tau(1)} \ldots x_{\tau(n)}) \end{array}.$$

Para $i = 1, \ldots, n$, consideremos

$$(T^i_{f_i})' : \begin{array}{ccc} \mathbb{F}_q^n & \longrightarrow & \mathbb{F}_q^n \\ (x_1 \ldots x_n) & \mapsto & (x_1 \ldots f_i(x_i) \ldots x_n) \end{array}.$$

Assim, das equações (1.1) e (1.2), temos

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

Portanto, usando o fato de que $T_\sigma^{-1} = T_{\sigma^{-1}}$ e que $T_\sigma \circ T_{\sigma'} = T_{\sigma\circ\sigma'}$ e pondo $\pi = \sigma^{-1} \circ \tau$, temos

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

o que prova o resultado.

□

Corolário 1.2.19. [*HV02*] *Sejam C e C' dois códigos em $\mathbb{F}_q^n$. Então C e C' são equivalentes se, e somente se, existem uma permutação π de $\{1, \ldots, n\}$ e bijeções $f_1, \ldots, f_n$ de $\mathbb{F}_q$ tais que*

$$C' = \{f_{\pi(1)}(x_{\pi(1)}) \ldots f_{\pi(n)}(x_{\pi(n)}) / x_1 \ldots x_n \in C\}.$$

Dois códigos de comprimento n sobre um alfabeto $\mathbb{F}_q$ (cujos elementos chamaremos de letras), são equivalentes se, e somente se, um pode ser obtido do outro mediante uma sequência de operações do tipo:

(i) Substituição das letras numa dada posição fixa em todas as palavras do código por meio de uma bijeção de $\mathbb{F}_q$.

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

1.3 Códigos Lineares

Nessa seção fazemos uma abordagem sobre os códigos lineares, destacando suas principais propriedades.

Definição 1.3.1. *Um código $C \subset \mathbb{F}_q^n$ é chamado **código linear** se é um subespaço vetorial de $\mathbb{F}_q^n$.*

Sejam k a dimensão de um código C e $\{v_1, \ldots, v_k\}$ uma bases de C, então todo elemento de C se escreve como combinação linear, de modo único, na forma

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

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

$$M = |C| = q^k,$$

e, consequentemente,

$$dim_k C = k = log_q q^k = log_q M.$$

Definição 1.3.2. *Dado* $\mathbf{x} = x_1 x_2 \dots x_n \in \mathbb{F}_q^n$, *define-se o* ***peso*** *de* $\mathbf{x}$ *como sendo o número inteiro*

$$\omega(\mathbf{x}) := |\{i : x_i \neq 0\}|.$$

Em outras palavras, $\omega(\mathbf{x}) = d(\mathbf{x}, \mathbf{0})$, onde d é a métrica de Hamming.

Definição 1.3.3. *Define-se o* ***peso mínimo*** *de um código linear* C *como o inteiro*

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

Proposição 1.3.4. [*HV02*] *Seja* $C \subset \mathbb{F}_q^n$ *um código linear com distância mínima* d, *então*
i) Para quaisquer $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$, *temos* $d(\mathbf{x}, \mathbf{y}) = \omega(\mathbf{x} - \mathbf{y})$.
ii) $d = \omega(C)$.

Demonstração. O item (i) segue diretamente das definições da métrica de Hamming e de peso de um código.

Em (ii), considere $\mathbf{x}, \mathbf{y} \in C$ com $\mathbf{x} \neq \mathbf{y}$ tais que $d(\mathbf{x}, \mathbf{y}) = d$. Daí $\mathbf{x}$ e $\mathbf{y}$ possuem exatamente d coordenadas distintas. Tomando $\mathbf{z} = \mathbf{x} - \mathbf{y} \in C \backslash \{0\}$, temos $d(\mathbf{x}, \mathbf{y}) = \omega(\mathbf{z})$, e como $\mathbf{z}$ tem o mínimo de coordenadas não nulas por construção, obtemos $\omega(\mathbf{z}) = \omega(C)$. Portanto, $d = \omega(C)$.

□

Com a proposição acima, basta efetuar $M - 1$ cálculos de distâncias em um código linear com M elementos para calcularmos a distância mínima, sendo que anteriormente era preciso efetuar $\begin{pmatrix} M \\ 2 \end{pmatrix}$ cálculos de distâncias. A partir do item (ii) da Proposição 1.3.4, definimos.

Definição 1.3.5. *A distância mínima de um código* C *é chamada de* ***peso mínimo*** *do código.*

Podemos descrever códigos lineares C como subespaços vetoriais C de um espaço vetorial $\mathbb{F}_q^n$. Mais precisamente como imagem ou como núcleo de transformações lineares.

Escolha uma base $\{v_1 \dots v_k\}$ de C e considere a aplicação linear

$$\begin{array}{rccc} T: & \mathbb{F}_q^k & \longrightarrow & \mathbb{F}_q^n \\ & x = x_1 x_2 \dots x_k & \mapsto & x_1 v_1 + \cdots + x_k v_k. \end{array}$$

Observe que T é uma transformação linear injetora tal que $Im(T) = C$. Portanto, dado um código $C \subset \mathbb{F}_q^n$ de dimensão k é possível a determinar uma transformação linear injetora

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

e definir $C = Im(T)$. Note que os elementos de C são parametrizados pelos elementos de $\mathbb{F}_q^k$ através de T, o que torna fácil gerar todos os elementos de C. Entretanto, fica difícil decidir se um elemento $\mathbf{v}$ de $\mathbb{F}_q^n$ pertence ou não a C, pois seria necessário resolver um sistema de n equações nas k incógnitas $x_1, \dots, x_k$

$$x_1 v_1 + x_2 v_2 + \cdots + x_k v_k = \mathbf{v},$$

e essa resolução geralmente tem um custo computacional elevado.

Por outro lado, para representarmos C através do núcleo de uma transformação linear, basta tomarmos $C' \subset \mathbb{F}_q^n$ um subespaço complementar de C, ou seja,

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

e considere a aplicação linear

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

cujo núcleo é exatamente C. Agora basta verificar se $H(v)$ é ou não o vetor nulo de $\mathbb{F}_q^{n-k}$ para saber se $v \in \mathbb{F}_q^n$ é ou não um elemento de C, o que tem um custo computacional muito menor.

Exemplo: Considere o corpo finito com três elementos $\mathbb{F}_3 = \{0, 1, 2\}$. Seja $C \subset \mathbb{F}_3^4$ o código gerado pelos vetores $\mathbf{v_1} = \mathbf{1011}$ e $\mathbf{v_2} = \mathbf{0112}$. Esse código possui 9 elementos, pois tem dimensão 2 sobre um corpo de 3 elementos.

Uma representação paramétrica de C é dada por

$$x_1 \mathbf{v_1} + x_2 \mathbf{v_2}$$

variando x_1 e x_2 em $\mathbb{F}_3$. O código C pode ser representado como núcleo da transformação linear

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

Definição 1.3.6. *Dois códigos lineares C e C' são* ***linearmente equivalentes*** *se existir uma isometria linear $T : \mathbb{F}_q^n \to \mathbb{F}_q^n$ tal que $T(C) = C'$.*

Com isso, C é linearmente equivalente a C' em $\mathbb{F}_q^n$ se, e somente se,

$$C' = \{c_1 x_{\pi(1)} \dots c_n x_{\pi(n)} / x_1 \dots x_n \in C, c_i \in \mathbb{F}_q^*\}.$$

Isto equivale a dizer que dois códigos lineares são linearmente equivalentes se, e somente se, cada um deles pode ser obtido do outro mediante uma seqüencia de operações elementares do tipo:

- Multiplicação dos elementos numa dada posição fixa por um escalar não nulo em todas as palavras.
- Permutação das posições de todas as palavras do código, mediante uma permutação fixa de $\{1, 2, \dots, n\}$.

1.3.1 Matriz Geradora de um Código

Definição 1.3.7. *Um* ***código linear*** *$C \subset \mathbb{F}_q^n$ de dimensão k é dito um $[n, k]_q$-código.*

Seja $\beta = \{\mathbf{v_1}, \dots, \mathbf{v_k}\}$ uma base ordenada de C, com $\mathbf{v_i} = v_{i1} \dots v_{in}$, para $i = 1, \dots, k$ e considere a seguinte matriz

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

Definição 1.3.8. *A matriz G é chamada* ***matriz geradora*** *de C associada à base β.*

Considere agora a seguinte transformação linear:

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

Se $\mathbf{x} = (x_1 \dots x_k) \in \mathbb{F}_q^k$, temos

$$T(\mathbf{x}) = \mathbf{x}G = x_1 v_1 + \cdots + x_k v_k,$$

logo $T(\mathbb{F}_q^k) = C$. Consideraremos, $\mathbb{F}_q^k$ como código da fonte, C o código de canal e T uma codificação.

Lembramos que G não é univocamente determinada, pois depende da escolha da base β. Uma base de um espaço vetorial pode ser obtida da outra através de operações do tipo:

- permutação de dois elementos da base;
- multiplicação de um elemento da base por um escalar não nulo;
- substituição de um elemento da base por ele mesmo somado a um múltiplo escalar de outro elemento da base.

Como os elementos da base do código C formam as linhas da matriz geradora, uma outra matriz geradora de C pode ser obtida por:

- (L1) permutação de duas linhas ;
- (L2) multiplicação de uma linha por um escalar não nulo;
- (L3) adição de um múltiplo escalar de uma linha a outra.

Com isso, dada uma matriz G qualquer cujas linhas são linearmente independentes, podemos construir um código C como imagem da transformação T.

Definição 1.3.9. *Uma matriz geradora G de um código C estará na forma padrão se*

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

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

Dado um código C, nem sempre teremos uma matriz geradora de C na forma padrão. Por exemplo, a matriz geradora

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

de um código $C \subset \mathbb{F}_2^5$ nunca estará na forma padrão, pois não é possível obtê-la usando apenas as operações descritas acima. Entretanto, se permutarmos as colunas trocando a primeira com a terceira e a segunda com a quarta, teremos uma matriz

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

na forma padrão, G' é matriz geradora de um código C' equivalente a C, pois as operações realizadas sobre as colunas de G são também efetuadas sobre cada palavra de C.

Assim, realizando operações do tipo:

- (C1) permutação de duas colunas;
- (C2) multiplicação de uma coluna por um escalar não nulo,

sobre uma matriz geradora G de um código C, obtemos G', que é matriz geradora de um código C' equivalente a C.

Com a operação $(C1)$ descrita acima, podemos partir para o próximo resultado.

Teorema 1.3.10. [*HV02*] *Dado um código C, existe um código equivalente C' com matriz geradora na forma padrão.*

Demonstração. Seja G uma matriz geradora de C.

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

Se G estiver na forma padrão, nada temos a fazer. Se G não está na forma padrão, realizando uma operação do tipo $(C1)$ podemos supor $g_{11} \neq 0$, pois a primeira linha de G é não nula devido à independência linear entre suas linhas. Multiplicando a primeira linha por g_{11}^{-1}, ficamos com 1 no lugar de g_{11} por meio de $(L2)$.

Somando à segunda, terceira, etc linhas, respectivamente, a primeira linha multiplicada respectivamente por $-g_{21}, -g_{31}$, etc, obtemos por meio de $(L3)$ uma matriz na forma

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

Na segunda linha dessa matriz certamente temos um elemento não nulo, e este pode ser colocado na segunda linha e segunda coluna por meio da operação $(C1)$. Multiplicando a segunda linha pelo inverso desse elemento, obtemos a matriz

$$\begin{pmatrix} 1 & c_{12} & c_{13} & \cdots & c_{1n} \\ 0 & 1 & c_{23} & \cdots & c_{2n} \\ 0 & c_{32} & c_{33} & \cdots & c_{3n} \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & c_{k2} & c_{k3} & \cdots & c_{kn} \end{pmatrix}.$$

Novamente através de operações $(L3)$ obtemos a matriz

$$\begin{pmatrix} 1 & 0 & d_{13} & \cdots & d_{1n} \\ 0 & 1 & d_{23} & \cdots & d_{2n} \\ 0 & 0 & d_{33} & \cdots & d_{3n} \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & d_{k3} & \cdots & d_{kn} \end{pmatrix}.$$

Procedendo sucessivamente dessa forma, obtemos uma matriz na forma padrão

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

□

1.3.2 Códigos Duais

Definição 1.3.11. *Sejam* $\mathbf{u}, \mathbf{v} \in \mathbb{F}_q^n$. *O* ***produto escalar*** *de* $\mathbf{u}$ *e* $\mathbf{v}$, *denotado por* $\langle \mathbf{u}, \mathbf{v} \rangle$, *é o elemento de* $\mathbb{F}_q^n$

$$\langle \mathbf{u}, \mathbf{v} \rangle = u_1 v_1 + \cdots + u_n v_n,$$

com $\langle \cdot \rangle$ *sendo uma forma bilinear definida em* $\mathbb{F}_q^n$.

Definição 1.3.12. *Seja* $C \subset \mathbb{F}_q^n$ *um código linear. O* ***dual*** *de* C, *denotado por* $C^\perp$ *é o conjunto*

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

Lema 1.3.13. [*HV02*] *Se* $C \subset \mathbb{F}_q^n$ *é um código linear com matriz geradora* G, *então*
i) $C^\perp$ *é um subespaço vetorial de* $\mathbb{F}_q^n$.
ii) $\mathbf{x} \in C^\perp$, *se e somente se,* $G\mathbf{x}^t = 0$.

Demonstração.
(i) Dados $\mathbf{u}, \mathbf{v} \in C^\perp$ e $\lambda \in \mathbb{F}_q$, temos,

$$\langle \mathbf{u} + \lambda \mathbf{v}, \mathbf{x} \rangle = \langle \mathbf{u}, \mathbf{x} \rangle + \lambda \langle \mathbf{v}, \mathbf{x} \rangle = 0, \quad \text{para todo } \mathbf{x} \in C.$$

Portanto, $\mathbf{u} + \lambda \mathbf{v} \in C^\perp$ e $C^\perp$ é um subespaço vetorial de $\mathbb{F}_q^n$.

(ii) $\mathbf{x} \in C^\perp$ se, e somente se, $\langle \mathbf{x}, \mathbf{v} \rangle = 0$, para todo $\mathbf{v} \in C$. Como os elementos de C são gerados por uma base, é suficiente dizer que $\mathbf{x}$ é ortogonal a uma base de C, implicando $G\mathbf{x}^\mathbf{t} = 0$, já que as linhas de G formam uma base de C.
□

Definição 1.3.14. *O subespaço vetorial $C^{\perp}$ de $\mathbb{F}_q^n$ é também um código linear e o chamaremos de* ***código dual*** *de C.*

Proposição 1.3.15. *[HV02] Seja $C \subset \mathbb{F}_q^n$ um código de dimensão k com matriz geradora $G = (Id_k|A)$ na forma padrão, então*
i) $dim C^{\perp} = n - k$;
ii) $H = (-A^t|Id_{n-k})$ é uma matriz geradora de $C^{\perp}$.

Demonstração. (i) Dado um código C com matriz geradora G, pelo Lema 1.3.13 temos que, $\mathbf{x} = x_1 \dots x_n \in C^{\perp}$ se, e somente se, $G \cdot \mathbf{x^t} = 0$. Como G está na forma padrão temos

$$G\mathbf{x^t} = 0 \Leftrightarrow \begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix} = -A \begin{pmatrix} x_{k+1} \\ \vdots \\ x_n \end{pmatrix}.$$

Como existem q^{n-k} possíveis escolhas distintas para $x_{k+1}, \dots, x_n$, concluímos que $C^{\perp}$ tem q^{n-k} elementos e sua dimensão é $n - k$.

(ii) Devido ao bloco Id_{n-k}, as linhas de H são linearmente independentes e, assim geram um subespaço vetorial de dimensão $n - k$ que está contido em $C^{\perp}$, pois as linhas de H são ortogonais às linhas de G. Como esses subespaços têm a mesma dimensão e o primeiro está contido no seguinte, estes coincidem. Portanto, $H = (-A^t|Idn - k)$ é uma matriz geradora de $C^{\perp}$.

□

Lema 1.3.16. *[HV02] Seja $C \subset \mathbb{F}_q^n$ um código linear. Para toda permutação π de $\{1, \dots, n\}$, para todo $c \in \mathbb{F}_q^*$ e para todo $j = 1, \dots, n$, temos*
i) $(T_{\pi}(C))^{\perp} = T_{\pi}(C^{\perp})$.
ii) $(T_c^j(C))^{\perp} = T_{c^{-1}}^j(C^{\perp})$.

Demonstração. i) Dado $\mathbf{u} = u_1 u_2 \dots u_n \in C$ temos que, para todo $\mathbf{v} = v_1 v_2 \dots v_n \in C^{\perp}$,

$$\langle \mathbf{u}, \mathbf{v} \rangle = u_1 v_1 + \dots + u_n v_n = 0.$$

Mas $u_{\pi(1)} v_{\pi(1)} + \dots + u_{\pi(n)} v_{\pi(n)} = 0$, pois $\pi(j) = i, \text{para todo} j = 1, \dots, n$. Com isso, $\langle T_{\pi}(\mathbf{u}), T_{\pi}(\mathbf{v}) \rangle = 0$ e portanto, $(T_{\pi}(C))^{\perp} = T_{\pi}(C^{\perp})$.

ii) Como acima, dados $\mathbf{u} \in C$ e $\mathbf{v} \in C^{\perp}$, temos

$$T_c^j(\mathbf{u}) = u_1 u_2 \dots c u_j \dots u_n$$

e

$$T_{c^{-1}}^j(\mathbf{v}) = v_1 v_2 \dots c^{-1} v_j \dots v_n.$$

Logo

$$\begin{aligned} \langle T_c^j(\mathbf{u}), T_{c^{-1}}^j(\mathbf{v})\rangle &= u_1v_1 + \cdots + cu_jc^{-1}v_j + \cdots + u_nv_n \\ = u_1v_1 + \cdots + u_jcc^{-1}v_j + \cdots + u_nv_n &= u_1v_1 + \cdots + u_jv_j + \cdots + u_nv_n = 0. \end{aligned}$$

Portanto, como $\langle T_c^j(C), T_{c^{-1}}^j(C^\perp)\rangle = 0$, concluímos que $(T_c^j(C))^\perp = T_{c^{-1}}^j(C^\perp)$.
□

Proposição 1.3.17. [*HV02*] *Sejam C e D dois códigos lineares em $\mathbb{F}_q^n$. Se C e D são linearmente equivalentes, então $C^\perp$ e $D^\perp$ também são linearmente equivalentes.*

Demonstração. Sejam C e D dois códigos lineares contidos em $\mathbb{F}_q^n$. Sabemos que se C e D são linearmente equivalentes, existem uma permutação π de $\{1,\ldots,n\}$ e $c_1,\ldots,c_n \in \mathbb{F}_q^*$ tais que

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

Agora, pelo Lema 1.3.16, segue,

$$D^\perp = (T_\pi \circ T_{c_1}^1 \circ \cdots \circ T_{c_n}^n(C))^\perp = T_\pi \circ T_{c_1^{-1}}^1 \circ \cdots \circ T_{c_n^{-1}}^n(C^\perp)$$

e portanto, $C^\perp$ é linearmente equivalente a $D^\perp$.
□

Corolário 1.3.18. [*HV02*] *Se $C \subset \mathbb{F}_q^n$ é um código linear de dimensão k, então $C^\perp$ é um código linear de dimensão $n-k$.*

Demonstração. Pelo Teorema 1.3.10, C é equivalente a um código D, com a mesma dimensão k e com matriz geradora na forma padrão. Daí, pela Proposição 1.3.15, $dim D^\perp = n-k$. Agora, pela Proposição 1.3.17, $D^\perp$ é equivalente a $C^\perp$ e de dimensão $n-k$ e isso mostra o resultado.
□

Lema 1.3.19. [*HV02*] *Suponha que C seja um código de dimensão k em $\mathbb{F}_q^n$ com matriz geradora G. Uma matriz H de ordem $(n-k)\times n$, com coeficientes em $\mathbb{F}_q$ e linhas linearmente independentes, é uma matriz geradora de $C^\perp$ se, e somente se,*

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

Demonstração. O subespaço vetorial gerado pelas linhas de H tem dimensão $n-k$, que é igual à dimensão de $C^\perp$. Representando por $\mathbf{g_i} = g_{i1},\ldots,g_{in}$, com $i = 1,\ldots,k$ e $\mathbf{h_j} = h_{j1},\ldots,h_{jn-k}$, com $j = 1,\ldots,n-k$, as linhas de G e H, respectivamente, temos

$$(G \cdot H^t)_{i,j} = \langle \mathbf{g_i}, \mathbf{h_j}\rangle = 0.$$

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

Por outro lado, $G \cdot H^t = 0$ nos diz que todos os vetores do subespaço gerado pelas linhas de H estão em $C^\perp$ e, como as dimensões desses subespaços coincidem, temos

$$G \cdot H^t = 0 \text{ se, e somente se, } C^\perp \text{ é gerado pelas linhas de } H.$$

□

Corolário 1.3.20. *[HV02]* $(C^\perp)^\perp = C$.

