Universidade Federal de Juiz de Fora
Instituto de Ciências Exatas
Programa de Mestrado Acadêmico em Matemática

Pedro Esperidião dos Santos Neto

Códigos Corretores de Erros em Espaços Poset

Juiz de Fora
2016

Pedro Esperidião dos Santos Neto

Códigos Corretores de Erros em Espaços Poset

Dissertação apresentada ao Programa de Mestrado Acadêmico em Matemática da Universidade Federal de Juiz de Fora, na área de concentração em , como requisito parcial para obtenção do título de Mestre em Matemática.

Orientadora: Beatriz Casulari da Motta Ribeiro

Juiz de Fora

2016

Ficha catalográfica elaborada através do Modelo Latex do CDC da UFJF
com os dados fornecidos pelo(a) autor(a)

Esperidião, Pedro.
Códigos Corretores de Erros em Espaços Poset / Pedro Esperidião dos Santos Neto. – 2016.
85 f. : il.

Orientadora: Beatriz Casulari da Motta Ribeiro
Dissertação (Mestrado) – Universidade Federal de Juiz de Fora, Instituto de Ciências Exatas. Programa de Mestrado Acadêmico em Matemática, 2016.

1. Poset. 2. Códigos Corretores de Erros. 3. Teoria da Informação. I. Motta, Beatriz, orient. II. Título.

Pedro Esperidião dos Santos Neto

Códigos Corretores de Erros em Espaços Poset

Dissertação apresentada ao Programa de Mestrado Acadêmico em Matemática da Universidade Federal de Juiz de Fora, na área de concentração em , como requisito parcial para obtenção do título de Mestre em Matemática.

Aprovada em 16 de dezembro de 2016

BANCA EXAMINADORA

Professora Dra. Beatriz Casulari da Motta Ribeiro
Orientadora
Universidade Federal de Juiz de Fora

Professor Dr. Allan de Oliveira Moura
Universidade Federal de Viçosa

Professora Dra. Flaviana Andrea Ribeiro
Universidade Federal de Juiz de Fora

AGRADECIMENTOS

É preciso agradecer a todos que, de alguma forma contribuíram para que hoje eu me tornasse mestre em Matemática. Não consegui chegar até aqui sozinho: tive a sorte de ter pessoas que me guiaram, ensinaram e apoiaram e sem elas isso não seria possível.

Os primeiros a quem gostaria de agradecer são meus pais, Cícero e Yara, que sempre priorizaram a educação dos filhos, mesmo que por muitas vezes fossem necessários sacrifícios. Obrigado pelo apoio em tudo que venho fazendo.

A meus irmãos, João e Marianna, pelo carinho e por sempre estarem lá para dar suporte e tornarem cada conquista ainda mais gratificantes.

A minha amiga e namorada, Eduarda, que acompanhou tudo desde antes do aceite no Mestrado, apoiou e ajudou a lidar com o desafio de estudar em dois cursos desafiadores ao mesmo tempo de forma mais tão presente.

A minha orientadora, Beatriz, pela parceria neste trabalho. Mesmo em condições pouco favoráveis apostou que poderíamos desenvolvê-lo e bem. Obrigado pela orientação e pela compreensão.

A minha primeira orientadora, Flaviana, que me "alfabetizou"em Matemática com vários "faz isso no quadro"nos primeiros estágios de PICME.

Aos demais professores do departamento de Matemática que contribuíram para minha formação.

A CAPES/CNPq pelo apoio financeiro e a todos os demais que contribuíram direta ou indiretamente com este trabalho.

RESUMO

O presente trabalho versa sobre códigos corretores de erros e seus duais sobre espaços poset. Inicialmente, veremos os conceitos do que é um código e a utilidade de um código corretor de erros em um sistema de comunicação e construiremos as principais propriedades de corpos finitos. Estes conceitos combinados serão utilizados para a construição de códigos corretores de erros em espaços de Hamming, amplamente aplicados hoje. Em seguida, construiremos os códigos corretores de erros sobre espaços poset e algumas de suas consequências, como o surgimento de códigos P-MDS. Enunciaremos o Teorema da Dualidade para espaços poset e, por fim, analisaremosos códigos do tipo P-cadeia e algumas de suas propriedades provenientes do Teorema da Dualidade.