Demonstração. Por definição $C \subseteq (C^\perp)^\perp$. Como

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

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

□

A proposição a seguir nos mostra como determinar se um elemento de $\mathbb{F}_q^n$ pertence ou não a um código $C \subset \mathbb{F}_q^n$.

Proposição 1.3.21. *[HV02] Seja $C \subset \mathbb{F}_q^n$ um código linear tal que $C^\perp$ tem matriz geradora H, então*

$$\mathbf{v} \in C \quad \textit{se, e somente se, } H\mathbf{v^t} = 0.$$

Demonstração. Pelo Corolário 1.3.20 e o Lema 1.3.13 (ii) temos

$$\mathbf{v} \in C \text{ se, e somente se, } \mathbf{v} \in (C^\perp)^\perp.$$

Como

$$\mathbf{v} \in (C^\perp)^\perp \text{ se, e somente se, } H\mathbf{v^t} = 0,$$

segue o resultado.

□

Com isso, os elementos de C ficam determinados por uma condição de anulamento, o que tem um custo computacional baixo, pois basta determinar se $H\mathbf{v^t}$ é o vetor nulo de $\mathbb{F}_q^n$ para que $\mathbf{v} \in C$. A matriz H geradora de $C^\perp$ é chamada de **matriz de verificação de paridade** de C.

Definição 1.3.22. *Dados um código linear $C \subset \mathbb{F}_q^n$ com matriz de verificação de paridade H e um vetor $\mathbf{v} \in \mathbb{F}_q^n$, dizemos que $H\mathbf{v^t}$ é a **síndrome** de $\mathbf{v}$.*

Vejamos a seguir as informações que a matriz de verificação de paridade pode nos oferecer à respeito do peso d de um código.

Proposição 1.3.23. *Dado um código C com matriz verificação de paridade H, temos que o peso de C é maior ou igual a s se, e somente se, quaisquer $s-1$ colunas de H são linearmente independentes.*

Demonstração. Sejam $\mathbf{c} = c_1 \dots c_n \in C^*$ e $\mathbf{h^1}, \dots, \mathbf{h^n}$ as colunas de H. Como $H\mathbf{c^t} = 0$, temos

$$0 = H\mathbf{c^t} = \sum c_i \mathbf{h^i}. \tag{1.3}$$

Como $\omega(\mathbf{c})$ é o número de coordenadas não nulas de $\mathbf{c}$, se $\omega(\mathbf{c}) \leq s-1$, teríamos uma combinação nula de t colunas de H, $1 \leq t \leq s-1$, contradizendo o fato de que quaisquer $s-1$ colunas de H são linearmente independentes. Logo $\omega(\mathbf{c}) \geq s$ e, portanto, $\omega(C) \geq s$.

Reciprocamente suponhamos que H tenha $s-1$ colunas linearmente dependentes, sendo elas $\mathbf{h^{i_1}}, \mathbf{h^{i_2}}, \dots, \mathbf{h^{i_{s-1}}}$. Daí, existem $c_{i_1}, c_{i_2}, \dots, c_{i_{s-1}} \in I\!F_q$ nem todos nulos, tais que

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

Com isso, $\mathbf{c} = 0 \dots c_{i_1} 0 \dots c_{i_2} 0 \dots c_{i_{s-1}} 0 \dots 0 \in C$ e, consequentemente, $\omega(\mathbf{c}) \leq s-1 < s$, o que é um absurdo, pois $\omega(C) \geq s$, por hipótese. Portanto, quaisquer $s-1$ colunas de H são linearmente independentes.

□

Teorema 1.3.24. *Seja H a matriz de verificação de paridade de um código C. Então $\omega(C) = s$ se, e somente se, quaisquer $s-1$ colunas de H são linearmente independentes e existem s colunas de H linearmente dependentes.*

Demonstração. Suponhamos que $\omega(C) = s$, logo todo conjunto de $s-1$ colunas de H é linearmente independente. Com isso, existem s colunas de H linearmente dependentes, pois caso contrário, pela Proposição 1.3.23, teríamos que $\omega(C) \geq s+1$, contradizendo a hipótese.

Reciprocamente supondo que quaisquer $s-1$ colunas de H são linearmente independentes e que existam s colunas linearmente dependentes, temos pela Proposição 1.3.23 que $\omega(C) \geq s$. Mas $\omega(C)$ não pode ser maior que s, pois novamente pela Proposição 1.3.23, existiriam s colunas de H linearmente independentes, contrariando a hipótese. Portanto, $\omega(C) = s$.

□

Corolário 1.3.25. *(Cota de Singleton) Os parâmetros (n, k, d) de um código linear satisfazem à desigualdade*

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

Demonstração. Sendo H a matriz de verificação de paridade, seu posto é $n - k$. Pelo Teorema 1.3.24, sabemos que $d - 1$ é menor ou igual ao posto da matriz H. Portanto,

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

□

Definição 1.3.26. *Quando tivermos um código em que $d = n - k + 1$, chamaremos esse código de* ***MDS*** *(Maximum Distance Separable).*

1.3.3 Exemplos de Códigos

Exemplo 1 (Código de Hamming.) Um **código de Hamming** de ordem m sobre $\mathbb{F}_2$ é um código com matriz teste de paridade H_m de ordem $m \times n$, cujas colunas são os elementos de $\mathbb{F}_2^m \backslash \{0\}$ numa ordem qualquer.

Se $C \subset \mathbb{F}_2^n$ é o código determinado pela matriz H_m, temos $n = 2^m - 1$, pela própria construção de H_m. Com isso, sua dimensão é $k = n - m = 2^m - m - 1$. A distância mínima em um código de Hamming é $d = 3$, pois é possível encontrar 3 colunas linearmente dependentes em H_m. Façamos um exemplo para ilustrar um código de Hamming. Considere a matriz

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

assim $m = 3$, $n = 2^3 - 1 = 7$ e $k = 7 - 3 = 4$.

Proposição 1.3.27. *Todo código de Hamming é perfeito.*

Demonstração. Como $d = 3$, temos $\kappa = [\frac{d-1}{2}] = [\frac{3-1}{2}] = 1$. Dado $\mathbf{c} \in \mathbb{F}_2^n$, temos $|D(\mathbf{c}, 1)| = n + 1$. Logo

$$|\bigcup_{\mathbf{c} \in C} D(\mathbf{c}, 1)| = [n + 1]2^k = [2^m - 1 + 1]2^{n-m} = 2^n.$$

Portanto,

$$\bigcup_{\mathbf{c} \in C} D(\mathbf{c}, 1) = \mathbb{F}_2^n$$

e todo código de Hamming é perfeito. □

Capítulo 2

Códigos Poset

2.1 Introdução

O estudo de códigos corretores de erros em espaços poset teve inicio com os trabalhos de Niederreider em [Nie91], Helleseth , T. Klove e O. Ytrehus em [HKY92] e Brualdi, Greaves e Lawrence em [BGL95].

Neste capítulo faremos uma descrição dos espaços com a métrica poset, dando ênfase aos códigos poset. Observaremos como é definido o peso de um elemento a partir de ideais de um conjunto parcialmente ordenado, o que nos dará uma nova métrica para os códigos corretores de erros. Depois, verificaremos que podemos identificar qualquer conjunto finito parcialmente ordenado com uma ordem mais adequada para o estudos de códigos. Finalizamos o capítulo verificando as principais propriedades dessa nova métrica no espaço $\mathbb{F}_q^n$, como por exemplo, que o raio de empacotamento nessa nova métrica é menor do que na métrica usual de Hamming.

As referências para esse capítulo são [BGL95], [Ham50], [HKY92], [Wei91] e [JH98].

2.2 Conjuntos Parcialmente Ordenados

Definição 2.2.1. *Seja X um conjunto não vazio.Uma* ***relação de ordem parcial*** *sobre X é uma relação que satisfaz as seguintes propriedades, para todos $x, y, z \in X$,*

- *xRx (Reflexiva).*
- *Se xRy e yRx, então $x = y$ (Antisimétrica).*
- *Se xRy e yRz, então xRz (Transitiva).*

Definição 2.2.2. *Um* ***conjunto parcialmente ordenado (poset)*** *é um par* $(X, \preceq)$*, onde* X *é um conjunto não vazio, chamado* **base***, e* $\preceq$ *é uma ordem parcial sobre* X*.*

Quando dois elementos $x, y \in X$ se relacionam, ou seja, $x \preceq y$ ou $y \preceq x$, dizemos que os elementos são **comparáveis**, caso contrário são ditos **incomparáveis**.

Exemplo: O conjunto $[n] := \{1, 2, \ldots, n\}$, com a relação divide $|$, $x|y \Leftrightarrow y = x.k, k \in \mathbb{Z}$ forma um poset.

Definição 2.2.3. *Dados* $a, b, c \in X$*, dizemos que* b ***cobre*** a *quando* $a \preceq b$ *e se,* $a \preceq c \preceq b$*, então* $a = c$ *ou* $a = b$*.*

Dado um poset $(X, \preceq)$, quando X for finito a cardinalidade de X será chamada de **comprimento do poset**.

Uma representação gráfica dos posets, quando X é finito, é dado pelo **diagrama de Hasse**. Dado um poset finito $(X, \preceq)$, os elementos do conjunto X são representados no diagrama de Hasse por vértices, e as relações entre os elementos são representados por arestas, convencionando que um elemento $a \in X$ está abaixo de $b \in X$ se, e só se, b cobre a. A transitividade entre dois elementos é um caminho crescente no diagrama entre eles.

Definição 2.2.4. *Seja o poset definido sobre* $[4] = \{1, 2, 3, 4\}$ *e com ordem* $\preceq = \{1 \leq 1, 2 \leq 2, 3 \leq 3, 4 \leq 4, 1 \leq 3, 2 \leq 3, 2 \leq 4\}$*). Este poset será chamado* ***poset*** N *e seu diagrama de Hasse é dado abaixo.*

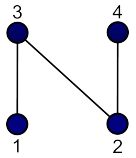

Figura 2.1: Poset N

Definição 2.2.5. *O poset* X*, definido sobre* $[n]$*, com a ordem parcial* $\preceq$ *formado apenas pelas relações reflexivas dos elementos é dito* ***poset anti cadeia*** *ou* ***poset de Hamming*** *e será denotado por* $\mathbb{H}_n$*.*

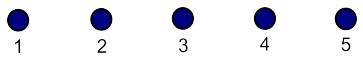

Figura 2.2: Poset $\mathbb{H}_5$

Definição 2.2.6. *Seja $(X, \preceq)$ um poset. Um elemento $x \in X$ é dito* ***elemento maximal*** *se nenhum elemento $y \in X - \{x\}$ cobre x.*

Definição 2.2.7. *Seja $(X, \preceq)$ um poset. Um elemento $x \in X$ é dito* ***elemento minimal*** *se nenhum elemento $y \in X - \{x\}$ é coberto por x.*

Definição 2.2.8. *Seja $(X, \preceq)$ um poset. Um elemento $x \in X$ é dito* ***elemento máximo (mínimo)*** *se $y \preceq x$ ($x \preceq y$), para todo $y \in X$.*

Exemplo:

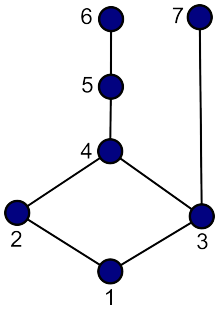

Figura 2.3: Poset sobre [7].

No exemplo acima temos que 1 é elemento mínimo e minimal, $6, 7$ são elementos maximais e não temos elementos máximos no poset.

Denotaremos a ordem de um poset $\mathbb{P} := (X, \preceq)$ por $\preceq_{\mathbb{P}}$. Assim com abuso de notação um elemento $x \in X$ será denotado por $x \in \mathbb{P}$.

Definição 2.2.9. *Seja $n \in \mathbb{N}$. O poset L_n, definido sobre $[n]$, com ordem total $\preceq$ é dito* ***linear*** *ou* ***cadeia*** *e será denotado por L_n. Se $L_4 = (\{1, 2, 3, 4\}, \preceq$ é ordem total) então seu diagrama de Hasse é*

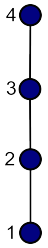

Figura 2.4: Poset L_4

Definição 2.2.10. *O poset* ***Rosenbloom-Tsfasman (RT)*** *é uma união disjunta de posets totalmente ordenados de mesmo comprimento.*

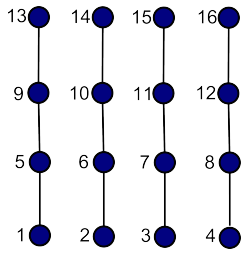

Figura 2.5: Poset Rosenbloom-Tsfasman

2.3 Rotulamentos

Agora mostraremos que podemos representar qualquer conjunto parcialmente ordenado de uma forma organizada, permitindo o estudo simplificado de qualquer poset finito.

Definição 2.3.1. *Seja* $(X, \preceq)$ *um poset com* $\mid X \mid = n$*. Uma função bijetora*

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

onde $V(X)$ *é o conjunto dos vértices do diagrama de Hasse de* $(X, \preceq)$*, é chamada de* **rotulamento** *de* X*. Diremos que* $(X, \preceq, R)$ *é um* ***poset rotulado****.*

Exemplo 2.3.2. $(N = \{a, b, c, d\}, \preceq = \{(a, a), (b, b), (c, c), (d, d), (a, c), (b, c), (b, d)\})$ *pode ser rotulado da seguinte forma:*

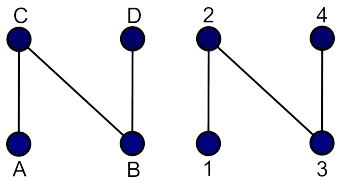

Figura 2.6: Rotulamento do poset N.

Observe que poderíamos ter rotulado N de várias formas. Porém restringiremos aos rotulamentos que preservam a ordem natural dos naturais quando olhamos os elementos através do rotulamento inverso definido por R.

Definição 2.3.3. *Um rotulamento R é dito* ***natural*** *se, quando $x \preceq y$ em V(X), na ordem parcial do poset, tivermos $R^{-1}(x) \leq R^{-1}(y)$, onde $\leq$ é a ordem natural de $\mathbb{N}$.*

Exemplo: $(N = \{a, b, c, d\}, \preceq = \{(a, a); (b, b); (c, c); (d, d); (a, c); (b, c); (b, d)\})$ pode ser rotulado das seguintes formas:

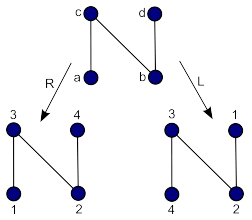

Figura 2.7: Rotulamentos R e L do poset N.

O rotulamento R é natural, pois se $x, y \in N$, com $x \preceq y$, temos $R^{-1}(x) \leq R^{-1}(y)$. Já L não é natural, pois $a \preceq c$, mas $R^{-1}(a) \geq R^{-1}(c)$ na ordem natural de $\mathbb{N}$.

Vamos mostrar agora que podemos rotular naturalmente qualquer poset. Antes enunciaremos um resultado clássico utilizado.

Lema 2.3.4. [*Mon78*] *Se X é um conjunto finito parcialmente ordenado, então X tem elemento minimal.*

Teorema 2.3.5. [*JH98*] *Todo poset finito $(X, \preceq)$ tem um rotulamento natural.*

Demonstração. Seja X um conjunto finito e $\preceq$ uma ordem parcial definida em X. Como X é finito e parcialmente ordenado, então tem pelo menos um elemento minimal. Seja x_1 um elemento minimal de X. Dessa forma, seja $x_1 = R(1)$.

Considere agora $X_1 = X - \{x_1\}$, que é um conjunto parcialmente ordenado com a ordem induzida de X, logo X_1 tem um elemento minimal. Seja x_2 esse elemento. Dessa forma definimos $x_2 = R(2)$. Seguindo esse procedimento, cada subconjunto $X_i \subset X$, para cada $1 \leq i \leq n$, tem um elemento minimal. Tomando x_i como minimal de X_i e pondo $x_i = R(i)$, obtemos uma função bijetora de $V(X)$ em $\mathbb{N}$.

□

Dessa forma podemos rotular qualquer conjunto finito parcialmente ordenado naturalmente. Seguiremos daqui em diante com o rotulamento natural, onde os elementos minimais, no mesmo nível, serão dispostos sempre da esquerda para direta.

2.4 Códigos ponderados por Ordens Parciais

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

Assim, podemos definir um peso ponderado pelo poset $\mathbb{P}$ sobre os elementos de $\mathbb{F}_q^n$ ponderado pela ordem $\preceq_{\mathbb{P}}$. Antes disso, introduziremos alguns conceitos necessários.

Definição 2.4.1. *Definimos por $M(I)$ o conjunto dos elementos maximais de $I \subseteq \mathbb{P}$.*

Definição 2.4.2. *Dado um poset $\mathbb{P} = (X, \preceq)$, um subconjunto $I \subset \mathbb{P}$ é dito um* **ideal** *se I tem a propriedade*

$$x \in I \ , \ y \in \mathbb{P} \text{ e } y \preceq x \text{ então } y \in I.$$

Exemplo 2.4.3. *No poset $\mathbb{H}$, temos que qualquer subconjunto é um ideal, pois temos apenas as relações $x \preceq x$.*

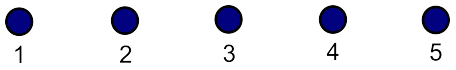

Figura 2.8: Poset $\mathbb{H}_5$.

Exemplo 2.4.4. *No poset N, do exemplo 2.2.4, temos $I_1 = \{1, 2, 3\}, I_2 = \{2, 4\}$ e $I_3 = \{2\}$ ideais de N. No entanto $I_4 = \{2, 3\}$ não é ideal, visto que $1 \preceq 3$, mas $1 \notin I_4$.*

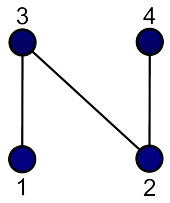

Figura 2.9: Poset N

Definição 2.4.5. *Dado $A \subset \mathbb{P}$, denotamos por $\langle A \rangle_{\mathbb{P}}$ o menor ideal de $\mathbb{P}$ contendo A, chamado de* **ideal de $\mathbf{P}$ gerado por $\mathbf{A}$**. *O conjunto formado por todos os* ***ideais de cardinalidade r*** *de $\mathbb{P}$ será denotado por $\Im^r(\mathbb{P})$.*

Observe que $I \subset \mathbb{P}$ é um ideal se, e somente se, $\langle M(I)\rangle_{\mathbb{P}} = I$.

Definição 2.4.6. *Dados dois poset $\mathbb{P}_1, \mathbb{P}_2$ sobre $[n]$, com $\preceq_1$ a ordem parcial de $\mathbb{P}_1$ e $\preceq_2$ a ordem parcial de $\mathbb{P}_2$, temos $\mathbb{P}_1 \subseteq \mathbb{P}_2$ se, dados x_1, x_2, com $x_1 \preceq_1 x_2$, temos $x_1 \preceq_2 x_2$.*

Para todo poset $\mathbb{P}$ sobre $[n]$, temos o poset $\mathbb{H} \subseteq \mathbb{P}$, visto que $\mathbb{H}$ é formado somente pelas relações reflexivas. Este fato é de grande importância. A seguir uma definição importante.

Definição 2.4.7. *O $\mathbb{P}$-**peso** de um elemento $\mathbf{x} \in \mathbb{F}_q^n$ é a **cardinalidade do ideal de $\mathbb{P}$ gerado pelo suporte de** $\mathbf{x}$, ou seja,*

$$w_P(\mathbf{x}) = \mid \langle supp(\mathbf{x})\rangle_{\mathbb{P}} \mid .$$

Exemplo 2.4.8. *Sejam $\mathbf{x} = \mathbf{0110} \in \mathbb{F}_2^4$, e os poset $\mathbb{H}$ e N sobre $[4]$ como abaixo. Então*

$$w_H(\mathbf{0110}) = \mid \langle supp(\mathbf{0110})\rangle_H \mid = \mid \langle 2,3\rangle_H \mid = \mid \{2,3\} \mid = 2.$$

$$w_N(\mathbf{0110}) = \mid \langle supp(\mathbf{0110})\rangle_N \mid = \mid \langle 2,3\rangle_N \mid = \mid \{1,2,3\} \mid = 3.$$

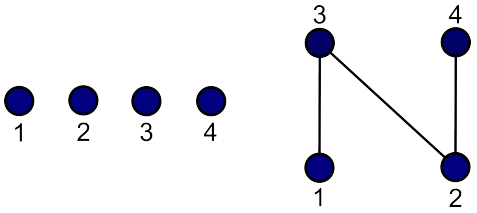

Figura 2.10: Poset $\mathbb{H}_4$ e N.

Observe que $\langle supp\ \mathbf{x}\rangle_{\mathbb{H}} = supp\ \mathbf{x}$, ou seja, quando o poset em questão é o poset de Hamming, o $\mathbb{P}$-peso e o peso de Hamming se equivalem. Isto motivou a chamarmos o poset $\mathbb{H}$ de poset de Hamming.

Em [BGL95], Brualdi, Greves e Lawrence mostraram que a função definida por:

$$d_{\mathbb{P}} : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{N}$$

$$(\mathbf{x}, \mathbf{y}) \mapsto d_{\mathbb{P}}(\mathbf{x}, \mathbf{y}) = w_{\mathbb{P}}(\mathbf{x} - \mathbf{y})$$

é uma métrica em $\mathbb{F}_q^n$.

Teorema 2.4.9. *[BGL95] Se $\mathbb{P} = ([n], \preceq)$ é um poset, então a $\mathbb{P}$-distância é uma métrica em $\mathbb{F}_q^n$.*

Demonstração. Sejam $\mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathbb{F}_q^n$.

Para mostrar a positividade observe a desigualdade $d(\mathbf{u}, \mathbf{v}) \geq 0$, pois por definição é a cardinalidade de um conjunto. Essa é 0 somente quando $u_i = v_i$, para todo i, $1 \leq i \leq n$.

Para mostrar a simetria observe a igualdade

$$supp(\mathbf{u} - \mathbf{v}) = supp(\mathbf{v} - \mathbf{u}).$$

Portanto,

$$d(\mathbf{u}, \mathbf{v}) = d(\mathbf{v}, \mathbf{u}).$$

Para a transitividade basta mostrar que, para todos $\mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathbb{F}_q^n$, temos

$$w_{\mathbb{P}}(\mathbf{u} + \mathbf{v}) \leq w_{\mathbb{P}}(\mathbf{u}) + w_{\mathbb{P}}(\mathbf{v}). \tag{2.1}$$

De fato,

$$d_{\mathbb{P}}(\mathbf{x}, \mathbf{y}) = w_{\mathbb{P}}(\mathbf{x} - \mathbf{y}) \leq w_{\mathbb{P}}(\mathbf{x} - \mathbf{z}) + w_{\mathbb{P}}(\mathbf{y} - \mathbf{z}) = d_{\mathbb{P}}(\mathbf{x}, \mathbf{z}) + d_{\mathbb{P}}(\mathbf{z}, \mathbf{y}).$$

Observamos $supp\ (\mathbf{x} + \mathbf{y}) \subseteq supp\ \mathbf{x} \cup supp\ \mathbf{y}$ e como a união desses ideais é um ideal, segue

$$w_{\mathbb{P}}(\mathbf{x} + \mathbf{y}) \leq | \langle supp\, \mathbf{x} \rangle_{\mathbb{P}} \cup \langle supp\, \mathbf{y} \rangle_{\mathbb{P}} | \leq | \langle supp\, \mathbf{x} \rangle_{\mathbb{P}} | + | \langle supp\, \mathbf{y} \rangle_{\mathbb{P}} | = w_{\mathbb{P}}(\mathbf{x}) + w_{\mathbb{P}}(\mathbf{y}).$$

□

Definição 2.4.10. *O par ordenado $(\mathbb{F}_q^n, d_{\mathbb{P}})$ é chamado um* ***espaço poset****, ou* ***$\mathbb{P}$-espaço****. Um subconjunto do espaço métrico $(\mathbb{F}_q^n, d_{\mathbb{P}})$ é chamado* ***código poset****. Se $C \subset \mathbb{F}_q^n$ é um subespaço vetorial de dimensão k, então C é um $[n, k]_q$* ***$\mathbb{P}$-código linear****.*

Definição 2.4.11. *Sejam $\mathbf{x} \in \mathbb{F}_q^n$ e r um inteiro positivo. A* ***$\mathbb{P}$-bola*** *de centro $\mathbf{x}$ e raio r é o conjunto*

$$B_{\mathbb{P}}(\mathbf{x}, r) = \{\mathbf{y} \in \mathbb{F}_q^n; d_{\mathbb{P}}(\mathbf{x}, \mathbf{y}) \leq r\}.$$

Definição 2.4.12. *Sejam $\mathbf{x} \in \mathbb{F}_q^n$ e r um inteiro positivo. A* ***$\mathbb{P}$-esfera*** *de centro $\mathbf{x}$ e raio r é o conjunto*

$$S_{\mathbb{P}}(\mathbf{x}, r) = \{\mathbf{y} \in \mathbb{F}_q^n; d_{\mathbb{P}}(\mathbf{x}, \mathbf{y}) = r\}.$$

Definição 2.4.13. *O* ***raio de recobrimento*** *de um código $C \subset \mathbb{F}_q^n$ é o menor*

inteiro positivo r tal que

$$\bigcup_{\mathbf{x}\in C} B_P(\mathbf{x}, r) = \mathbb{F}_q^n.$$

Definição 2.4.14. *O **raio de empacotamento** de um código $C \subset \mathbb{F}_q^n$ é o maior inteiro positivo r tal que, dados $\mathbf{x}, \mathbf{y} \in C$,*

$$B_P(\mathbf{x}, r) \bigcap B_P(\mathbf{y}, r) = \emptyset.$$

Denotaremos este por $r = r_{\mathbb{P}}(C)$.

Observando que $\langle supp\ \mathbf{x}\rangle_{\mathbb{H}} = supp\ \mathbf{x} \subseteq \langle supp\ \mathbf{x}\rangle_{\mathbb{P}}$, temos $\omega_{\mathbb{H}}(\mathbf{x}) \leq \omega_{\mathbb{P}}(\mathbf{x})$. Portanto, $B_{\mathbb{P}}(\mathbf{0}, r) \subseteq B_{\mathbb{H}}(\mathbf{0}, r)$. Isso significa que conseguimos aumentar o raio de empacotamento de um código C, ou seja, $r_{\mathbb{H}}(C) \leq r_{\mathbb{P}}(C)$.

Definição 2.4.15. *Seja $\mathbb{P}$ um poset sobre $[n]$. Um código $C \subset \mathbb{F}_q^n$ é chamado **r-corretor de erros $\mathbb{P}$-perfeito** se as $\mathbb{P}$-bolas de raio r são disjuntas e a união das mesmas é todo o espaço $\mathbb{F}_q^n$.*

Exemplo 2.4.16. *Seja L o poset cadeia sobre $[4]$. Seja $C = \{\mathbf{0000}, \mathbf{1111}\} \subset \mathbb{F}_2^4$. Vamos mostrar que C é um código perfeito.*

Primeiramente vamos mostrar que a interseção de duas bolas centradas nas palavras do código são disjuntas. De fato, suponha que exista $\mathbf{x} \in C$ de modo que $\mathbf{x} \in B_L(\mathbf{0000}, 3)$ e $\mathbf{x} \in B_L(\mathbf{1111}, 3)$. Dessa forma se $\mathbf{x} \in B_L(\mathbf{0000}, 3)$ então $d_L(\mathbf{x}, \mathbf{0000}) = w_L(\mathbf{x}) \leq 3$, ou seja $x_4 = 0$ e se $\mathbf{x} \in B_L(\mathbf{1111}, 3)$ então $d_L(\mathbf{x}, \mathbf{1111}) = w_L(\mathbf{x} - \mathbf{1111}) = w_L(y_1y_2y_31) = 4$, ou seja, essa interseção é vazia.

Agora vamos mostrar que a união disjuntas destas bolas formam todo o espaço $\mathbb{F}_q^n$. De fato, se $\mathbf{x} \in B_L(\mathbf{0000}, 3)$, então $x_4 = 0$, ou seja, $\mid B_L(\mathbf{0000}, 3) \mid = 2^3$, pois temos 2 possibilidades para cada umas das 3 coordenadas. E se $\mathbf{y} \in B_L(\mathbf{1111}, 3)$, então $y_4 = 1$, ou seja, $\mid B_L(\mathbf{1111}, 3) \mid = 2^3$, pois temos 2 possibilidades para cada umas das 3 coordenadas. Logo

$$\mid B_L(\mathbf{0000}, 3) \mid + \mid B_L(\mathbf{1111}, 3) \mid = 2^3 + 2^3 = 2^4 = \mid \mathbb{F}_2^4 \mid .$$

Portanto, C é um código 3-corretor de erros L-perfeito, porém na teoria clássica esse código não é perfeito.

Capítulo 3

Peso Generalizado de Hamming

3.1 Introdução

Neste capítulo, descrevemos o trabalho de Wei, em [Wei91], que generaliza o conceito de peso de um elemento para subespaços vetoriais de um código. Este permite definir o peso mínimo de cada subcódigo de um código, gerando assim uma hierarquia de pesos do código C. Wei apresenta também o Teorema da Dualidade que relaciona a hierarquia de pesos de um código C e de seu código dual $C^{\perp}$. A seguir, baseado nos trabalhos de Panek, Bando e Lazarroto, em [LLB08], generalizamos os conceitos apresentados por Wei, como r-ésimo peso mínimo, hierarquia de pesos e Teorema da Monotonicidade, para a métrica poset. Finalizamos o capítulo apresentando os conceitos de multiconjuntos, uma ferramenta necessária para demonstração do Teorema da Dualidade Poset, demonstrado por Moura e Firer em [MF10] e o Teorema da Distribuição de Pesos, demonstrado por Hyun e Kim em [HK08], que permite contar o número de palavras do código ponderado com peso r.

Na Seção 3.1 apresentaremos a generalização de peso de Hamming para subespaços, e na Seção 3.2 apresentaremos a generalização de peso de Hamming para subespaços no caso da métrica poset. Na Seção 3.3 veremos a ferramenta de multiconjuntos e a adiante a demonstração do Teorema da Dualidade Poset. Na Seção 3.4 fazemos uma descrição dos códigos ponderados I-perfeitos e na Seção 3.5 apresentamos o resultado principal deste capítulo, o Teorema da Distribuição de Pesos de um código ponderado.

As principais referências desse capítulo são [BGL95], [HK08], [HKY92], [JH98], [LLB08], [MF10] e [TG95].

Definição 3.1.1. *O **peso generalizado de Hamming** de um subespaço $D \subset \mathbb{F}_q^n$ é a cardinalidade do suporte desse subespaço, isto é,*

$$\omega(D) := \mid supp(D) \mid .$$

Definição 3.1.2. *O* ***r-ésimo peso mínimo generalizado de Hamming*** *de um* $[n,k]_q$ *código* C *é o menor peso dos subespaços de dimensão* r*.*

$$d_r(C) := min\{\omega(D); D \subset C, dimD = r\}.$$

Definição 3.1.3. *A sequência*

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

é chamada ***hierarquia de pesos*** *do código* C*.*

Um primeiro resultado nos mostra que a hierarquia de pesos de C está bem ordenada.

Teorema 3.1.4. [*Wei91, Teorema* 1] *[Monotonicidade] Para um* $[n,k]_q$ *código* C*, com* $k > 0$*, a hierarquia de pesos é uma sequência crescente, ou seja,*

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

E temos um limitante para cada hierarquia de peso.

Proposição 3.1.5. [*Wei91, Corolário* 1] *Seja* C *um* $[n,k]_q$ *código, então, para* $r \in \{1,2,\ldots,k\}$ *e* $t \in \{0,1,\ldots,k-r\}$*,* $d_r(C) + t \leq d_{r+t}(C)$*.*

Teorema 3.1.6. [*Wei91, Corolário* 2]*[Limitante de Singleton] Seja* C *um* $[n,k]_q$*, então*

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

Um resultado, demonstrado por Wei, em [Wei91], nos diz como a hierarquia de um código se comporta em relação a hierarquia de seu dual.

Teorema 3.1.7. [*Wei91, Teorema* 3]*[Teorema da Dualidade de Wei] Sejam* C *um* $[n,k]_q$ *código e* $C^{\perp}$ *seu dual. Então*

$$\{d_r(C), 1 \leq r \leq k\} = \{1,2,\ldots,n\}/\{n+1-d_r(C^{\perp}), 1 \leq r \leq n-k\}.$$

ou seja, se

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

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

então

$$X \cup Y = [n] = \{1,2,\ldots,n\} \text{ e } X \cap Y = \emptyset.$$

Proposição 3.1.8. [*Wei91*] *Sejam $\mathbb{P}$ um poset sobre $[n]$ e $C \subset \mathbb{F}_q^n$ um $\mathbb{P}$-código. Então*

$$| C | \leq q^{n-d_{\mathbb{P}}(C)+1}.$$

Definição 3.1.9. *A $\mathbb{P}$-**distância de** C, denotada por $d_{\mathbb{P}}(C)$, é o menor dos $\mathbb{P}$-pesos das palavras de C, ou seja,*

$$d_{\mathbb{P}}(C) = min\{w_{\mathbb{P}}(\mathbf{x}); \mathbf{x} \in C\}.$$

Corolário 3.1.10. [*Wei91*] *Seja C um $[n,k]_q$ $\mathbb{P}$-código, então,*

$$d_{\mathbb{P}}(C) \leq n - k + 1.$$

Definição 3.1.11. *Seja $\mathbb{P}$ um poset sobre $[n]$. Um $\mathbb{P}$-código $C \subset \mathbb{F}_q^n$ é dito um **MDS** se, e somente se, $d_{\mathbb{P}}(C) = n - k + 1$.*

Definição 3.1.12. *Dado um poset $\mathbb{P}$ sobre $[n]$. O **poset oposto**, denotado por $\widetilde{\mathbb{P}}$, é definido, também sobre $[n]$, com a ordem $\preceq_{\widetilde{\mathbb{P}}}$ definida por,*

$$x \preceq_{\mathbb{P}} y \text{ se, e somente se, } y \preceq_{\widetilde{\mathbb{P}}} x.$$

Exemplo 3.1.13. *Dado $\mathbb{P}$ o poset sobre* [7],

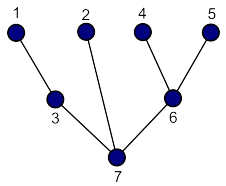

Figura 3.1: Poset $\mathbb{P}$ sobre o conjunto [7].

O poset oposto $\widetilde{\mathbb{P}}$ é dado por

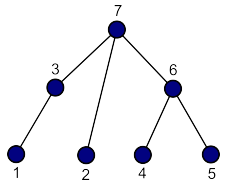

Figura 3.2: Poset oposto de $\mathbb{P}$ sobre [7].

3.2 $\mathbb{P}$-peso generalizado de Hamming

Uma pergunta para o espaço poset era se o Teorema da Dualidade de Wei, [Wei91], se aplicava aos códigos poset. Numa primeira tentativa via-se que se

$$X = \{d_1^{\mathbb{P}}(C), d_2^{\mathbb{P}}(C), \ldots, d_k^{\mathbb{P}}(C)\} \text{ e}$$
$$Y = \{n+1-d_1^{\mathbb{P}}(C^{\perp}), d_2^{\mathbb{P}}(C^{\perp}), \ldots, d_{n-k}^{\mathbb{P}}(C^{\perp})\},$$

então esse conjuntos não estavam relacionados, como em [Wei91].

Em [MF10], Moura e Firer demonstraram que a seguinte relação de dualidade acontecia. Se

$$X = \{d_1^{\mathbb{P}}(C), d_2^{\mathbb{P}}(C), \ldots, d_k^{\mathbb{P}}(C)\} \text{ e}$$
$$Y = \{n+1-d_1^{\widetilde{\mathbb{P}}}(C^{\perp}), d_2^{\widetilde{\mathbb{P}}}(C^{\perp}), \ldots, d_{n-k}^{\widetilde{\mathbb{P}}}(C^{\perp})\},$$

então

$$X \cup Y = [n] \text{ e } X \cap Y = \emptyset.$$

Nessa seção vamos apresentar alguns resultados para a demonstração do Teorema da Dualidade de Wei generalizado, feito em [MF10]. Verificaremos que C é um $\mathbb{P}$-código é $\mathbb{P}$-MDS se, e somente se, $\widetilde{\mathbb{P}}$-código é $\widetilde{\mathbb{P}}$-MDS, demonstrado por Hyun e Kim em [HK08].