Palavras-chave: Códigos. Poset. Códigos corretores de erros.

ABSTRACT

This piece of work treats of error correcting codes and their dual codes in poset spaces. Initially we will cover the concepts of what is a code and the need of an error correction code in a communication system and the main properties of finite fields. These concepts combined are used for building the error correction codes in Hamming spaces, which are currently largely applied. Poset spaces are proposed as a generalization of the Hamming spaces e we will build the codes over poset spaces and some of their consequences, as the occurrence of P-MDS codes. Then, we will state and prove the Duality Theorem for poset spaces. Lastly, we will analyze the P-chain codes some and of their properties derived from the Duality Theorem.

Key-words: Codes. Poset. Error correction codes.

SUMÁRIO

1 INTRODUÇÃO

Desde que seus fundamentos foram lançados por Shannon, em 1948, a Teoria da Informação tem sido progressivamente desenvolvida, buscando formas de contornar o limite da performance da taxa de informação através de um canal de comunicação, estimado pelo Teorema de Shannon-Hartley (Teorema 17 de [1], veja anexo A), a proteção de informação e a quebra de segredos através de sua subárea de Criptografia e a segurança de uma transmissão de informação correta, pelos métodos de correção de erros.

Desta grande área, este trabalho aborda o tópico dos Códigos Corretores de Erros Lineares, de dentro dos métodos de correção de erros, em que as mensagens a serem transmitidas são codificadas como elementos de um subespaço vetorial e tratamos os possíveis erros que surjam como aditivos a vetores que representam palavras, em especial os códigos sobre espaços poset, que apresentam uma generalização da métrica de Hamming e potenciais aprimoramentos para as técnicas de correção de erros, em especial tornar códigos que não eram perfeitos em perfeitos, reduzindo ambiguidades.

As principais referências deste trabalho são [3] e [7]. A primeira trata de corpos finitos, extensões destes corpos e códigos lineares e será o guia para os capítulos 3 e 4, de onde é retirada a maior parte dos resultados. Com o conceito de um espaço poset sendo apresentado no capítulo 5, na segunda metade deste texto este papel é ocupado por [7].

O Capítulo 2 deste texto se baseia em [2] e apresenta os conceitos básicos acerca dos Sistemas de Comunicação, uma perspectiva da área de Engenharia de Telecomunicações desta área, descrevendo um sistema de comunicação, o papel dos códigos corretores de erros nestes sistemas e as definições de informação e entropia em um sistema de comunicação.

O Capítulo 3 se volta à álgebra de corpos finitos, elementos básicos para a construção de códigos corretores de erros lineares, extensivamente utilizados ao longo do texto, enunciando os principais resultados a serem utilizados.

O Capítulo 4 retorna aos códigos, apresentando as definições matemáticas de distâncias dentro de um código, as operações a que estes conjuntos se submetem e necessários para que a correção de erros seja de fato executada.

O Capítulo 5 apresenta o conceito de posets, conjuntos parcialmente ordenados, partindo do conceito de ordem parcial e construindo a métrica por ela induzida. Os resultados deste capítulo serão fundamentais para a construção dos resultados dos capítulos 7 e 8.

O Capítulo 6 estuda os multiconjuntos e enuncia resultados que permitirão a demonstração do Teorema da Dualidade para Códigos Poset.

O Capítulo 7 utiliza destes resultados e dos obtidos no Capítulo 5 para a demonstração do Teorema da Dualidade para Códigos Poset.