Definição 3.2.1. *O* ***$\mathbb{P}$-peso generalizado de Hamming*** *de um subespaço $D \subset \mathbb{F}_q^n$ é a cardinalidade do suporte desses subespaço, ou seja,*

$$\omega_{\mathbb{P}}(D) := \mid \langle supp(D) \rangle_{\mathbb{P}} \mid .$$

Definição 3.2.2. *O* ***r-ésimo $\mathbb{P}$-peso mínimo generalizado de Hamming*** *de um $[n,k]_q$ $\mathbb{P}$-código C é o menor $\mathbb{P}$-peso dos subespaços de dimensão r, ou seja,*

$$d_r^{\mathbb{P}}(C) := min\{\omega_{\mathbb{P}}\ D : D \subset C, dim D = r\}.$$

Chamaremos $d_r^{\mathbb{P}}(C)$ somente como r-ésimo $\mathbb{P}$-peso mínimo como abuso de escrita.

Definição 3.2.3. *A sequência*

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

é chamada ***$\mathbb{P}$-hierarquia de pesos*** *do código C.*

Teorema 3.2.4. [*LLB08*] *[Monotonicidade Poset] Para um $[n,k]_q$ $\mathbb{P}$-código C, a hierarquia de pesos é uma sequência crescente, ou seja,*

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

Demonstração. Dado D um subespaço de C de dimensão r, ele contém subespaços de dimensão $r-1$. De fato, fazendo

$$I_i := \{\mathbf{x} \in D : x_i = 0 \text{ para } i \in supp\ D\},$$

temos que I_i tem dimensão $r-1$.

Seja $D \subset C$ um subcódigo de dimensão r, com $1 \leq r \leq k$, tal que $d_r^{\mathbb{P}}(C) = \omega(D)$. Considerando $i \in M(\langle supp\ D\rangle_{\mathbb{P}})$, seja $D_i := \{\mathbf{x} \in D : x_i = 0\}$. Temos $dim\ D = r$ e os elementos de D_i tem uma entrada nula no suporte de D, logo $dim\ D_i = r-1$. Como o $r-1$-ésimo $\mathbb{P}$-peso mínimo é o menor dos $\mathbb{P}$-pesos dos subespaços de C, segue

$$d_{r-1}^{\mathbb{P}}(C) \leq |\ \langle supp\ D_i\rangle_{\mathbb{P}}\ | \leq |\ \langle supp\ D\rangle_{\mathbb{P}}\ | - 1 = d_r^{\mathbb{P}}(C) - 1.$$

□

Corolário 3.2.5. *[LLB08] Seja C um $[n,k]_q$ $\mathbb{P}$-código. Então, para cada $r \in \{1,2,\ldots,k\}$ e para cada $t \in \{0,1,\ldots,k-r\}$, temos*

$$d_r(C) + t \leq d_{r+t}(C).$$

Demonstração. Faremos a demonstração por processo de indução sobre t.

Fixando r, mostraremos a desigualdade $d_r(C) + t \leq d_{r+t}(C)$. De fato, se $t = 1$ o resultado segue pelo Teorema da Monotonicidade Poset.

Suponha $d_r(C) + t \leq d_{r+t}(C)$, para $t \in \{0,1,\ldots,k-r-1\}$. Assim

$$d_r(C) + t + 1 \leq d_{r+t}(C) + 1.$$

Agora

$$d_{r+t}(C) + 1 \leq d_{r+t+1}(C).$$

Portanto,

$$d_r(C) + t + 1 \leq d_{r+t+1}(C).$$

□

3.3 Multiconjuntos

Nessa seção faremos uma breve descrição dos multiconjuntos e suas aplicações ao Teorema da Dualidade Poset, demonstrado por Moura e Firer. Uma referência para essa seção é [MF10].

Definição 3.3.1. *Um **multiconjunto** sobre um conjunto S é uma coleção de elementos de S não necessariamente distintos.*

Definição 3.3.2. *Para cada multiconjunto, podemos definir a aplicação*

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

*onde $m(\mathbf{s})$, com $\mathbf{s} \in S$, é o número de ocorrências de $\mathbf{s}$ em S. $m(\mathbf{s})$ será chamada a **multiplicidade** de um elemento $\mathbf{s} \in S$.*

Exemplo: Seja $C = \langle \mathbf{1001}, \mathbf{0110} \rangle$ um $[4, 2]_2$ código. Uma matriz geradora de C é

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

Um multiconjunto sobre $\{\textit{colunas de } G\}$ é $m_G = \{\mathbf{10}, \mathbf{01}, \mathbf{01}, \mathbf{10}\}$.
A multiplicidade $m_G : \mathbb{F}_2^2 \to \mathbb{N}$ é:

$$m_G(\mathbf{s}) = \begin{cases} 2, & s = 10 \\ 1, & s = 11 \textit{ ou } 01 \\ 0, & s = 00 \end{cases}$$

Definição 3.3.3. *Um $\mathbb{P}$-código C é dito **degenerado** se existe uma matriz geradora com uma coluna nula, caso contrário é **não degenerado**.*

Sejam C um $[n, k]_q$-código, G e G' duas matrizes geradoras de C. Como as linhas de G e G' são linearmente independentes, existe uma matriz T de ordem k de posto completo tal que

$$G = T \cdot G'.$$

Podemos definir o automorfismo de C.

$$\phi(\mathbf{v}) = T \cdot \mathbf{v}, \tag{3.1}$$

que substitui uma coluna $\mathbf{g_i}$ por $\mathbf{g'_i}$. Portanto, $m_G = m_{G'}$, ou seja, os multiconjuntos de C independem da matriz geradora escolhida.

Definição 3.3.4. *Dado C um $[n, k]_q$-código o multiconjunto $m_C := m_G$ é chamado **multiconjunto induzido pelo código** C.*

Definição 3.3.5. *$m_C(\mathbf{x})$ é o número de ocorrências do elemento $\mathbf{x}$ em m_C.*

Definição 3.3.6. *Para um subconjunto $U \subset \mathbb{F}_q^k$ definimos a* ***multiplicidade de U*** *por*

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

Definição 3.3.7. *Dado um conjunto D, denotaremos por $\wp(D)$* ***o conjunto das partes*** *de D.*

Definição 3.3.8. *O multiconjunto induzido pelo $\mathbb{P}$-código C não degenerado é o* ***multiconjunto*** *sobre $\wp(\mathbb{F}_q^k)$.*

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

onde $U_i = \langle\{\mathbf{g_j};\ j \leq_{\mathbb{P}} i\}\rangle_{\mathbb{P}}$.

Observe que o isomorfismo ϕ, definido na equação (3.1), garante que $m_C^{\mathbb{P}}$ independe da escolha da matriz geradora de C.

Teorema 3.3.9. *[HKY92] Sejam $C \subset \mathbb{F}_q^n$ um $\mathbb{P}$-código de dimensão $k \leq n$ e $\omega_{\mathbb{P}}$ o $\mathbb{P}$-peso de C. Dado um subespaço $D \subset C$ de dimensão r, existe um subespaço $U \subset \mathbb{F}_q^k$ tal que a dimensão do espaço quociente de $\mathbb{F}_q^k$ por U é r e*

$$m_C^{\mathbb{P}}(U) = n - \omega_{\widetilde{\mathbb{P}}}(D),$$

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

Demonstração. Seja G uma matriz geradora de C, com vetores coluna $\{\mathbf{g_1}, \mathbf{g_2}, \ldots, \mathbf{g_n}\}$ e considere ψ, definido por

$$\psi : \mathbb{F}_q^k \to C$$
$$\mathbf{v} \mapsto \psi(\mathbf{v}) = \mathbf{v}.G$$

Temos C e $\mathbb{F}_q^k$ são isomorfos, pois ψ é um isomorfismo e dim $C = k$.

Dado $D \subset C$, existe $V \subset \mathbb{F}_q^k$ tal que $\psi(V) = D$. Observe que $i \in supp(D)$ se, e somente se, existe $\mathbf{v} \in V$ tal que a i-ésima coordenada de $\mathbf{v}.G$ é não nula. Logo $i \in supp(D)$ se, e somente se, $\mathbf{g_i} \notin V^{\perp}$. Portanto,

$$\begin{aligned}
\omega_{\widetilde{\mathbb{P}}}(D) &= |\ \{i : \exists j \ com\ i \preceq j, \mathbf{g_j} \notin V^{\perp}\}\ | \\
&= n - |\ \{i : j \preceq i \Rightarrow \mathbf{g_j} \in V^{\perp}\}\ | \\
&= n - |\ \{i : [\{\mathbf{g_j} : j \preceq i\}] \subseteq V^{\perp}\}\ | \\
&= n - |\ \{i : U_i \subseteq V^{\perp}\}\ | \\
&= n - m_C^{\mathbb{P}}(V^{\perp}).
\end{aligned}$$

□

3.3.1 Levantamento

Dado C um $[n,k]_q$ código linear e $\{\mathbf{g_1}, \mathbf{g_2}, \ldots, \mathbf{g_n}\}$ o conjunto das colunas de uma matriz geradora G de C. Considere

$$\begin{array}{rccc} \mu_C: & \mathbb{F}_q^n & \to & \mathbb{F}_q^n/C^\perp \\ & \mathbf{x} & \mapsto & \mathbf{x}+C^\perp \end{array}$$

o epimorfismo canônico e a transformação linear

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

Pelo Teorema do Homomorfismo de Módulos, existe um isomorfismo τ

$$\tau : \mathbb{F}_q^n/C^\perp \to \mathbb{F}_q^k.$$

Sejam $\mathbf{x}+C^\perp \in \mathbb{F}_q^n/C^\perp$ e $\mathbf{c} \in C$. Definimos

$$(\mathbf{x}+C^\perp).\mathbf{c} = \mathbf{x}.\mathbf{c},$$

onde $\mathbf{x}.\mathbf{c}$ é o produto canônico dos vetores $\mathbf{x}$ e $\mathbf{c}$. Para $\mathbf{x} = \mathbf{e_i}$ e $\mathbf{c} = \mathbf{v}.G$, temos

$$\mu_C(\mathbf{e_i}).\mathbf{c} = (\mathbf{e_i}+C^\perp) = \mathbf{e_i}.\mathbf{c} = c_i = \mathbf{g_i}.\mathbf{v}.$$

Desta maneira associamos o vetor $\mathbf{e_i}$ com a coluna $\mathbf{g_i}$ e identificamos $\mathbb{F}_q^k$ e C através de μ_C.

Definição 3.3.10. *Dado um código C, definimos o* ***conjunto de cobertura ortogonal de*** *$\mathbb{F}_q^n/C^\perp$ como a coleção ordenada*

$$B_{\mathbb{P}} := \{V_1, V_2, \ldots, V_n\},$$

onde $V_i = \langle\{\mathbf{g_j};\ j \leq_{\mathbb{P}} i\}\rangle_{\mathbb{P}}$.

Assim

$$m_C^{\tilde{\mathbb{P}}} = \mu_C(B_{\mathbb{P}}) := \{\mu_C(V_1), \mu_C(V_2), \ldots, \mu_C(V_n)\}.$$

Desta forma, para cada elemento de $\wp(\mathbb{F}_q^n/C^\perp)$, existe um único elemento de $\wp(\mathbb{F}_q^k)$. Como dim $\mathbb{F}_q^n/C^\perp$ = dim $\mathbb{F}_q^k$, esta correspondência é biunívoca.

Definição 3.3.11. *Seja C um $[n,k]_q$ $\mathbb{P}$-código, seu* ***multiconjunto associado*** *é o multiconjunto $m_C^{\tilde{\mathbb{P}}} := \mu_C^{\tilde{\mathbb{P}}}(B_{\tilde{\mathbb{P}}})$ definido sobre $\wp(\mathbb{F}_q^n/C^\perp)$.*

3.3.2 Submulticonjuntos

Definição 3.3.12. *Um* ***submulticonjunto*** $B' \subseteq B$*, sobre um mesmo conjunto* S*, é um multiconjunto tal que* $B'(s) \leq B(s)$*, para todo* $s \in S$*.*

Definição 3.3.13. *Denotaremos por* $[B]$ *o subespaço gerado pelos elementos de* B*.*

Lema 3.3.14. [*MF10, Lema* 3.13] *Sejam* C *um* $\mathbb{P}$*-código e* $m_C^{\widetilde{\mathbb{P}}}$ *seu multiconjunto associado. Se* $J \subseteq [n]$ *e* $B_J := \{V_j : j \in J\}$*, com* $V_j = [\{\mathbf{e_i} : i \in \langle j \rangle_{\widetilde{\mathbb{P}}}\}]$*, então* $m_J := \mu_C(B_J)$ *é um submulticonjunto de* $m_C^{\widetilde{\mathbb{P}}}$*.*

Proposição 3.3.15. [*MF10, Proposição* 3.15] *Sejam* C *um* $[n,k]_q$ $\mathbb{P}$*-código e* $D \subseteq C$ *um subcódigo de dimensão* r*. Então existe um ideal* J *de* $\widetilde{\mathbb{P}}$ *tal que a dimensão do espaço quociente de* $[\mu_C(B_J)]$ *por* $\mathbb{F}_q^k$ *é* r *e*

$$\omega_{\widetilde{\mathbb{P}}}(D) = n - \mid J \mid = n - \mid B_J \mid . \tag{3.2}$$

A partir dessa proposição temos que analisar as propriedades de B_J relacionadas com o ideal J.

Proposição 3.3.16. [*MF10*] *A igualdade* $[B_J] = [\{\mathbf{e_i} : i \in \langle J \rangle_{\widetilde{\mathbb{P}}}\}]$ *acontece para qualquer submulticonjunto* $J \subseteq [n]$*.*

Demonstração. Dado $j \in \langle J \rangle_{\widetilde{\mathbb{P}}}$, o vetor $\mathbf{e_j} \in V_j = [\{\mathbf{e_i} : i \in \langle j \rangle_{\widetilde{\mathbb{P}}}\}]$, logo $\mathbf{e_j} \in [B_J]$ e portanto,

$$[\{\mathbf{e_j} : j \in \langle J \rangle_{\widetilde{\mathbb{P}}}\}] \subseteq [B_J].$$

□

Proposição 3.3.17. [*MF10*] *A desigualdade* $dim\,[B_J] \geq \mid B_J \mid$ *sempre acontece e a igualdade acontece se, e somente se,* J *é um ideal de* $\widetilde{\mathbb{P}}$*.*

Demonstração. De fato,

$$dim[B_J] = dim[\{\mathbf{e_j} : j \in \langle J \rangle_{\widetilde{\mathbb{P}}}\}] = \mid \langle J \rangle_{\widetilde{\mathbb{P}}} \mid \geq \mid J \mid = \mid B_J \mid .$$

A igualdade decorre de J ser um ideal de $\widetilde{\mathbb{P}}$ se, e somente se, $\langle J \rangle_{\widetilde{\mathbb{P}}} = J$.
□

Lema 3.3.18. [*MF10*] *Sejam* C *um* $[n,k]_q$ $\mathbb{P}$*-código e* m_C *o multiconjunto associado sobre* $\wp(\mathbb{F}_q^n/C^\perp)$ *associado a* C*. Então*

$$d_r^{\mathbb{P}}(C^\perp) = min\{\mid J \mid : \mid J \mid - dim[\mu_C(B_J)] \geq r\}. \tag{3.3}$$

Demonstração. Para $D \subset C^{\perp}$, de modo que $\omega_{\widetilde{\mathbb{P}}}(D) = d_r^{\widetilde{\mathbb{P}}}(C^{\perp})$, considere o ideal $I = \langle supp\ D \rangle_{\widetilde{\mathbb{P}}}$. Pela Proposição 3.3.16, temos $B_I = \{\mathbf{e_i}; i \in I\}$, $\mid B_I \mid = \mid I \mid$ e $D = [B_I] \cap C^{\perp}$. Como

$$D = [\{\mathbf{e_i} : i \in supp\ D\}] \cap C^{\perp} \subseteq [\{\mathbf{e_i} : i \in \langle supp\ D \rangle_{\widetilde{\mathbb{P}}}\}] \cap C^{\perp} = [B_I] \cap C^{\perp},$$

para todo $D \subseteq C$, então D está contido no núcleo de $\widehat{\mu_C}$, a restrição de μ_C a $\langle B_I \rangle$. Assim

$$dim[B_I] - dim[\mu_C(B_I)] = dim\ ker\ \widehat{\mu_C} \geq dim\ D.$$

Como I é um ideal, então $dim[B_I] = \mid B_I \mid = \omega_{\widetilde{\mathbb{P}}}(D)$. Logo $\omega_{\widetilde{\mathbb{P}}}(D)$ é um elemento do conjunto $d_r^{\mathbb{P}}(C^{\perp})$ e , consequentemente,

$$d_r^{\mathbb{P}}(C^{\perp}) \geq min\{\mid J \mid : \mid J \mid - dim[\mu_C(B_J)] \geq r\}.$$

Para mostrar a outra desigualdade, seja J um ideal de $\widetilde{\mathbb{P}}$ que atinge o mínimo de $\{\mid J \mid : \mid J \mid - dim[\mu_C(B_J)] \geq r\}$. Então

$$\mid B_J \mid - dim[\mu_C(B_J)] \geq r.$$

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

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

Como $\langle supp\ D' \rangle_{\widetilde{\mathbb{P}}} \subseteq J$, então $dim[B_J] \geq \omega_{\widetilde{\mathbb{P}}}(D')$. De J ser um ideal, pela Proposição 3.3.17, temos $dim[B_J] = \mid B_J \mid$, donde

$$\mid B_J \mid \geq \omega_{\widetilde{\mathbb{P}}}(D')$$

e

$$dim\ D' = \mid B_J \mid - dim[\mu_C(B_J)] = r' \geq r.$$

Pelo Teorema da Monotonicidade Poset temos

$$d_r^{\widetilde{\mathbb{P}}}(C^{\perp}) \leq d_{r'}^{\widetilde{\mathbb{P}}}(C^{\perp}).$$

Portanto,

$$d_r^{\mathbb{P}}(C^{\perp}) \geq min\{\mid J \mid : \mid J \mid - dim[\mu_C(B_J)] \geq r\}.$$

□

Exemplo: Sejam C um $[4,2]_2$ $\mathbb{P}$-código, com matriz geradora

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

$\mathbb{P}$ um poset sobre $[4]$ e $\widetilde{\mathbb{P}}$ seu poset dual, dados por

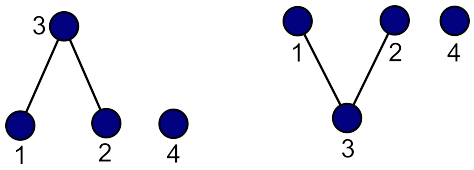

Figura 3.3: Poset sobre [4].

Uma matriz geradora para o $\widetilde{\mathbb{P}}$-código $C^{\perp}$ é

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

Dessa forma

$$\mu_C(\mathbf{1000}) = \mathbf{1000} + C^{\perp} \longleftrightarrow \mathbf{10}$$
$$\mu_C(\mathbf{0100}) = \mathbf{0100} + C^{\perp} \longleftrightarrow \mathbf{11}$$
$$\mu_C(\mathbf{0010}) = \mathbf{0010} + C^{\perp} \longleftrightarrow \mathbf{10}$$
$$\mu_C(\mathbf{0001}) = \mathbf{0001} + C^{\perp} \longleftrightarrow \mathbf{01}.$$

Logo

$$V_1 = [\{\mathbf{e_1}, \mathbf{e_3}\}],\ V_2 = [\{\mathbf{e_2}, \mathbf{e_3}\}],$$
$$V_3 = [\{\mathbf{e_3}\}],\ V_4 = [\{\mathbf{e_4}\}].$$

Portanto, o multiconjunto associado é $m_C^{\widetilde{\mathbb{P}}} = \{\mu_C(V_1), \mu_C(V_2), \mu_C(V_3), \mu_C(V_4)\}$ com hierarquia de $\mathbb{P}$-pesos

$$\begin{aligned} d_1(C) &= \omega_{\mathbb{P}}([\mathbf{0101}] \\ &= \omega_{\mathbb{P}}([\mathbf{01}].G) \\ &= 4 - m_C([\mathbf{01}]^{\perp}) \\ &= 4 - m_C([\mathbf{10}]) = 2 \end{aligned}$$

$$\begin{aligned} d_2(C) &= \omega_{I\!P}(C) \\ &= \omega_{I\!P}(I\!F_2^2.G) \\ &= 4 - m_C((I\!F_2^2)^\perp) \\ &= 4 - m_C([\mathbf{00}]) = 4 \end{aligned}$$

Em [MF10], Moura e Firer demonstram a relação entre as hierarquias de um $I\!P$-código C e seu dual.

Teorema 3.3.19. *[MF10][Teorema da Dualidade Poset] Sejam C um $[n,k]_q$ $I\!P$-código e $C^\perp$ seu dual. Então*

$$\{d_r^{I\!P}(C), 1 \leq r \leq k\} = \{1,2,\ldots,n\} - \{n+1-d_r^{\widetilde{I\!P}}(C^\perp), 1 \leq r \leq n-k\},$$

ou seja, se

$$X := \{d_1^{I\!P}(C), d_2^{I\!P}(C), \ldots, d_k^{I\!P}(C)\} \text{ e}$$

$$Y := \{n+1-d_1^{\widetilde{I\!P}}(C^\perp), n+1-d_2^{\widetilde{I\!P}}(C^\perp), \ldots, n+1-d_{n-k}^{\widetilde{I\!P}}(C^\perp)\},$$

então

$$X \cup Y = [n] = \{1,2,\ldots,n\} \text{ e } X \cap Y = \emptyset.$$

Demonstração. Como

$$X, Y \subset [n], \mid X \mid = k \text{ e } \mid Y \mid = n-k,$$

temos $\mid X \mid + \mid Y \mid = n$. Assim é suficiente mostrarmos a igualdade $X \cap Y = \emptyset$.

Dado $r \in \{1,2,\ldots,k\}$, pelo Lema 3.3.18, existe $J \subset [n]$ tal que

$$\mid B_J \mid = d_r^{\widetilde{I\!P}}(C^\perp) \tag{3.4}$$

e

$$dim[\mu_C(B_J)] \leq d_r^{\widetilde{I\!P}}(C^\perp) - r.$$

Seja t a dimensão do espaço quociente de $I\!F_q^n$ por $[\mu_C(B_J)]$. Dessa forma

$$t \geq k - d_r^{\widetilde{I\!P}}(C^\perp) + r. \tag{3.5}$$

Pela Proposição 3.3.15, existe um subcódigo $D \subseteq C$ com $\psi([\mu_C(B_J)]) = D$ tal que $dim\ D = t$ e

$$\omega_{I\!P}(D) = n - \mid B_J \mid .$$

Utilizando a Equação (3.4) obtemos

$$\omega_{I\!P}(D) = n - d_r^{\widetilde{I\!P}}(C^\perp).$$

Pela definição de r-ésimo $I\!P$-peso mínimo generalizado, temos

$$d_t(C) \leq \omega(E), \text{ para todo } E \subset C \text{ com } dim\ E = t.$$

Em particular, a desigualdade vale para o subespaço D. Segue

$$d_t^{I\!P}(C) \leq n - d_r^{\widetilde{I\!P}}(C^\perp). \tag{3.6}$$

Agora mostraremos que $n + 1 - d_r^{\widetilde{I\!P}}(C^\perp)$ não está na hierarquia X. Suponha o contrário, então a Equação (3.6) restringe as possibilidades a

$$d_{t+l}(C) = n + 1 - d_r^{\widetilde{I\!P}}(C^\perp), \tag{3.7}$$

para algum inteiro $l > 0$. A Proposição 3.3.15 garante a existência de $I \subset [n]$ tal que $\langle \mu_C(B_I) \rangle = U \subset I\!F_q^k$ e a dimensão do quociente de $I\!F_q^n$ por U é $t + l$, onde

$$m_C^{\widetilde{I\!P}}(U) = \mid B_I \mid = n - d_{t+l}^{I\!P}(C) \tag{3.8}$$

e

$$dim[\mu_C(B_I)] = k - (t + l). \tag{3.9}$$

Utilizando a Equação (3.7) na Equação (3.8), teríamos

$$\mid B_I \mid = d_r^{\widetilde{I\!P}}(C^\perp) - 1, \tag{3.10}$$

e usando o valor de t da Inequação (3.5) na Equação (3.9) obteríamos

$$dim[\mu_C(B_I)] \leq d_r^{\widetilde{I\!P}}(C^\perp) - r - l. \tag{3.11}$$

Isto implicaria que a diferença da Equação (3.10) com a Equação (3.11) seria

$$\mid B_I \mid - dim[\mu_C(B_I)] \geq r + l - 1 > r. \tag{3.12}$$

Pelo Teorema 3.3.18, teríamos $\mid B_I \mid \geq d_r^{\widetilde{I\!P}}(C^\perp)$, contradizendo a Equação (3.10). □

3.4 $\mathbb{P}$-Códigos I-Perfeitos

Nessa seção descreveremos o Teorema da Distribuição de $\mathbb{P}$-pesos de C, mostrado em [HK08] por Hyun e Kim. Como referências para esta seção temos [MF10], [LLB08], [PFKH08] e [HK08].

Verificamos agora que é possível construir ideais encaixados de $\mathbb{P}$ a partir de ideais de cardinalidade r. Lembrando que $\Im^r(\mathbb{P})$ denota os ideiais de $\mathbb{P}$ de cardinalidade r.

Proposição 3.4.1. [*HK08*]

(a) Sejam $0 \leq r \leq s \leq n$ e $I \in \Im^r(\mathbb{P})$, então existe $J \in \Im^s(\mathbb{P})$ tal que $I \subseteq J$.
(b) Sejam $0 \leq s \leq r \leq n$ e $I \in \Im^r(\mathbb{P})$, então existe $J \in \Im^s(\mathbb{P})$ tal que $J \subseteq I$

Demonstração. (a) Se $s = r + 1$, seja $j \in I^C = \mathbb{P} - I$ um elemento minimal.

$Afirmação: J = I \cup \{j\}$ é $\mathbb{P}$-ideal.

De fato, dados $x \in \mathbb{P}$ e $y \in J$, com $x \leq y$, se $y \in I$, então $x \in I$ pois I é $\mathbb{P}$-ideal. Se $y = j$, como $x \leq y$, então $x \notin I^C$, pois j é minimal de I^C, logo $x \in I$. Assim $I \subset J$ e $\mid J \mid = r + 1$.

Desta forma, podemos construir um ideal J de $\mathbb{P}$ tal que $I \subseteq J$ e $\mid J \mid = s$, para $r \leq s \leq n$, adicionando a cada passo um elemento minimal do conjunto $\mathbb{P} - I$.

(b) Se $s = r - 1$, seja $j \in I$ um elemento maximal. Note que $J = I - \{j\}$ é $\mathbb{P}$-ideal, pois I é ideal e removemos um elemento maximal de I. Portanto, $J \subset I$ e $\mid J \mid = r - 1$.

Desta forma, podemos construir um ideal J de $\mathbb{P}$ tal que $J \subseteq I$ e $\mid J \mid = s$, para $0 \leq s \leq r$, removendo a cada passo um elemento maximal do conjunto I.□

Definição 3.4.2. *Sejam $\mathbb{P}$ um poset, $I \subset \mathbb{P}$ um $\mathbb{P}$-ideal e $u \in \mathbb{F}_q^n$.*

Chamaremos o conjunto

$$B_I(\mathbf{u}) = \{\mathbf{v} \in \mathbb{F}_q^n; \langle supp(\mathbf{u} - \mathbf{v})\rangle_{\mathbb{P}} \subseteq I\}$$

*de I-**bola** de centro em $\boldsymbol{u}$ e*

$$S_I(\mathbf{u}) = \{\mathbf{v} \in \mathbb{F}_q^n; \langle supp(\mathbf{u} - \mathbf{v})\rangle_{\mathbb{P}} = I\}$$

*a I-**esfera** de centro em $\boldsymbol{u}$.*

Denotemos por B_I e S_I, respectivamente, a I-bola e I-esfera centradas em $\mathbf{0}$.

Proposição 3.4.3. [*HK08*] *Sejam $\mathbb{P}$ um poset sobre $[n]$ e I um $\mathbb{P}$-ideal não vazio. Então*

(a) B_I é um subespaço vetorial de $\mathbb{F}_q^n$ de dimensão $\mid I \mid$.
(b) Para $\mathbf{u} \in \mathbb{F}_q^n$ temos $B_I(\mathbf{u}) = \mathbf{u} + B_I$.
(c) Para $\mathbf{u}, \mathbf{v} \in \mathbb{F}_q^n$ temos $B_I(\mathbf{u}) = B_I(\mathbf{v})$ se e só se $supp(\mathbf{u} - \mathbf{v}) \subseteq I$.
(d) $\mathbb{F}_q^n$ é particionado pelas I-bolas, para todo ideal I.

Demonstração. (a) Sejam $\mathbf{u}, \mathbf{v} \in B_I$ e $c \in \mathbb{F}_q$. Vamos mostrar que $\mathbf{u} + \mathbf{v} \in B_I$ e $c.\mathbf{v} \in B_I$. Como $supp(\mathbf{u} + \mathbf{v}) \subseteq supp(\mathbf{u}) \cup supp(\mathbf{v}) \subseteq I \cup I = I$, temos $\mathbf{u} + \mathbf{v} \in B_I$. Agora $supp(c.\mathbf{v}) \subseteq supp(\mathbf{v}) \subseteq I$, logo $c.\mathbf{v} \in B_I$.

Denote por $\mathbf{e_i}$ o elemento da base canônica de $\mathbb{F}_q^n$ cuja i-ésima coordenada tem valor 1 e as demais são nulas. O conjunto $\{\mathbf{e_i}\}_{i \in I}$ forma uma base de B_I. Portanto, $\mid I \mid$ é a dimensão de B_I.

(b) Se $\mathbf{v} \in B_I(\mathbf{u})$, então por definição $supp(\mathbf{u} - \mathbf{v}) \in I$. Como

$$supp(\mathbf{u} - \mathbf{v}) = supp(\mathbf{0} - (\mathbf{v} - \mathbf{u})),$$

temos

$$\mathbf{v} - \mathbf{u} \in B_I.$$

Assim

$$\mathbf{v} = \mathbf{u} + (\mathbf{v} - \mathbf{u}) \in \mathbf{u} + B_I,$$

ou seja,

$$B_I(\mathbf{u}) \subseteq \mathbf{u} + B_I.$$

Reciprocamente, se $\mathbf{w} \in B_I$, então $supp(\mathbf{w}) \subseteq I$. Como

$$supp(\mathbf{w}) = supp(-\mathbf{w}) = supp(\mathbf{u} - (\mathbf{u} + \mathbf{w})) \subset I,$$

temos $\mathbf{u} + \mathbf{w} \in B_I(\mathbf{u})$. Logo $-\mathbf{w} \in B_I(\mathbf{u})$ e $\mathbf{w} \in B_I(\mathbf{u})$. Portanto, $\mathbf{u} + B_I \subseteq B_I(\mathbf{u})$.

(c) Decorre das equivalências

$$B_I(\mathbf{u}) = B_I(\mathbf{v}) \Leftrightarrow \mathbf{u} + B_I = \mathbf{v} + B_I \Leftrightarrow \mathbf{u} - \mathbf{v} \in B_I \Leftrightarrow supp(\mathbf{u} - \mathbf{v}) \subseteq I.$$

(d) Temos que B_I é subespaço de $\mathbb{F}_q^n$ e

$$\mathbb{F}_q^n = \bigcup_{\mathbf{u} \in \mathbb{F}_q^n} B_I(\mathbf{u}).$$

Pelo item (c) essa união é disjunta e portanto, $\mathbb{F}_q^n$ é particionado pelas I-bolas.□

Definição 3.4.4. *Denotaremos por*

$$\overset{\circ}{\bigcup_{\mathbf{x}\in C}} B_I(\mathbf{x})$$

a união disjunta de I-bolas centradas em $\mathbf{x}$.

Definição 3.4.5. *Sejam $\mathbb{P}$ um poset sobre $[n]$ e I um $\mathbb{P}$-ideal. Um $\mathbb{P}$-código linear sobre $\mathbb{F}_q^n$ é dito* ***I-perfeito*** *se a união disjunta das I-bolas centradas nas palavras do código formam todo o espaço $\mathbb{F}_q^n$, ou seja, se*

$$\mathbb{F}_q^n = \overset{\circ}{\bigcup_{\mathbf{x}\in C}} B_I(\mathbf{x}).$$

Proposição 3.4.6. [*HK08*] *Sejam $\mathbb{P}$ um poset sobre $[n]$, I um $\mathbb{P}$-ideal e C um $[n,k]_q$ $\mathbb{P}$-código. Se C é I-perfeito, então $\mid I \mid = n-k$.*

Demonstração. Se C é I-perfeito, então

$$\mid \mathbb{F}_q^n \mid = \mid \overset{\circ}{\bigcup_{\mathbf{x}\in C}} B_I(\mathbf{x}) \mid \Rightarrow\ q^n = \mid C \mid .q^{|I|} = q^k.q^{|I|} \ \Rightarrow\ \mid I \mid = n-k.$$

□

Proposição 3.4.7. [*HK08*] *Sejam $\mathbb{P}$ um poset sobre $[n]$ e $\mathbf{u},\mathbf{v} \in \mathbb{F}_q^n$, então $\mathbf{u}$ e $\mathbf{v}$ estão na mesma I-bola de um $\mathbb{P}$-ideal I, com $\mid I \mid = s$ se, e somente se, $d_{\mathbb{P}}(\mathbf{u},\mathbf{v}) \leq s$.*

Demonstração. Sejam I um $\mathbb{P}$-ideal de $\mathbb{P}$, com $\mid I \mid = s$, e $\mathbf{u},\mathbf{v} \in B_I$. Temos $\mathbf{u}-\mathbf{v} \in B_I$, pois B_I é um subespaço de $\mathbb{F}_q^n$. Assim

$$\langle supp(\mathbf{u}-\mathbf{v})\rangle_{\mathbb{P}} \subseteq I \Rightarrow d_{\mathbb{P}}(\mathbf{u},\mathbf{v}) = \mid \langle supp(\mathbf{u}-\mathbf{v})\rangle_{\mathbb{P}} \mid \leq \mid I \mid = s.$$

Reciprocamente, $d_{\mathbb{P}}(\mathbf{u},\mathbf{v}) \leq s$ se, e somente se, $\mid \langle supp(\mathbf{u}-\mathbf{v})\rangle_{\mathbb{P}} \mid \leq s$. Agora $\langle supp(\mathbf{u}-\mathbf{v})\rangle_{\mathbb{P}}$ é o menor ideal de $\mathbb{P}$ contendo $supp(\mathbf{u}-\mathbf{v})$, assim, pela Proposição 3.4.1, existe $J \subset \mathbb{P}$ $\mathbb{P}$-ideal tal que $\mid J \mid = s$ e $\langle supp(\mathbf{u}-\mathbf{v})\rangle_{\mathbb{P}} \subset J$. Portanto, $\mathbf{v} \in B_J(\mathbf{u})$.

□

Definição 3.4.8. *Um $\mathbb{P}$-código C é dito* ***$\mathbb{P}$-MDS*** *se, e somente se,*

$$d_{\mathbb{P}}(C) = n-k+1.$$

Diremos apenas que C é um $\mathbb{P}$-código MDS quando não confundirmos a métrica usual nesta seção.

Teorema 3.4.9. [*HK08*] *Seja $\mathbb{P}$ um poset sobre $[n]$ e C um $[n,k]_q$ $\mathbb{P}$-código. Então C é $\mathbb{P}$-MDS se, e somente se, ele for I-perfeito para todo $I \in \Im^{n-k}(\mathbb{P})$.*

Demonstração. Se C é $\mathbb{P}$-código MDS, então $d_{\mathbb{P}}(C) = n-k+1$. Se $I \in \Im^{n-k}(\mathbb{P})$, então, pela Proposição 3.4.3, $\mathbb{F}_q^n$ é particionado pelas I-bolas e o número de I-bolas na partição é $q^{n-|I|} = q^k =\mid C \mid$.

Se $\mathbf{x}, \mathbf{y} \in C$, então, pela Proposição 3.4.7, temos

$$\mid I \mid = n-k < n-k+1 \leq d_{\mathbb{P}}(\mathbf{x}, \mathbf{y}).$$

Assim $B_I(\mathbf{x}) \cap B_I(\mathbf{y}) = \emptyset$. Logo

$$\mathbb{F}_q^n = \overset{\circ}{\bigcup_{\mathbf{x} \in C}} B_I(\mathbf{x}).$$

Reciprocamente, seja C um $\mathbb{P}$-código I-perfeito, para todo $I \in \Im^{n-k}(\mathbb{P})$. Suponha, por absurdo, que existam $\mathbf{x}, \mathbf{y} \in C$ com $d_{\mathbb{P}}(\mathbf{x}, \mathbf{y}) \leq n-k$. Pela Proposição 3.4.1, que existe J ideal de $\mathbb{P}$ tal que $\mid J \mid = n-k$ e $\langle supp(\mathbf{x}-\mathbf{y}) \rangle_{\mathbb{P}} \subset J$. Assim $\mathbf{y} \in B_I(\mathbf{x})$, o que é um absurdo, pois C é perfeito. Logo $d_{\mathbb{P}}(C) > n-k$ e, pelo Limitante de Singleton, temos $d_{\mathbb{P}}(C) \leq n-k+1$. Portanto, $d_{\mathbb{P}}(C) = n-k+1$, ou seja, C é MDS.

□

3.5 $\mathbb{P}$-Distribuição de Pesos e $\mathbb{P}$-códigos MDS

Demonstraremos agora o resultado principal deste capítulo, o Teorema da Distribuição de $\mathbb{P}$-pesos, demonstrado por Hyun e Kim em [HK08]. As principais referências para esta seção são [MF10], [HK08], [BGL95].

Definição 3.5.1. *Sejam $\mathbb{P}$ um poset sobre $[n]$ e C um $\mathbb{P}$-código sobre $\mathbb{F}_q^n$. Chamaremos de* ***$\mathbb{P}$-distribuição de pesos de*** *C o conjunto $\{A_{0,\mathbb{P}}, A_{1,\mathbb{P}}, \ldots, A_{n,\mathbb{P}}\}$, onde*

$$A_{r,\mathbb{P}}(C) :=\mid \{\mathbf{x} \in C; \omega_{\mathbb{P}}(\mathbf{x}) = r\} \mid .$$

Note que $A_{r,\mathbb{P}}(C) =\mid S_{r,\mathbb{P}} \cap C \mid$.

Agora vamos verificar que as palavras código estão uniformemente distribuídas nas I-bolas.