O Capítulo 8, por fim, trata dos códigos do tipo cadeia em espaços poset. Um código C desta família de códigos lineares tem a propriedade de ter subcódigos aninhados $\{0\} = C_0 \subsetneq C_1 \subsetneq \ldots \subsetneq C_k = C$, com $dim_F C_i = i$ e C_i o subcódigo de C que utiliza menos símbolos não-nulos.

2 SISTEMAS DE COMUNICAÇÃO

2.1 CONCEITOS BÁSICOS

Comunicação é o processo de transmissão de mensagens partindo de um ponto a outro distante ou a um grupo de pontos distantes. Chamamos o ponto de partida da mensagem de fonte de informação, ou simplesmente, fonte e um ponto de destino de receptor. Telecomunicação é a transmissão física destas mensagens através de impulsos eletromagnéticos através de um canal de comunicação, normalmente chamado apenas por canal, que é o meio físico por onde a informação trafega (cabos de cobre, cabos ópticos de vidro ou ar, no caso de transmissões *wireless*, por exemplo).

Existem dois modos básicos de comunicações: ponto-a-ponto (*peer-to-peer* ou P2P) quando envolvem uma única fonte e um único receptor e *broadcast* quando envolvem uma fonte (em todo o tempo, ou um por vez, *multiplexado*) e vários receptores. Quanto à natureza da transmissão, elas também podem ser digitais ou analógicas. Para o primeiro grupo, as mensagens transmitidas são elementos de um conjunto discreto pré-determinado. Para o segundo, as mensagens são sinais (magnitudes de grandezas eletromagnéticas, como tensão elétrica ou corrente) contínuos no tempo, $s(t)$. Por exemplo, as ondas eletromagnéticas transmitidas em modulação AM tem sua amplitude expressa na forma $s(t) = m(t) \cdot cos(\omega_c t + \theta)$, em que $m(t)$ é também um sinal analógico, mas de espectro de frequências $\omega << \omega_c$.

Neste contexto, podemos definir um Sistema de Comunicação, ou Sistema de Telecomunicação, como um conjunto de fontes e receptores (e os equipamentos envolvidos) interligados por meio de canais que visam a transmissão de informação de forma eficiente, segura, confiável e de alta performance. Tomaremos Sistemas de Comunicação e Sistemas de Telecomunicação como sinônimos neste texto.

2.2 ESTRUTURA DE UM SISTEMA DE COMUNICAÇÃO

O real significado de transmissão eficiente, segura, confiável e de alta performance pode ser melhor apreciado após uma observação sobre o caminho usual que a informação percorre entre uma fonte e um receptor, que pode ser observado na Figura 1.

Os elementos elencados na Figura 1 realizam as seguintes operações:

1. Fonte: Gera o dado a ser transmitido, seja uma transmissão *streamming* ou um SMS, por exemplo.

2. Codificador de fonte: Comprime dados removendo reduncância.

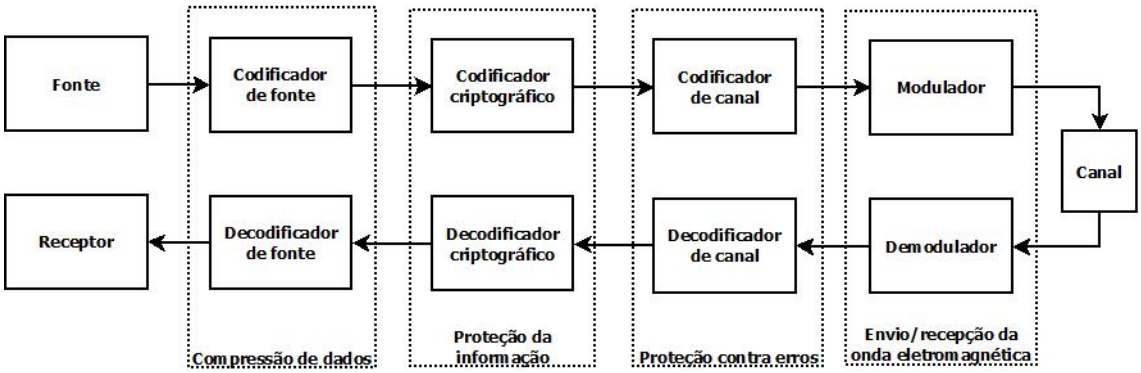

Figura 1 – Estrutura geral de um sistema de comunicação

3. Codificador criptográfico: ou encriptador, esconde a informação, de forma que se uma fonte indesejada captura a mensagem, não conseguirá extrair seu significado.

4. Codificador de canal: Insere dados redundantes à mensagem, de modo a conseguir identificar e/ou corrigir possíveis erros que possam ser inseridos por imperfeições do sistema.

5. Modulador: Converte mensagens em sinais eletromagnéticos a serem transmitidos.

6. Canal: É o meio físico por onde o sinal portador de informação propaga. É a principal fonte de erros de um sistema de comunicação.

7. Demodulador: ou equalizador, transforma o sinal recebido em símbolos, a menor porção individual de informação possível no sistema.

8. Decodificador de canal: Se utiliza das reduncâncias inseridas pelo codificador de canal para eliminar quaisquer erros que possam ter sido introduzidos.

9. Decodificador criptográfico: ou decriptador, desfaz a criptografia inserida, revelando a mensagem originalmente transmitida pelo codificador de fonte.

10. Decodificador de fonte: Descompacta a informção.

11. Receptor: É o destino da informação.

Um sistema de informação eficiente utilizará o mínimo de dados necessário, reduzindo o quantidade de dados transmitida pela fonte e tratada pelos codificadores e decodificadores de fonte. Ele também será seguro se for criptografado cumprindo o objetivo de esconder a informação transmitida; é o foco de transações bancárias, por exemplo, proteger as informações sobre as contas de seus clientes e evitar ataques externos. Este sistema também será confiável se propagar o mínimo de erros possível. Uma figura de mérito sobre a confiabilidade de um sistema de comunicação é a *BER* (*bit error rate*),

quantidade de bits erroneamente transmitidos pelo total, expressa normalmente em partes por milhão. E por fim, sua performance será a melhor quanto maior for a taxa de dados transmitida, medida em *bits por segundo, b/s*, para sistemas digitais.

É sobre a proteção contra erros que se aplicam os código detectores e corretores de erros.

2.3 CÓDIGOS DE CONTROLE DE ERROS

Códigos corretores de erros são meios pelos quais quaisquer erros que possam ter sido introduzidos aos dados transmitidos por um canal são corrigidos baseados na mensagem recebida pelo decodificador de canal, como descrito na Seção 2.2. Os códigos detectores de erros são os meios pelos quais tais erros são detectados. Ambas as classes estão dentro de um conjunto de códigos chama códigos de controle de erros.

Exemplo 2.3.1. Todo leitor de *Blu-Ray*, por exemplo, aplica códigos corretores de erros ao ler seus dados (em especial, os da classe Reed-Solomon). Por este motivo que mesmo com pequenos arranhões é possível extrair o seu conteúdo.

Exemplo 2.3.2. Um exemplo cotidiano e simples de código detector de erros são os dois últimos dígitos (dígitos de verificação) do CPF (Cadastro de Pessoa Física), que são função dos nove primeiros dígitos (redundância introduzida).

Seja um número de CPF representado por $c_1c_2c_3.c_4c_5c_6.c_7c_8c_9\text{-}c_{10}c_{11}$, com $c_i \in \{0, 1, \ldots, 9\}$, $\forall i = 0, 1, \ldots, 11$. Para a determinação de c_{10} em função dos primeiros nove dígitos, atribua os pesos 10, 9, ..., 2 aos dígitos c_1, c_2, ...,c_9, respectivamente e os some:

$$s_{10} = \sum_{i=1}^{9} (11 - i) \cdot c_i$$

Em seguida se obtém o resto r_{10} da divisão de s_{10} por 11.