Proposição 3.5.2. *[HK08] Seja $\mathbb{P}$ um poset sobre $[n]$ e C um $[n,k]_q$ $\mathbb{P}$-código. Se C é MDS, então, para um ideal $I \subseteq \mathbb{P}$ e $\mathbf{u} \in \mathbb{F}_q^n$, temos*

$$\mid B_I(\mathbf{u}) \cap C \mid = \begin{cases} q^{|I|-n+k}, & se \quad \mid I \mid \geq n-k; \\ 1, & se \quad \mid I \mid < n-k; \\ 0, & se \quad \mathbf{u} \notin C \ e \ \mid I \mid < n-k. \end{cases}$$

Demonstração. Seja $I \subset \mathbb{P}$ um ideal de cardinalidade s. Vamos fazer a demonstração em 3 partes.

Se $s < n-k$, então pela Proposição 3.4.7 a I-bola centrada na origem contém apenas uma palavra código, a palavra nula, pois caso contrário, existiria $\mathbf{y} \in C$, com

$$d_{\mathbb{P}}(\mathbf{0}, \mathbf{y}) \leq n-k < d_{\mathbb{P}}(C) = n-k+1.$$

Se $s = n-k$, então o Teorema 3.4.9 nos garante que C é perfeito, logo cada I-bola contém apenas uma palavra código de C.

Se $s > n-k$, então pela Proposição 3.4.1 existe um ideal $J \subset \mathbb{P}$ tal que $\mid J \mid = n-k$ e B_J e B_I são subespaços vetoriais de $\mathbb{F}_q^n$, com $B_J \subset B_I$ e B_J é um subespaço vetorial de B_I de dimensão $\mid I \mid - \mid J \mid$. Logo $B_I(\mathbf{u})$ contém exatamente $q^{|I|-|J|}$ classes laterais de B_J para $\mathbf{u} \in \mathbb{F}_q^n$, já que, $\mathbf{u} + B_J = B_J$ se $\mathbf{u} \in B_J$. Como C é MDS, pelo Teorema 3.4.9 C é J-perfeito. Assim cada B_J contém exatamente uma palavra código de C e portanto, $B_I(\mathbf{u})$ contém exatamente

$$q^{|I|-|J|} = q^{|I|-n+k}$$

palavras de C.

□

Introduziremos algumas notações que utilizaremos daqui em diante.

Definição 3.5.3. *Seja $I \subset \mathbb{P}$ um ideal de um poset $\mathbb{P}$. Denotaremos por $M(I)$* ***o conjunto dos elementos maximais de I*** *e $I_M := I - M(I)$.*

O conjunto I_M é um ideal de $\mathbb{P}$, pela Proposição 3.4.1.

Definição 3.5.4. *Definimos $\Upsilon(I) := \{J : I_M \subseteq J \subseteq I\}$.*

Como os elementos de $\Upsilon(I)$ são ideais de $\mathbb{P}$, podem ser construídos a partir de I_M adicionando, a cada passo, um elemento $x \in M(I)$ ou removendo um elemento maximal de I.

Apresentaremos agora alguns resultados clássicos da Teoria de Caracteres Aditivos para Códigos, estes, que utilizaremos para demonstrar o Teorema da Distribuição de

$\mathbb{P}$-pesos de C. As principais referências são [Nie91] e [Sta72].

Definição 3.5.5. *Seja $\chi(E|\cdot) : \mathbb{F}_q^n \to \mathbb{N}$. A **função característica** de $E \subset \mathbb{F}_q^n$, é definida da seguinte forma; a imagem de um elemento $\mathbf{x} \in \mathbb{F}_q^n$ vale 1, se $\mathbf{x} \in E$, e 0, caso contrário.*

Definição 3.5.6. *Dados um subconjunto $A \subset \mathbb{P}$ e $u \in \mathbb{F}_q^n$, definimos os conjuntos*

$$B_A^{\vee}(\mathbf{u}) := \{\mathbf{v} \in \mathbb{F}_q^n;\ supp\ (\mathbf{u} - \mathbf{v}) \subseteq A\}\ e$$

$$S_A^{\vee}(\mathbf{u}) := \{\mathbf{v} \in \mathbb{F}_q^n;\ supp\ (\mathbf{u} - \mathbf{v}) = A\}.$$

No caso em que o subconjunto A é um ideal ordem de $\mathbb{P}$, temos a igualdade dos dois conjuntos $B_A^{\vee}(\mathbf{u})$ e $B_A(\mathbf{u})$.

Definição 3.5.7. *Um **caracter aditivo** λ de $\mathbb{F}_q$ é um homomorfismo entre $(\mathbb{F}_q, +)$ e $(S_1, \cdot)$, o grupo dos números complexos com norma 1.*

Vamos citar alguns resultados clássicos da teoria de caracteres aditivos para códigos lineares que utilizaremos nesse trabalho.

Proposição 3.5.8. [*Sta72, Teorema* 1.3] *Seja λ um caracter aditivo de $\mathbb{F}_q$ e $\mathbf{x} \in \mathbb{F}_q^n$. Então*

$$\sum_{\beta \in \mathbb{F}_q} \lambda(\mathbf{x}.\beta) = \begin{cases} q, & se\ \mathbf{x} = 0, \\ 0, & se\ \mathbf{x} \neq 0, \end{cases}$$

onde $\mathbf{x}.\beta = \sum_{i=1}^{n} x_i\beta_i$, para $x_i, \beta_i \in \mathbb{F}_q$.

Proposição 3.5.9. [*Sta72, Teorema* 1.4] *Seja λ um caracter aditivo de $\mathbb{F}_q$. Então, para um código linear $C \subset \mathbb{F}_q^n$, temos*

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

onde $C^{\perp}$ é o complemento ortogonal de C.

Definição 3.5.10. *Seja f uma função complexa definida em $\mathbb{F}_q^n$. A **transformada de Fourier** $\hat{f}$ de f é dada por*

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

A proposição abaixo decorre da Proposição 3.5.9.

Proposição 3.5.11. [*Sta72, Teorema* 1.5] *[Fórmula do Somatório de Poison] Sejam $C \subset \mathbb{F}_q^n$ um código linear e f uma função em $\mathbb{F}_q^n$. Então*

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

Observando que a relação de inclusão natural é uma relação de ordem sobre o conjuntos das partes de $\mathbb{P}$ e que os ideais principais de $\mathbb{P}$ são finitos, podemos utilizar o seguinte resultado para funções definidas em $A \subset \mathbb{P}$.

Proposição 3.5.12. [*Sta72, Teorema* 1.6]*[Inversão de Moebius]*
Sejam f, g duas funções complexas definidas em um subconjunto $A \subset \mathbb{P}$. Então

$$f(A) = \sum_{B\subseteq A} g(B) \;\Leftrightarrow\; g(A) = \sum_{B\subseteq A} (-1)^{|A|-|B|} f(B).$$

Proposição 3.5.13. [*HK08*] *Seja $I \subset \mathbb{P}$ um ideal. Então*

$$(a)\ \chi(S_A^{\vee}|\mathbf{x}) = \sum_{E\subseteq A} (-1)^{|A|-|E|} \chi(B_E^{\vee}|\mathbf{x}).$$

$$(b)\ \chi(S_I|\mathbf{x}) = \sum_{J\in\Upsilon(I)} (-1)^{|I|-|J|} \chi(B_J^{\vee}|\mathbf{x}).$$

Demonstração. (a) Se $\chi(B_A^{\vee}|\mathbf{x}) = 1$, então $\mathbf{x} \in B_A^{\vee}$. Dessa forma, $supp\ \mathbf{x} \subseteq A$.

Logo

$$\chi(S_{supp\ \mathbf{x}}^{\vee}|\mathbf{x}) = 1$$

e

$$\chi(S_D^{\vee}|\mathbf{x}) = 0,\ \textit{se}\ D \neq supp\ \mathbf{x}.$$

Em outras palavras,

$$\chi(B_A^{\vee}|\mathbf{x}) = \sum_{E\subseteq A} \chi(S_E^{\vee}|\mathbf{x}). \tag{3.13}$$

Aplicando a Proposição 3.5.12 na Equação (3.13), obtemos

$$\chi(S_A^{\vee}|\mathbf{x}) = \sum_{E\subseteq A} (-1)^{|A|-|E|} \chi(B_E^{\vee}|\mathbf{x}).$$

(b) Observamos

$$\chi(S_I|\mathbf{x}) = 1 \text{ se, e somente se, } \langle supp\ \mathbf{x}\rangle = I \text{ e}$$

$$\langle supp\ \mathbf{x}\rangle = I \text{ se, e somente se, } M(I) \subseteq supp\ \mathbf{x} \subseteq I.$$

Dessa observação e das considerações feitas em (a), temos

$$\chi(S_I|\mathbf{x}) = \sum_{M(I)\subseteq A\subseteq I} \chi(S_A^{\vee}|\mathbf{x}). \tag{3.14}$$

Pelas propriedades de somatório, temos

$$\sum_{M(I)\subseteq A\subseteq I} \chi(S_A^{\vee}|\mathbf{x}) = \sum_{M(I)\subseteq A\subseteq I} \sum_{E\subseteq A} (-1)^{|A|-|E|}\chi(B_E^{\vee}|\mathbf{x}) \tag{3.15}$$

e

$$\sum_{M(I)\subseteq A\subseteq I} \sum_{E\subseteq A} (-1)^{|A|-|E|}\chi(B_E^{\vee}|\mathbf{x}) = \sum_{E\subseteq I} \sum_{M(I)\cup E\subseteq A\subseteq I} (-1)^{|A|}(-1)^{-|E|}\chi(B_E^{\vee}|\mathbf{x}). \tag{3.16}$$

Como

$$\sum_{E\subseteq I} \sum_{M(I)\cup E\subseteq A\subseteq I} (-1)^{|A|}(-1)^{-|E|}\chi(B_E^{\vee}|\mathbf{x}) = \sum_{E\subseteq I} (-1)^{-|E|}\chi(B_E^{\vee}|\mathbf{x}) \sum_{M(I)\cup E\subseteq A\subseteq I} (-1)^{|A|},$$

temos

$$\chi(S_I|\mathbf{x}) = \sum_{E\subseteq I} (-1)^{-|E|}\chi(B_E^{\vee}|\mathbf{x}) \sum_{M(I)\cup E\subseteq A\subseteq I} (-1)^{|A|}. \tag{3.17}$$

Agora temos

$$\sum_{M(I)\cup E\subseteq A\subseteq I} (-1)^{|A|} = \begin{cases} (-1)^{|I|}, & \text{se } M(I)\cup E = I, \\ 0, & \text{caso contrário,} \end{cases}$$

pois, utilizando argumentos de contagem de subconjuntos, o número de parcelas no somatório para $M(I)\cup E \neq I$ é $2^{|I|} - 2^{|M(I)\cup E|}$, ou seja, um número par.

Temos também

$$M(I)\cup E = I \Leftrightarrow I_M \subseteq E \subseteq I \Leftrightarrow E \in \Upsilon(I).$$

Além disso, cada ideal de $\Upsilon(I)$ é construído adicionando um elemento minimal ao conjunto $M(I)$, ou seja, o sinal de $1^{|A|}$ alterna no somatório. Logo $\sum 1^{|A|} = 0$.

$$\chi(S_I|\mathbf{x}) = \sum_{E\subseteq I}(-1)^{-|E|}\chi(B_E^{\vee}|\mathbf{x}) \sum_{M(I)\cup E\subseteq A\subseteq I}(-1)^{|A|}.$$

Portanto,

$$= \sum_{E\in\Upsilon(I)}(-1)^{|I|-|E|}\chi(B_E^{\vee}|\mathbf{x}).$$

□

3.5.1 Teorema da $\mathbb{P}$-Distribuição de Pesos

Teorema 3.5.14. *[HK08] Seja $\mathbb{P}$ um poset sobre $[n]$ e C um $\mathbb{P}$-código de dimensão k com $d_{\mathbb{P}}(C)$ sua $\mathbb{P}$-distância mínima. Se C é um $\mathbb{P}$-código MDS, então*

$$A_{r,\mathbb{P}}(C) = \begin{cases} 1, & \text{se } r = 0, \\ 0, & \text{se } 1 \leq r \leq d_{\mathbb{P}} - 1, \\ (q-1)\displaystyle\sum_{I\in\Im^r(\mathbb{P})}\sum_{j=0}^{r-d_{\mathbb{P}}}(-1)^j\binom{\mid M(I)\mid -1}{j}q^{r-d_{\mathbb{P}}-j}, & \text{se } r \geq d_{\mathbb{P}} \end{cases}$$

Demonstração. Faremos esta demonstração em 3 partes da seguinte forma.

Se $r = 0$, então $A_{r,\mathbb{P}}(C) = 0$, pois $\mathbf{0}$ é a única palavra de peso nulo.

Se $r \leq d_{\mathbb{P}} - 1$, então $A_{r,\mathbb{P}}(C) = 0$, pois $d_{\mathbb{P}}(C) \leq \omega_{\mathbb{P}}(\mathbf{x})$, para todo $\mathbf{x} \in \mathbb{F}_q^n$.

Se $r \geq d_{\mathbb{P}}$, temos

$$A_{r,\mathbb{P}}(C) = \sum_{I\in\Im^r(\mathbb{P})} \mid S_I \cap C \mid .$$

Agora vamos contar o número de elementos de $\mid S_I \cap C \mid$, para cada $I \in \Im^r(\mathbb{P})$. Por definição

$$\mid S_I \cap C \mid = \sum_{\mathbf{x}\in C}\chi(S_I|\mathbf{x}).$$

Pela Proposição 3.5.13 temos

$$\sum_{\mathbf{x}\in C}\chi(S_I|\mathbf{x}) = \sum_{\mathbf{x}\in C}\sum_{J\in\Upsilon(I)}(-1)^{|I|-|J|}\chi(B_J|\mathbf{x}). \tag{3.18}$$

Agora

$$\sum_{\mathbf{x}\in C}\sum_{J\in\Upsilon(I)}(-1)^{|I|-|J|}\chi(B_J|\mathbf{x}) = \sum_{J\in\Upsilon(I)}(-1)^{|I|-|J|} \mid B_J \cap C \mid . \tag{3.19}$$

Primeiramente, temos

$$\mid I \mid = \mid I_M \mid + \mid M(I) \mid .$$

Agora os ideais $J \in \Upsilon(I)$ são construídos adicionando algum elemento maximal de I, ou seja,

$$\mid J \mid = \mid I_M \mid + h, \text{com } 0 \leq h \leq \mid M(I) \mid .$$

Porém há varias formas de adicionarmos esses elementos maximais em $\Upsilon(I)$ e o número formas é dado por

$$\binom{\mid M(I) \mid}{h},$$

onde h é o número de maximais adicionados a cada passo. Logo, da Equação (3.19), temos

$$\mid S_I \cap C \mid = \sum_{h=0}^{|M(I)|} (-1)^{|M(I)|+h} \binom{\mid M(I) \mid}{h} \mid B_I \cap C \mid . \tag{3.20}$$

Observe no somatório acima a igualdade

$$(-1)^{|M(I)|+h} = (-1)^{|M(I)|-h}.$$

Agora, da Proposição 3.5.2, temos

$$\mid B_J \cap C \mid = \begin{cases} 1, & \mid J \mid \leq n-k \\ q^{|J|-d_{\mathbb{P}}+1}, & \mid J \mid \geq n-k+1. \end{cases}$$

Substituindo a Equação (3.20) em $\mid B_J \cap C \mid$, obtemos

$$\begin{aligned} \mid S_I \cap C \mid \;\; &= \sum_{h=0}^{n-k-|I_M|} (-1)^{|M(I)|+h} \binom{\mid M(I) \mid}{h} \\ &+ \sum_{h=n-k-|I_M|+1}^{|M(I)|} (-1)^{|M(I)|+h} \binom{\mid M(I) \mid}{h} q^{|I_M|+h-n+k.} \end{aligned}$$

Observando as relações dos coeficientes binomiais, temos $\sum_{h=0}^{n} (-1)^l \binom{n}{h} = 0$ e, dessa forma,

$$\sum_{h=0}^{n-k-|I_M|} (-1)^{|M(I)|+h} \binom{\mid M(I) \mid}{h} = - \sum_{h=n-k-|I_M|+1}^{|M(I)|} (-1)^{|M(I)|+h} \binom{\mid M(I) \mid}{h}.$$

Logo

$$\mid S_I \cap C \mid = \sum_{l=d_{\mathbb{P}}-|I_M|}^{|M(I)|} (-1)^{|M(I)|+h} \binom{\mid M(I) \mid}{h} (q^{|I_M|+h-d_{\mathbb{P}}+1} - 1).$$

Substituindo $r = h - d_{\mathbb{P}} + \mid I_M \mid$, temos

$$\mid S_I \cap C \mid = \sum_{r=0}^{|I|-d_{\mathbb{P}}} (-1)^{|I|+r+d_{\mathbb{P}}} \binom{\mid M(I) \mid}{r + d_{\mathbb{P}} - \mid I_M \mid} (q^{r+l} - 1).$$

Realizando a mudança $j = \mid I \mid -d_{\mathbb{P}} - r$, segue

$$\begin{aligned} \mid S_I \cap C \mid &= \sum_{r=0}^{|I|-d_{\mathbb{P}}} (-1)^j \binom{\mid M(I) \mid}{j} (q^{|I|-d_{\mathbb{P}}+1-j} - 1) \\ &= \sum_{j=0}^{|I|-d_{\mathbb{P}}} (-1)^j \left(\binom{\mid M(I) \mid -1}{j} + \binom{\mid M(I) \mid -1}{j-1} \right) (q^{|I|-d_{\mathbb{P}}+1-j} - 1) \\ &= (q-1) \sum_{j=0}^{|I|-d_{\mathbb{P}}} (-1)^j \binom{\mid M(I) \mid -1}{j} q^{|I|-d_{\mathbb{P}}-j}. \end{aligned}$$

Portanto, somando agora todos os ideais de cardinalidade r, obtemos

$$\mid S_I \cap C \mid = (q-1) \sum_{I \in \Im^r(\mathbb{P})} \sum_{j=0}^{r-d_{\mathbb{P}}} (-1)^j \binom{\mid M(I) \mid -1}{j} q^{r-d_{\mathbb{P}}-j}.$$

□

Lema 3.5.15. [*HK08*] *Seja $I \subseteq \mathbb{P}$ um ideal. Para $\mathbf{u}, \mathbf{v} \in \mathbb{F}_q^n$, temos*

$$\hat{\chi}(B_{I,\mathbb{P}}(\mathbf{v})|\mathbf{u}) = \lambda(\mathbf{u}.\mathbf{v}) q^{|I|} \chi(B_{I^C,\widetilde{\mathbb{P}}}|\mathbf{u}).$$

Em particular

$$\hat{\chi}(B_{I,\mathbb{P}}|\mathbf{u}) = q^{|I|} \chi(B_{I^C,\widetilde{\mathbb{P}}}|\mathbf{u}).$$

Demonstração. Considere $\chi(B_{I,\mathbb{P}}(\mathbf{v})|\mathbf{u})$ a função característica em $B_{I,\mathbb{P}}(\mathbf{v})$. Sua transformada de Fourier é dada por

$$\begin{aligned}\hat{\chi}(B_{I,\mathbb{P}}(\mathbf{v})|\mathbf{u}) &= \sum_{\mathbf{w}\in\mathbb{F}_q^n} \lambda(\mathbf{u}.\mathbf{w})\chi(B_{I,\mathbb{P}}(\mathbf{v})|\mathbf{w}) \\ &= \sum_{\mathbf{w}\in B_{I,\mathbb{P}}(\mathbf{v})} \lambda(\mathbf{u}.\mathbf{w}) = \sum_{\mathbf{w}\in B_{I,\mathbb{P}}} \lambda(\mathbf{u}.(\mathbf{v}+\mathbf{w})) \\ &= \lambda(\mathbf{u}.\mathbf{w}) = \sum_{\mathbf{w}\in B_{I,\mathbb{P}}} \lambda(\mathbf{u}.\mathbf{w}).\end{aligned}$$

Como $B_{I,\mathbb{P}}$ é subespaço vetorial, então, pela Proposição 3.5.9, temos

$$\sum_{\mathbf{w}\in B_{I,\mathbb{P}}} \lambda(\mathbf{u}.\mathbf{w}) = \begin{cases} q^{|I|}, & se\ \mathbf{u}\in B_{I,\mathbb{P}}^{\perp} \\ 0, & se\ \mathbf{u}\notin B_{I,\mathbb{P}}^{\perp}. \end{cases}$$

Sendo assim, basta verificarmos a propriedade quando $\mathbf{u}\in B_{I,\mathbb{P}}^{\perp}$. Logo

$$\hat{\chi}(B_{I,\mathbb{P}}(\mathbf{v})|\mathbf{u}) = \lambda(\mathbf{u}.\mathbf{v})q^{|I|}\chi(B_{I,\mathbb{P}}^{\perp}|\mathbf{u}).$$

Afirmação: $B_{I,\mathbb{P}}^{\perp} = B_{I^C,\widetilde{\mathbb{P}}}$

Demonstração. Seja $\mathbf{x}\in B_{I^C,\widetilde{\mathbb{P}}}$ e suponha, por absurdo, que exista $\mathbf{y}\in B_{I,\mathbb{P}}$ tal que $\mathbf{x}.\mathbf{y} = \sum_{i=1}^n x_i.y_i \neq 0$. Assim para algum $i\in[n]$, temos $x_i.y_i\neq 0$, daí $x_i, y_i\neq 0$, ou seja, $i\in supp\ \mathbf{x}\subseteq I$ e $i\in supp\ \mathbf{y}\subseteq I^C$, o que é um absurdo, pois $I\cap I^C=\emptyset$. Logo se, $\mathbf{x}\in B_{I^C,\widetilde{\mathbb{P}}}$ e $\mathbf{y}\in B_{I,\mathbb{P}}$, então $\mathbf{x}.\mathbf{y} = \sum_{i=1}^n x_i.y_i = 0$, ou seja,

$$B_{I^C,\widetilde{\mathbb{P}}}\subseteq B_{I,\mathbb{P}}^{\perp}.$$

Agora, pela Proposição 3.4.3, temos

$$dim\ B_{I^C,\widetilde{\mathbb{P}}} = \mid I^C \mid = n - \mid I \mid = dim\ B_{I,\mathbb{P}}^{\perp}.$$

Logo $B_{I^C,\widetilde{\mathbb{P}}} = B_{I,\mathbb{P}}^{\perp}$.