Caso $r_{10} < 2$, c_{10} recebe o valor 0. Caso contrário, $c_{10} = 11 - r_{10}$.

Para o segundo dígito, atribua agora os pesos 11, 10, ..., 2 aos dígitos c_1, c_2, ..., c_{10}. A partir deste ponto o algoritmo para obtenção de c_{11} é análogo ao da obtenção de c_{10}.

Como será definido no Capítulo 4, códigos são um conjunto de mensagens que carregam algum significado para o receptor. Estas mensagens são construídas sobre um conjunto chamado alfabeto, cujos elementos são denominados símbolos, a menor entidade que pode carregar significado, análogo à formação de palavras na Língua Portuguesa a partir do alfabeto latino.

2.4 INFORMAÇÃO

Apesar de ser peça central em um sistema de comunicação, ainda não definimos o que é informação. Intuitivamente podemos assumir a informação como o significado que alguma mensagem leva à fonte. Entretanto, a Teoria da Informação (ou Teoria Matemática da Comunicação) define informação como uma grandeza mensurável relacionada com a incerteza que a mensagem que a contém dissipa.

Por exemplo, seja um led (diodo emissor de luz) que pode fisicamente emitir as cores vermelho, verde e azul, mas sempre emite apenas a vermelha, por algum motivo. Como esta luz é sempre vermelha, não há incerteza alguma sobre a mensagem transmitida por esse led a ser dissipada: a informação é zero. Entretanto, o resultado do lançamento de um dado honesto sempre transmitirá informação, já que insere dados não previstos.

Seja então um alfabeto $A = \{a_1, ..., a_q\}$ e uma fonte de informação em que $p_1, ..., p_q$ são as probabilidades de $a_1, ..., a_q$ serem transmitidos, respectivamente. A definição matemática para a informação de um símbolo a_i é dada por 2.1.

$$I(a_i) = -log_b(p_i) \tag{2.1}$$

Também definimos a entropia de um símbolo a_i originado pela referida fonte como $H(a_i)$:

$$H(a_i) = -p_i log_b(p_i)$$

Convenciona-se que se $p_i = 0$, então $H(a_i) = 0$.

E a entropia da fonte de informação como a média da informação dos símbolos de A sob esta fonte, ou a soma de suas entropias, em 2.2.

$$H(A) = -\sum_{i=1}^{q} p_i log_b(p_i) \tag{2.2}$$

Definimos a unidade de entropia de um símbolo como nat se escolhermos a base $b = e$, e o número de Euler, bit se escolhermos $b = 2$ e hartley, se $b = 10$. Para a entropia do código, usamos as unidades nat/símbolo, bit/símbolo e hartley/símbolo, respectivamente.

Note que quanto mais uniforme for a distribuição dos p_i's, mais equiprováveis forem os símbolos, então maior a entropia e a incerteza sobre o alfabeto A.

3 CORPOS FINITOS

Este capítulo se destina a definir e enunciar os principais resultados acerca de corpos finitos, tendo como base [3] e [4]. Os resultados aqui discutidos são importantes para lidar com os espaços vetoriais sobre corpos finitos, sobre os quais são construídos os códigos lineares, a serem tratados mais adiante.

3.1 DEFINIÇÕES PRELIMINARES

Definição 3.1.1. Seja $n \in \mathbb{N}\backslash\{0\}$. Definimos o conjunto $[n] \subset \mathbb{N}\backslash\{0\}$ como

$$[n] = \{m \in \mathbb{N}\backslash\{0\};\ m \leq n\}$$

Definição 3.1.2. Seja A um anel. Para todo $n \in \mathbb{N}$ e todo $a \in A$, definimos $\underline{na}$ ou $\underline{n \cdot a}$ em A como

$$na = \begin{cases} \underbrace{a + a + ... + a}_{n \text{ parcelas}} & \text{, se } n > 0 \\ 0 & \text{, se n=0} \\ \underbrace{(-a) + (-a) + ... + (-a)}_{|n| \text{ parcelas}} & \text{, se } n < 0 \end{cases}$$