Consequentemente

$$\hat{\chi}(B_{I,\mathbb{P}}(\mathbf{v})|\mathbf{u}) = \lambda(\mathbf{u}.\mathbf{v})q^{|I|}\chi(B_{I^C,\widetilde{\mathbb{P}}}|\mathbf{u}).$$

Note que $\lambda(\mathbf{u}.\mathbf{0}) = \lambda(\mathbf{0}) = 1$, pois λ é caracter aditivo. Portanto,

$$\hat{\chi}(B_{I,\mathbb{P}}|\mathbf{u}) = q^{|I|}\chi(B_{I^C,\widetilde{\mathbb{P}}}|\mathbf{u}).$$

□

Agora vamos provar uma equivalência que nos dará um limitante para $d_{\widetilde{\mathbb{P}}}(C^\perp)$ em função da ordem de um ideal ordem $I \subseteq \mathbb{P}$. Esse limitante foi a primeira variação observada em relação a $d_1^{\widetilde{\mathbb{P}}}(C^\perp)$ que motivou a definição apresentada no capítulo seguinte.

Teorema 3.5.16. *[HK08] Sejam $\mathbb{P}$ um poset sobre $[n]$ e C um $[n,k]_q$ $\mathbb{P}$-código e $C^\perp$ seu código dual. Para cada inteiro $0 \leq \delta \leq k$ as afirmações abaixo são equivalentes:*

(a) Para cada ideal $I \subset \mathbb{P}$, de cardinalidade $n-k+\delta$, cada I-bola centrada na origem contém exatamente q^δ palavras de C.

(b) $d_{\widetilde{\mathbb{P}}}(C^\perp) \geq k - \delta + 1$.

Demonstração. $(a) \Rightarrow (b)$ Seja $I \subset \mathbb{P}$ um $\mathbb{P}$-ideal com $\mid I \mid = n-k+\delta$. Aplicando a Fórmula do Somatório de Poison, 3.5.8, na função $\chi(B_{I^C,\widetilde{\mathbb{P}}}|\mathbf{u})$ e pelo Lema 3.5.15 temos

$$\begin{aligned} \mid C^\perp \cap B_{I^C,\widetilde{\mathbb{P}}} \mid &= \sum_{\mathbf{u}\in C^\perp} \chi(B_{I^C,\widetilde{\mathbb{P}}}|\mathbf{u}) \\ &= \tfrac{1}{|C|}\sum_{\mathbf{u}\in C} \hat{\chi}(B_{I^C,\widetilde{\mathbb{P}}}|\mathbf{u}) \\ &= \tfrac{1}{|C|}\sum_{\mathbf{u}\in C} q^{|I^C|}\hat{\chi}(B_{I,\mathbb{P}}|\mathbf{u}) \\ &= q^{-\gamma} \mid C \cap B_{I,\mathbb{P}} \mid = 1. \end{aligned}$$

Suponha agora, por absurdo, que exista $\mathbf{y} \in C^\perp$ não nulo tal que

$$d_{\widetilde{\mathbb{P}}}(\mathbf{0},\mathbf{y}) \leq k - \gamma.$$

Pela Proposição 3.4.1, existe um ideal J^C com $supp\ \mathbf{y} \subseteq J^C$ e $\mid J^C \mid = k-\gamma$. Como $supp\ \mathbf{y} = supp\ \mathbf{y} - \mathbf{0}$, pela definição da J-bola $\mathbf{y}, \mathbf{0} \in B_J^C$, o que é um absurdo, pois $\mid C^\perp \cap B_{I^C,\widetilde{\mathbb{P}}} \mid = 1$. Portanto,

$$d_{\widetilde{\mathbb{P}}}(C^\perp) \geq k - \gamma + 1.$$

$(b) \Rightarrow (a)$ Se $d_{\widetilde{\mathbb{P}}}(C^\perp) \geq k - \gamma + 1$, então

$$\mid C^\perp \cap B_{I^C,\widetilde{\mathbb{P}}} \mid = 0, \ se \ \mid I \mid = n - k + \gamma$$

e

$$\mid C \cap B_I(\mathbf{x}) \mid = \sum_{\mathbf{z} \in C} \chi(B_I(\mathbf{x})|\mathbf{z}).$$

Utilizando a fórmula do somatório de Poison temos

$$\begin{aligned} \mid C \cap B_I(\mathbf{x}) \mid &= \sum_{\mathbf{z} \in C} \chi(B_I(\mathbf{x})|\mathbf{z}) \\ &= \tfrac{q^{|I|}}{|C^{\perp}|} \sum_{\mathbf{u} \in C^{\perp}} \lambda(\mathbf{z}.\mathbf{x}) \hat{\chi}(B_{I^C, \widetilde{\mathbb{P}}}|\mathbf{z}) \\ &= q^{\gamma} \sum_{\mathbf{z} \in C^{\perp} \cap B_{I^C, \widetilde{\mathbb{P}}}} \lambda(\mathbf{z}.\mathbf{x}) \\ &= q^{\gamma} \lambda(\mathbf{0}) = q^{\gamma}. \end{aligned}$$

□

Teorema 3.5.17. [*HK08*] *Seja $\mathbb{P}$ um poset sobre $[n]$, então*
C é um $\mathbb{P}$-código MDS se, e somente se, $C^{\perp}$ é um $\widetilde{\mathbb{P}}$-código MDS.

Demonstração. Seja C é um $\mathbb{P}$-código MDS. Pelo Teorema 3.4.9, C é um $\mathbb{P}$-código MDS se, e somente se, C é I-perfeito para todo ideal I com $\mid I \mid = n - k$.

Agora, pelo Teorema 3.5.16, C é I-perfeito para todo ideal I com $\mid I \mid = n-k$ se, e somente se, $d_{\widetilde{\mathbb{P}}}(C^{\perp}) \geq k + 1$. Assim, pelo Limitante de Singleton Generalizado, temos

$$d_{\widetilde{\mathbb{P}}}(C^{\perp}) = k + 1.$$

Portanto, $C^{\perp}$ é um $\widetilde{\mathbb{P}}$-código MDS.
□

Capítulo 4

Teorema da Minimalidade $\mathbb{P}$-MDS

4.1 Introdução

Definição 4.1.1. *Dizemos que um $\mathbb{P}$-código C é $(\mathbb{P},t)$-MDS se $d_t^{\mathbb{P}}(C) = n-k+t$.*

No trabalho [MF10], Moura e Firer demonstraram a relação de dualidade em espaços poset para um $\mathbb{P}$-código C e de seu dual $C^{\perp}$, um $\widetilde{\mathbb{P}}$-código. Dessa maneira, uma questão que surgiu foi se, dado um $\mathbb{P}$-código C $(\mathbb{P},t)$-MDS, poderíamos obter informações sobre $C^{\perp}$ e assim verificar se $C^{\perp}$ é $(\widetilde{\mathbb{P}}, j(t))$-MDS, ou seja,

Dado C, um $[n,k]_q$ $\mathbb{P}$-código $(\mathbb{P},s)-MDS$, quais são as condições para que $C^{\perp}$ seja um código $(\widetilde{\mathbb{P}}, r(s))-MDS$?

A partir daí, ao utilizarmos o software *Mathematica*, foi possível observar que havia relação entre um $\mathbb{P}$-código C e seu dual. Porém na tentativa de responder essa pergunta, notou-se que deveríamos saber melhor de onde partir em busca dessa relação, pois,

Se um código C é $(\mathbb{P},r)-MDS$ então ele é $(\mathbb{P},t)-MDS$, para todo $r \leq t \leq k$,

ou seja, o fato de um código C ser $(\mathbb{P},r)-MDS$ não é uma informação precisa. Assim, tornou-se natural, já que trabalhamos num universo bem ordenado, perguntar

Qual o menor $j \in \mathbb{N}$ tal que C é $(\mathbb{P},j)-MDS$?

E essa pergunta faz surgir outra questão:

Esse número está definido para qualquer $\mathbb{P}-$código ?

Com esse intuito, neste capítulo definiremos $\Omega_{\mathbb{P}}(C)$, a *Minimalidade $\mathbb{P}$-MDS de C*. A partir daí, utilizando o Teorema 3.3.19, demonstraremos o *Teorema da Minimalidade $\mathbb{P}$-MDS de C* que relaciona a minimalidade $\mathbb{P}$-MDS de C e o peso mínimo de seu dual. Seguindo adiante, faremos uma demonstração alternativa do Teorema 3.5.17, apresentada por Kim e Hyun em [HK08], utilizando o *Teorema da Minimalidade $\mathbb{P}$-MDS de C*.

Finalizamos este capítulo estudando a classe de $\mathbb{P}$-códigos não degenerados nos quais seu dual também é não degenerado. Dessa forma, definimos mais um parâmetro dentro dessa classe, a *variância $\mathbb{P}$-MDS de C*, afim de tentar medir qual a relação de distância entre as minimalidade um $\mathbb{P}$-código C e de seu dual. Com isso, demonstramos o *Teorema da Variância $\mathbb{P}$-MDS de C*, que fornece a *Identidade de Minimalidades de C*, que relaciona a minimalidade $\mathbb{P}$-MDS de C e $C^{\perp}$, os pesos mínimos e as dimensões de um $\mathbb{P}$-código C e seu dual.

4.2 Minimalidade $\mathbb{P}$-MDS de C

Definiremos nessa seção a *minimalidade $\mathbb{P}$-MDS de C*, um novo parâmetro para $\mathbb{P}$-códigos não degenerados, enunciaremos e mostraremos então o *Teorema da Minimalidade $\mathbb{P}$-MDS*.

Lema 4.2.1. *[Corolário de [MF10]] Sejam $\mathbb{P}$ um poset sobre $[n]$ e C um $[n,k]_q$ $\mathbb{P}$-código. Então*

$$2 \leq d_1^{\widetilde{\mathbb{P}}}(C^{\perp}) \text{ se, e somente se, } C \text{ é } (\mathbb{P},k) - MDS$$

Demonstração. Sejam C um $[n,k]_q$ um $\mathbb{P}$-código tal que $2 \leq d_1^{\widetilde{\mathbb{P}}}(C^{\perp})$ e

$$Y = \{d_1^{\widetilde{\mathbb{P}}}(C^{\perp}), d_2^{\widetilde{\mathbb{P}}}(C^{\perp}), \ldots, d_{n-k}^{\widetilde{\mathbb{P}}}(C^{\perp})\}$$

a hierarquia de $\widetilde{\mathbb{P}}$-pesos de $C^{\perp}$. Pelo Teorema da Monotonicidade Poset, temos $1 \notin Y$. Ainda pelo Teorema da Dualidade Poset, temos

$$X = \{n+1-d_1^{\mathbb{P}}(C), n+1-d_2^{\mathbb{P}}(C), \ldots, n+1-d_k^{\mathbb{P}}(C)\},$$

$$X \cup Y = [n] \text{ e } X \cap Y = \emptyset.$$

Logo, $1 \in X$. Como a hierarquia de pesos é uma sequência crescente, temos

$$d_1^{\mathbb{P}}(C) < d_2^{\mathbb{P}}(C) < \ldots < d_k^{\mathbb{P}}(C).$$

Com isso

$$n+1-d_k^{\mathbb{P}}(C) < n+1-d_{k-1}^{\mathbb{P}}(C) < \ldots < n+1-d_1^{\mathbb{P}}(C),$$

ou seja, $n+1-d_k^{\mathbb{P}}(C)$ é o menor elemento de X. Assim

$$n+1-d_k^{\mathbb{P}}(C) = 1 \Rightarrow d_k^{\mathbb{P}}(C) = n.$$

Portanto, C é $(\mathbb{P}, k) - MDS$.

Reciprocamente, seja C um $\mathbb{P}$-código $(\mathbb{P}, k) - MDS$, logo $d_k^{\mathbb{P}}(C) = n$. Seja X a hierarquia de $\mathbb{P}$-pesos de C, então

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

Pelo Teorema da Dualidade Poset temos

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

e

$$X \cup Y = [n], X \cap Y = \emptyset \text{ e } n \notin Y.$$

Assim,

$$máx\ Y \leq n-1.$$

Pelo Teorema da Monotonicidade Poset, para o $\widetilde{\mathbb{P}}$-código $C^{\perp}$, temos

$$d_1^{\widetilde{\mathbb{P}}}(C^{\perp}) < d_2^{\widetilde{\mathbb{P}}}(C^{\perp}) < \ldots < d_{n-k}^{\widetilde{\mathbb{P}}}(C^{\perp}).$$

Logo

$$n+1-d_{n-k}^{\widetilde{\mathbb{P}}}(C^{\perp}) < n+1-d_{n-k-1}^{\widetilde{\mathbb{P}}}(C^{\perp}) < \ldots < n+1-d_1^{\widetilde{\mathbb{P}}}(C^{\perp}).$$

Portanto,

$$máx\ Y = n+1-d_1^{\widetilde{\mathbb{P}}}\ (C^{\perp})$$

e

$$n+1-d_1^{\widetilde{\mathbb{P}}}\ (C^{\perp}) \leq n-1 \Rightarrow 2 \leq d_1^{\widetilde{\mathbb{P}}}\ (C^{\perp}).$$

□

Definição 4.2.2. *Um código C é dito* ***não degenerado*** *se $2 \leq d_{\mathbb{H}}(C^{\perp})$, onde $d_{\mathbb{H}}$ é a distância de Hamming.*

Lema 4.2.3. *[Corolário de [MF10]] Se C é um $[n,k]_q$ $\mathbb{P}$-código não degenerado, então C é $(\mathbb{P}, k) - MDS$.*

Demonstração. Seja C um $[n,k]_q$ $\mathbb{P}$-código não degenerado, logo

$$2 \leq d_{\mathbb{H}}(C^{\perp}).$$

Como

$$d_{\mathbb{H}}(C^{\perp}) \leq d_{\widetilde{\mathbb{P}}}(C^{\perp}),$$

temos

$$2 \leq d_{\widetilde{\mathbb{P}}}(C^{\perp}) = d_1^{\widetilde{\mathbb{P}}}(C^{\perp}).$$

Portanto, pelo Lema 4.2.1, C é $(\mathbb{P},k) - MDS$.
□

Esse resultado respondeu parcialmente nossas perguntas. Para códigos não degenerados podemos definir um novo parâmetro no espaço poset.

Definição 4.2.4. *Seja C um $[n,k]_q$ $\mathbb{P}$-código não degenerado. A* ***minimalidade*** *$\mathbb{P}-MDS$* ***de*** *C, denotada por $\Omega_{\mathbb{P}}(C)$, é o menor $t \in \mathbb{N}$ tal que C é $(\mathbb{P},t)-MDS$.*

Observe que

$$1 \leq \Omega_{\mathbb{P}}(C) \leq k,$$

pois se C é não degenerado, então, pelo Lema 4.2.3, C é $(\mathbb{P},k) - MDS$.

O Teorema da Dualidade Poset, demonstrado por Moura e Firer, em [MF10], se mostrou fundamental para nos familiarizarmos com a hierarquia de $\mathbb{P}$-pesos de C e de seu dual. Dessa forma, ao estudarmos a hierarquia de $\mathbb{P}$-pesos de diversos $\mathbb{P}$-códigos com o software *Mathematica*, percebemos que esse novo parâmetro $\Omega_{\mathbb{P}}(C)$ e $d_1^{\mathbb{P}}(C^{\perp})$ estavam intimamente relacionados, e com sua existência garantida pelo Lema 4.2.3, enunciamos e provamos o *Teorema da Minimalidade $\mathbb{P}$-MDS*, um dos resultados principais desse trabalho, que é decorrente do Teorema 3.3.19 e da definição de $\Omega_{\mathbb{P}}(C)$.

Teorema 4.2.5. *[Teorema da Minimalidade $\mathbb{P}$-MDS] Seja C um $[n,k]_q$ $\mathbb{P}$-código não degenerado, então*

$$\Omega_{\mathbb{P}}(C) = r \text{ se, e somente se, } d_1^{\widetilde{\mathbb{P}}}(C^{\perp}) = k - r + 2.$$

Demonstração. Seja C um $[n,k]_q$ $\mathbb{P}$-código não degenerado, com $\Omega_{\mathbb{P}}(C) = r$. Então

$$d_r^{\mathbb{P}}(C) = n - k + r,$$

$$d_{r+1}^{\mathbb{P}}(C) = n - k + r + 1,$$

$$\vdots$$

$$d_k^{\mathbb{P}}(C) = n$$

e

$$d_{r-1}^{\mathbb{P}}(C) < n - k + r - 1.$$

Seja X a hierarquia de $\mathbb{P}$-pesos de C, então

$$X = \{d_1^{\mathbb{P}}(C), d_2^{\mathbb{P}}(C), \ldots; d_{r-1}^{\mathbb{P}}(C), n - k + r, n - k + r + 1, \ldots, n\}.$$

Logo

$$n - k + r - 1 \notin X.$$

Agora, pelo Teorema da Dualidade Poset, temos

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

$$X \cup Y = [n] \text{ e } X \cap Y = \emptyset.$$

Logo

$$n - k + r - 1 \in Y,$$

e

$$n - k + r - 1 = máx\ Y,$$

pois

$$\{n - k + r, n - k + r + 1, \ldots, n\} \subset X.$$

Pelo Teorema da Monotonicidade Poset, temos

$$d_1^{\tilde{\mathbb{P}}}(C^{\perp}) < d_2^{\tilde{\mathbb{P}}}(C^{\perp}) < \ldots < d_{n-k}^{\tilde{\mathbb{P}}}(C^{\perp}).$$

Assim

$$n + 1 - d_{n-k}^{\tilde{\mathbb{P}}}(C^{\perp}) < n + 1 - d_{n-k-1}^{\tilde{\mathbb{P}}}(C^{\perp}) < \ldots < n + 1 - d_1^{\tilde{\mathbb{P}}}(C^{\perp}).$$

Como $n - k + r - 1 = máx\ Y$, segue

$$n - k + r - 1 = n + 1 - d_1^{\tilde{\mathbb{P}}}(C^{\perp}) \Rightarrow d_1^{\tilde{\mathbb{P}}}(C^{\perp}) = k - r + 2.$$

Reciprocamente, seja C um $[n, k]_q$ $\mathbb{P}$-código não degenerado com

$$d_1^{\tilde{\mathbb{P}}}(C^{\perp}) = k - r + 2.$$

Seja Y a hierarquia de $\widetilde{\mathbb{P}}$-pesos de $C^{\perp}$, assim

$$Y = \{d_1^{\widetilde{\mathbb{P}}}(C^{\perp}), d_2^{\widetilde{\mathbb{P}}}(C^{\perp}), \ldots, d_{n-k}^{\widetilde{\mathbb{P}}}(C^{\perp})\}.$$

Pelo Teorema da Monotonicidade Poset, como

$$d_1^{\widetilde{\mathbb{P}}}(C^{\perp}) < d_2^{\widetilde{\mathbb{P}}}(C^{\perp}) < \ldots < d_{n-k}^{\widetilde{\mathbb{P}}}(C^{\perp}),$$

então $\{1, 2, \ldots, k-r+1\}$ não está contido em Y.

Pelo Teorema da Dualidade Poset, que

$$X = \{n+1-d_1^{\mathbb{P}}(C), n+1-d_2^{\mathbb{P}}(C), \ldots, n+1-d_k^{\mathbb{P}}(C)\},$$

$$X \cup Y = [n] \text{ e } X \cap Y = \emptyset.$$

Assim

$$\{1, 2, \ldots, k-r+1\} \subseteq X \text{ e } k-r+2 \notin X.$$

Pelo Teorema da Monotonicidade Poset, como

$$d_1^{\mathbb{P}}(C) < d_2^{\mathbb{P}}(C) < \ldots < d_k^{\mathbb{P}}(C),$$

temos

$$n+1-d_k^{\mathbb{P}}(C) < n+1-d_{k-1}^{\mathbb{P}}(C) < \ldots < n+1-d_1^{\mathbb{P}}(C).$$

Logo

$$n+1-d_k^{\mathbb{P}}(C) = 1 \Rightarrow d_k^{\mathbb{P}}(C) = n.$$

$$n+1-d_{k-1}^{\mathbb{P}}(C) = 2 \Rightarrow d_{k-1}^{\mathbb{P}}(C) = n-1.$$

$$\vdots$$

$$n+1-d_r^{\mathbb{P}}(C) = k-r+1 \Rightarrow d_r^{\mathbb{P}}(C) = n-k+r.$$

Dessa forma C é $(\mathbb{P}, r) - MDS$ e $\Omega_{\mathbb{P}}(C) \leq r$. Como $k-r+2 \notin X$, temos

$$n+1-d_{r-1}^{\mathbb{P}}(C) > k-r+2 \Rightarrow d_{r-1}^{\mathbb{P}}(C) < n-k+r-1.$$

Portanto, r é o menor número tal que C é $(\mathbb{P}, r) - MDS$, ou seja, $\Omega_{\mathbb{P}}(C) = r$.
□

O Teorema da Minimalidade $\mathbb{P}$-MDS é de interesse na Teoria de Códigos visto que, dado C um $[n,k]_q$ $\mathbb{P}$-código não degenerado, ao calcularmos $d_1^{\widetilde{\mathbb{P}}}(C^{\perp})$, o Teorema da Minimalidade $\mathbb{P}$-MDS nos fornece

$$\Omega_{\mathbb{P}}(C) = k - d_1^{\widetilde{\mathbb{P}}}(C^{\perp}) + 2,$$

ou seja, C é $(\mathbb{P}, r) - MDS$, em outras palavras, já temos $k - \Omega_{\mathbb{P}}(C) + 1$ $\mathbb{P}$-pesos mínimos calculados na hierarquia de $\mathbb{P}$-pesos de C.

Como consequência do Teorema da Minimalidade $\mathbb{P}$-MDS, segue o Teorema 3.5.17, demonstrado por Hyun e Kim em [HK08], utilizando os conceitos de I-bola e $\mathbb{P}$-códigos I-perfeitos.

Corolário 4.2.6. *Sejam C um $[n,k]_q$ $\mathbb{P}$-código e $C^{\perp}$ seu código dual. Então*

$$C \text{ é } \mathbb{P} - MDS \text{ se, e somente se } C^{\perp} \text{ é } \widetilde{\mathbb{P}} - MDS.$$

Demonstração. Seja C um $[n,k]_q$ $\mathbb{P}$-código MDS, então

$$d_{\mathbb{P}}(C) = d_1^{\mathbb{P}}(C) = n - k + 1,$$

ou seja

$$\Omega_{\mathbb{P}}(C) = 1.$$

Pelo Teorema da Minimalidade $\mathbb{P}$-MDS para C, temos

$$d_1^{\widetilde{\mathbb{P}}}(C^{\perp}) = k + 1.$$

Logo $C^{\perp}$ é $\widetilde{\mathbb{P}}$-MDS.
Reciprocamente, seja $C^{\perp}$ um $[n, n-k]_q$ $\widetilde{\mathbb{P}}$-código MDS, então

$$d_1^{\widetilde{\mathbb{P}}}(C^{\perp}) = k + 1.$$

Pelo Teorema da Minimalidade $\mathbb{P}$-MDS para C, temos

$$\Omega_{\mathbb{P}}(C) = 1.$$

Portanto, C é $\mathbb{P}$-MDS.
□

Definição 4.2.7. *A* **$\mathbb{P}$-discrepância** *de C, denotada por $\delta_{\mathbb{P}}(C)$, é o menor inteiro s tal que*

$$d_{s+1}^{\mathbb{P}}(C) > n - k.$$

Observando as definições de $\Omega_{\mathbb{P}}(C)$ e $\delta_{\mathbb{P}}(C)$ temos que a minimalidade $\mathbb{P}$-MDS é sempre menor que a $\mathbb{P}$-discrepância de C. Dessa forma, enunciamos a seguinte proposição.

Proposição 4.2.8. *Seja C um $[n,k]_q$ $\mathbb{P}$-código não degenerado. Então*

$$\delta_{\mathbb{P}}(C) < \Omega_{\mathbb{P}}(C).$$

Demonstração. Seja C um $[n,k]_q$ $\mathbb{P}$-código não degenerado tal que $\Omega_{\mathbb{P}}(C) = r$. Então

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

Como

$$n - k < n - k + r = d_r^{\mathbb{P}}(C),$$

pela definição de $\mathbb{P}$-discrepância, temos

$$\delta_{\mathbb{P}}(C) \leq r - 1.$$

Assim

$$\delta_{\mathbb{P}}(C) \leq \Omega_{\mathbb{P}}(C) - 1 < \Omega_{\mathbb{P}}(C).$$

Portanto,

$$\delta_{\mathbb{P}}(C) < \Omega_{\mathbb{P}}(C).$$

□

O parâmetro $\Omega_{\mathbb{P}}(C)$ nos permite contar o número de palavras código nas I-bolas onde $\mid I \mid = n - k + \Omega_{\mathbb{P}}(C) - 1$.

Corolário 4.2.9. *Se C um $[n,k]_q$ $\mathbb{P}$-código não degenerado, então para cada ideal $I \subset \mathbb{P}$, com $\mid I \mid = n - k + \Omega_{\mathbb{P}}(C) - 1$, cada I-bola contém exatamente $q^{\Omega_{\mathbb{P}}(C)-1}$ palavras de C.*

Demonstração. Basta tomar $\delta = \Omega_{\mathbb{P}}(C) - 1$ no Teorema 3.5.16.
□

4.3 Variância $\mathbb{P}$-MDS de C

Para a classe de códigos onde C e $C^{\perp}$ são não degenerados, observamos que podemos aplicar o Teorema da Minimalidade $\mathbb{P}$-MDS para C e $C^{\perp}$. Dessa forma podemos estudar melhor a relação $r(s)$ perguntada nessa seção.

Definição 4.3.1. *Um $\mathbb{P}$- código C é dito* ***dualmente não degenerado*** *se, e somente se, C e $C^{\perp}$ são não degenerados.*

Esta definição garante que os números $\Omega_{\mathbb{P}}(C)$ e $\Omega_{\widetilde{\mathbb{P}}}(C^{\perp})$ estão definidos, pois como C é dualmente não degenerado, então C é $(\mathbb{P}, k) - MDS$ e $C^{\perp}$ é $(\widetilde{\mathbb{P}}, n-k) - MDS$. Agora com os parâmetros $\Omega_{\mathbb{P}}(C)$ e $\Omega_{\widetilde{\mathbb{P}}}(C^{\perp})$ bem definidos, podemos pensar em como $\Omega_{\mathbb{P}}(C)$ varia em relação a $\Omega_{\widetilde{\mathbb{P}}}(C^{\perp})$ e vice-versa. Assim, definimos um novo parâmetro que visa medir a distância entre as minimalidade de um $\mathbb{P}$-código C e de seu dual. Enunciamos e provamos então o *Teorema da Variância $\mathbb{P}$-MDS de C.*

Definição 4.3.2. *Dado C um $\mathbb{P}$- código dualmente não degenerado, definimos a* ***variância $\mathbb{P}$-MDS de C****, denotado por $\Delta_{\mathbb{P}}(C)$, como sendo o número inteiro*

$$\Delta_{\mathbb{P}}(C) = \Omega_{\mathbb{P}}(C) - \Omega_{\widetilde{\mathbb{P}}}(C^{\perp}).$$

Observe

$$k - n \leq \Delta_{\mathbb{P}}(C) \leq k - 1$$

e

$$\Delta_{\mathbb{P}}(C) = -\Delta_{\widetilde{\mathbb{P}}}(C^{\perp}).$$

Dessa forma, enunciamos.

Teorema 4.3.3. *[Teorema da Variância $\mathbb{P}$-MDS] Seja C um $[n,k]_q$ $\mathbb{P}$-código dualmente não degenerado. Então*

$$\Delta_{\mathbb{P}}(C) = d_1^{\mathbb{P}}(C) - d_1^{\widetilde{\mathbb{P}}}(C^{\perp}) - n + 2k.$$

Demonstração. Seja C um $[n,k]_q$ $\mathbb{P}$-código dualmente não degenerado com

$$\Delta_{\mathbb{P}}(C) = \Omega_{\mathbb{P}}(C) - \Omega_{\widetilde{\mathbb{P}}}(C^{\perp}),$$

a variância $\mathbb{P}$-MDS de C.

Pelo Teorema da Minimalidade $\mathbb{P}$-MDS, temos

$$\Omega_{\mathbb{P}}(C) = k - d_1^{\widetilde{\mathbb{P}}}(C^{\perp}) + 2$$

e

$$\Omega_{\widetilde{\mathbb{P}}}(C^{\perp}) = n - k - d_1^{\mathbb{P}}(C) + 2.$$

Assim

$$\Delta_{\mathbb{P}}(C) = k - d_1^{\widetilde{\mathbb{P}}}(C^{\perp}) + 2 - (n - k - d_1^{\mathbb{P}}(C) + 2).$$

Portanto,

$$\Delta_{\mathbb{P}}(C) = d_1^{\mathbb{P}}(C) - d_1^{\widetilde{\mathbb{P}}}(C^{\perp}) - n + 2k.$$

□

Como consequência do Teorema da Variância $\mathbb{P}$-MDS, surge uma identidade que relaciona o peso mínimo, a minimalidade e a dimensão de um $\mathbb{P}$-código C e de seu dual $C^{\perp}$.

Corolário 4.3.4. *Todo $\mathbb{P}$-código C dualmente não degenerado satisfaz*

$$d_{\mathbb{P}}(C) - d_{\widetilde{\mathbb{P}}}(C^{\perp}) - \Omega_{\mathbb{P}}(C) + \Omega_{\widetilde{\mathbb{P}}}(C^{\perp}) = dim\ C^{\perp} - dim\ C. \tag{4.1}$$

Demonstração. Seja C um $[n,k]_q$ $\mathbb{P}$-código dualmente não degenerado. Considere $\Omega_{\mathbb{P}}(C)$ e $\Omega_{\widetilde{\mathbb{P}}}(C^{\perp})$ as minimalidade de C e $C^{\perp}$.

Pelo Teorema da Variância $\mathbb{P}$-MDS, temos

$$\Delta_{\mathbb{P}}(C) = d_1^{\mathbb{P}}(C) - d_1^{\widetilde{\mathbb{P}}}(C^{\perp}) - n + 2k.$$

Por definição

$$\Delta_{\mathbb{P}}(C) = \Omega_{\mathbb{P}}(C) - \Omega_{\widetilde{\mathbb{P}}}(C^{\perp}).$$

Assim, obtemos

$$\Omega_{\mathbb{P}}(C) - \Omega_{\widetilde{\mathbb{P}}}(C^{\perp}) = d_1^{\mathbb{P}}(C) - d_1^{\widetilde{\mathbb{P}}}(C^{\perp}) - n + 2k.$$

Logo

$$d_1^{\mathbb{P}}(C) - d_1^{\widetilde{\mathbb{P}}}(C^{\perp}) - \Omega_{\mathbb{P}}(C) + \Omega_{\widetilde{\mathbb{P}}}(C^{\perp}) = n - 2k = n - k - k.$$

Portanto,

$$d_{\mathbb{P}}(C) - d_{\widetilde{\mathbb{P}}}(C^{\perp}) - \Omega_{\mathbb{P}}(C) + \Omega_{\widetilde{\mathbb{P}}}(C^{\perp}) = dim\ C^{\perp} - dim\ C.$$

□

A equação (4.1) será chamada **Identidade de Minimalidades $\mathbb{P}$-MDS de C**. Uma consequência imediata desse resultado é apresentada a seguir.

Corolário 4.3.5. *Seja C um $[n,k]_q$ $\mathbb{P}$-código dualmente não degenerado, então*

$$d_1^{\mathbb{P}}(C) - d_1^{\widetilde{\mathbb{P}}}(C^{\perp}) = n - 2k \text{ se, e somente se, } \Omega_{\mathbb{P}}(C) = \Omega_{\widetilde{\mathbb{P}}}(C^{\perp}).$$

Demonstração. Segue diretamente da *Identidade de Minimalidades $\mathbb{P}$-MDS de C.*

□

4.4 Perspectivas Futuras

O objetivo central desse trabalho foi estudar a distribuição de $\mathbb{P}$-pesos, apresentada em [HK08], a fim de nos ambientarmos com o espaço de distribuição do mesmo.

No decorrer deste trabalho, estudamos todas os principais resultados sobre códigos corretores de erros dentro da nova métrica, introduzida em [BGL95] por Brualdi, Greaves e Lawrence. Um resultado determinante para conclusão desse trabalho foi o Teorema da Dualidade Poset, provada em [MF10], por Moura e Firer.

Observando a relação entre a minimalidade $\mathbb{P}$-MDS de um código C e o peso mínimo do seu dual, conseguimos mostrar que, para um $\mathbb{P}$-código C, dualmente não degenerado, é possível saber a variação entre $\Omega_{\mathbb{P}}(C)$ e $\Omega_{\widetilde{\mathbb{P}}}(C^{\perp})$, através da variância $\Delta_{\mathbb{P}}(C)$. A Identidade de Minimalidades veio confirmar a boa definição desses novos parâmetro para a classe de códigos dualmente não degenerados.

Como perspectiva futura, verificaremos quais as aplicações dessa identidade para os canais Wire-Tap II, que originaram os trabalhos de Wei, e buscaremos informações e propriedade de $\mathbb{P}$-códigos a partir desses novos parâmetros. Se possível, buscaremos classificar $\mathbb{P}$-códigos não degenerados, através da minimalidade $\mathbb{P}$-MDS de C, $\Omega_{\mathbb{P}}(C)$. No caso onde C é dualmente não degenerados podemos nos perguntar quais propriedades podemos encontrar a partir de $\Delta_{\mathbb{P}}(C)$, a variância $\mathbb{P}$-MDS de C.

Referências Bibliográficas

[BGL95] R. A. Brualdi, J. S. Graves, and K. M. Lawrence. Codes with a poset metric. *Discrete Math*, 147:57–72, 1995.

[Ham50] R. W. Hamming. Error detecting and error correcting codes. *Bell System Tech*, 1(29):147160, 1950.

[HK08] J.Y Hyun and H.K. Kim. Maximum distance separable poset codes. *Codes Cryptografy - Springer*, 48:247–261, 2008.

[HKY92] T. Helleseth, T. Klove, and O. Ytrehus. Generalized hamming weight of linear codes. *Trans. Inform. Theory*, 38(3):1133–1140, 1992.

[HV02] A. Hefez and M. L. T. Villela. *Códigos Corretores de Erros*. Série Computação e Matemática, IMPA, Rio de Janeiro, 2002.

[JH98] J.Neggers and H.S.Kim. *Basis Posets*. World Cientific Publishing Co. Inc., 1998.

[LLB08] L.Panek, E. Lazarotto, and F.M. Bando. Codes satisfying the chain condition over rosenbloom-tsfasman spaces. *Int. J. Pure Appl. Math.*, 48:217–222, 2008.

[MF10] A. O. Moura and M. Firer. Duality for poset codes. *IEEE Trans. Inform. Theory*, 56(7):3180 – 3186, 2010.

[Mon78] L. H. Jacy Monteiro. *Elementos de algebra*. Rio de Janeiro: Livros Tecnicos e Cientificos, 1978.

[Nie91] H. Niederreiter. A combinatorial problem for vector spaces over finite fields. *Discrete Math.*, 96(3):221–228, 1991.

[PFKH08] L. Panek, M. Firer, H. K. Kim, and J. Y. Hyun. Groups of linear isometries on poset structures. *Discrete Math*, 308(18):4116–4123, 2008.

[Sha48] C . E. Shannon. A mathematical theory of communication. *Bell System Tech*, 1(27):379–423, 1948.

[Sta72] R. P. Stanley. *Enumerative Combinatorics*. Brooks -Cole, 1972.

[TG95] M. A. Tsfasman and Vladut S. G. Geometric approach to higher weights. *IEEE Trans. Inform. Theory*, 41(6):1564–1588, 1995.

[Wei91] V. K. Wei. Generalized hamming weights for linear code. *IEEE Trans. Inform. Theory*, 37:1412–1418, 1991.