Definição 3.1.3. Seja A um anel. Definimos a $\underline{\text{característica de } A}$ como $char(A)$:

$$char(A) = \begin{cases} n = min\{k \in \mathbb{N} \setminus \{0\}; ka = 0, \forall a \in A\}, \text{ caso exista tal } n \\ 0, \text{ caso não exista} \end{cases}$$

Proposição 3.1.4. Seja A um anel com unidade.

a) Se $n \cdot 1 \neq 0$, $\forall n \in \mathbb{N}$, então $char(A) = 0$

b) Se existe $n \in \mathbb{N}$ tal que $n \cdot 1 = 0$, então $char(A) = min\{n \in \mathbb{N}; n \cdot 1 = 0\}$

Demonstração.

a) Suponha que exista $mchar(A) > 0$. Então $m \cdot 1 = 0$, contradição.

b) Sejam $Z_A = \{n \in \mathbb{N};\ n \cdot a = 0,\ \forall a \in A\}$ e $Z_1 = \{m \in \mathbb{N};\ m \cdot 1 = 0\}$. Naturalmente, $Z_A \subset Z_1$.

Seja agora $m \in Z_1$:

$$\begin{aligned} m \cdot a &= \underbrace{a + \ldots + a}_{m \text{ parcelas}} \\ &= \underbrace{1 \cdot a + \ldots + 1 \cdot a}_{m \text{ parcelas}} \\ &= \underbrace{(1 + \ldots + 1)}_{m \text{ parcelas}} \cdot a \\ &= (m \cdot 1) \cdot a \\ &= 0 \cdot a \\ &= 0, \ \forall a \in A \end{aligned}$$

Dessa forma, verificamos que $m \in Z_A$ e, portanto, $Z_1 = Z_A$. Assim,

$$char(A) = min(Z_1) = min\{n \in \mathbb{N};\ n \cdot 1 = 0\}.$$

■

Proposição 3.1.5. Todo domínio de integridade A tem característica 0 ou prima.

Demonstração.

Se $char(A) = 0$, não há o que demonstrar.

Se $char(A) \neq 0$, suponha $r, s \in \mathbb{N}\backslash\{0, 1\}$ tais que $char(A) = rs$.

Então,

$$\begin{aligned} 0 &= rs \cdot 1 \\ &= (r \cdot 1) \cdot (s \cdot 1) \\ &\Rightarrow r \cdot 1 = 0 \text{ ou } s \cdot 1 = 0 \end{aligned}$$

Logo a característica de A é menor ou igual a r ou s e ambos são menores que rs, contradição.

Portanto, a característica de um domínio de integridade deve ser prima. ■

Corolário 3.1.6. Todo corpo finito possui característica prima.

Demonstração.

Todo corpo é um domínio de integridade, logo, pela proposição anterior, tem característica prima ou nula. Sendo um corpo finito, pela finitude de seus elementos temos que sua característica é não nula. Portanto, todo corpo finito possui característica prima. ■

Definição 3.1.7. Seja $p \in \mathbb{N}\backslash\{0\}$. Chamemos de $\mathbb{Z}_p$ o anel das classes de equivalência módulo p em $\mathbb{Z}$.

$$\mathbb{Z}_p = \{\bar{i};\ i \in [p]\}$$

Teorema 3.1.8. $\mathbb{Z}_p$, conjunto das classes de equivalência de $\mathbb{Z}$ módulo p, é corpo se, e somente se, p é primo.

Demonstração.

Sejam p primo e $s \in [p]$, $s \neq p$. Como $mdc(s,p) = 1$, existem $s, t \in \mathbb{N}\backslash\{0\}$ tais que $rs + tp = 1$. Assim, em $\mathbb{Z}_p$, temos $\overline{rs} = \overline{r} \cdot \overline{s} = \overline{1}$, isto é, existe $\overline{r} \in \mathbb{Z}_p$ tal que $\overline{r} \cdot \overline{s} = \overline{1}$.

Reciprocamente, suponha que $p = rs$, onde $r, s \in \mathbb{N}$, com $1 < r, s \neq p$. Então, $0 = \overline{p} = \overline{rs} = \overline{r}\,\overline{s}$, donde $\mathbb{Z}_p$ possui divisores de zero. Portanto, $\mathbb{Z}_p$ não é corpo se p não for primo. ■

Definição 3.1.9. Denotaremos os corpos finitos com q elementos por $\mathbb{F}_q$. No caso de $\mathbb{Z}_p$, p primo, temos que $\mathbb{Z}_p = \mathbb{F}_p$. Como será visto mais à frente, cada $\mathbb{F}_q$ é único, salvo por isomorfismos.

Definição 3.1.10. Sejam F e K dois corpos tais que $K \subset F$. Dizemos que K é subcorpo de F. Se $K \neq F$, dizemos que K é subcorpo próprio de F.

Exemplo 3.1.11. Seja $\mathbb{F}_3$. Suponha que haja um subcorpo F de dois elementos de $\mathbb{F}_3$.

Para isso, $\overline{0}, \overline{1} \in F$. Porém, $\overline{1} + \overline{1} = \overline{2} \neq \overline{0}$ e $\overline{2} \in \mathbb{F}_3\backslash F$.

Portanto, não há subcorpos próprios de $\mathbb{F}_3$.

Definição 3.1.12. Seja F um corpo. Dizemos que F é um corpo primo se F não contiver subcorpos próprios.

Proposição 3.1.13. Seja F um corpo finito de característica p. Todo subcorpo não-trivial K de F possui também característica p.

Demonstração. Sejam

$$Z_F = \{r \in \mathbb{N} \setminus \{0\}; r \cdot a = 0\, \forall a \in F\}$$

$$Z_K = \{s \in \mathbb{N} \setminus \{0\}; s \cdot b = 0\, \forall b \in K\}$$

Temos que:

$$\begin{aligned} m \in Z_F &\Rightarrow m \cdot a = 0, \forall a \in F \\ &\Rightarrow m \cdot b = 0, \forall b \in K (K \subset F) \\ &\Rightarrow m \in Z_K \\ &\Rightarrow Z_F \subset Z_K \\ &\Rightarrow min(Z_F) \geq min(Z_K) \\ &\Rightarrow char(Z_F) \geq char(Z_K) \\ &\Rightarrow p \geq p' \end{aligned}$$

Mas $p \cdot b = 0$, $\forall b \in K$ e por isso $p' | p$.

Como K é não-trivial e tem característica prima (pois é corpo finito), segue que $char(K) = p$. ■

Proposição 3.1.14. Todo corpo F com $char(F) = p$ contém uma cópia de $\mathbb{F}_p$

Demonstração.

Considere o homomorfismo

$$\begin{aligned} \varphi : \mathbb{F}_p &\to F \\ \bar{i} &\mapsto i1_F, \qquad i \in [p] \end{aligned}$$

Este homomorfismo é injetivo. Sejam i, $j \in [p]$,

$$\bar{i} \neq \bar{j} \Rightarrow i \neq j \Rightarrow \underbrace{(i-j)}_{0<|i-j|<p} 1_F \neq 0_F.$$

Desta forma, φ é isometria entre $\mathbb{F}_\mathrm{p}$ e $\varphi(\mathbb{F}_\mathrm{p})$, donde F contém uma cópia de $\mathbb{F}_\mathrm{p}$. ■

Proposição 3.1.15. O (único) subcorpo primo de um corpo F de característica p, onde p é um número primo, é isomorfo a $\mathbb{F}_p$.

Demonstração. Seja K um subcorpo primo de F. Pelas Proposição 3.1.13, $char(K) = p$ e pela Proposição 3.1.14, K contém uma cópia de $\mathbb{F}_p$. Portanto, K é, ele mesmo, uma cópia de $\mathbb{F}_p$ e, pelo *corolário 3.1.16*, este é o único subcorpo primo possível para qualquer corpo finito F com característica p. ■

Corolário 3.1.16. $\mathbb{F}_\mathrm{p}$ é um corpo primo, se $p \in \mathbb{N} \backslash \{0\}$ for primo.

Demonstração.

De fato, seja $F \subset \mathbb{F}_\mathrm{p}$, $F \neq \{0\}$. Pelo resultado anterior, $char(F) = p = \#\,\mathbb{F}_\mathrm{p}$, levando a $F = \mathbb{F}_\mathrm{p}$. Logo, se $\mathbb{F}_\mathrm{p}$ contém um subcorpo diferente de $\{0\}$, este subcorpo é ele mesmo. ■

Proposição 3.1.17. Sejam F um corpo finito com característica p e $q = p^n$, $n \in \mathbb{N}$. Se $a, b \in F$, então $(a+b)^q = a^q + b^q$.

Demonstração. Temos que

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k}$$

Como p é primo e $k \not| \, p$ para todo $k \neq \pm 1, \pm p$, segue que $p \Big| \binom{p}{k}$ para todo $k \neq \pm 1, \pm p$, donde

$$\binom{p}{k} a^k b^{p-k} = p \cdot (m \cdot a^k b^{p-k}) = 0 \, \forall k \neq \pm 1, \pm p$$
$$\Rightarrow (a+b)^p = a^p + b^p, \; p \text{ primo}$$

Sejam, então, $n \in \mathbb{N}$ e $q = p^n$.

$$\begin{aligned}
(a+b)^q &= (a+b)^{p^n} \\
&= [(a+b)^p]^{p^{n-1}} \\
&= (a^p + b^p)^{p^{n-1}} \\
&= ((a^p)^p + (b^p)^p))^{p^{n-2}} \\
&= (a^{p^2} + b^{p^2})^{p^{n-2}} \\
&= ... \\
&= a^q + b^q
\end{aligned}$$

■

3.2 CARACTERIZAÇÃO DOS CORPOS FINITOS

Proposição 3.2.1. Sejam F e K corpos finitos com $K \subset F$, $\#K = q \in \mathbb{N}$. Então, $\#F = q^m$, onde $m = [F : K]$.

Demonstração. Se F é extensão de K de grau m, então existem $a_1, \ldots, a_m \in F$ tais que F é um espaço vetorial sobre K com base $\mathcal{B} = \{a_i\}_{i=1}^m$.

Por este motivo, para todo $x \in F$, existem únicos $k_1, \ldots, k_m$ tais que

$$x = \sum_{j=0}^{m} k_j a_j, \text{ onde } k_j \in K$$
$$\Rightarrow \#F = \prod_{j=1}^{m} \#K$$
$$\Rightarrow \#F = (\#K)^m$$
$$\Rightarrow \#F = q^m$$

■

Teorema 3.2.2. Sejam F um corpo finito e p a sua característica. Então, F tem p^n elementos para algum $n \in \mathbb{N}\backslash\{0\}$.

Demonstração. Sabemos que F contém um único subcorpo primo F_p isomorfo a $\mathbb{F}_p$ com p elementos. Então, sendo $n = [F : F_p]$, pelo último resultado, $\#F = (\#F_p)^n = p^n$. ■

Proposição 3.2.3. Seja F um corpo finito de cardinalidade q. Então $a^q = a \, \forall a \in F$.

Demonstração. $G = (F\backslash\{0\}, \cdot)$ é um grupo (abeliano) de cardinalidade $q - 1$. Então $a^q = a^{q-1}a = 1 \cdot a = a$. Para $a = 0$, $a^q = 0^q = 0 = a \, \forall n \in \mathbb{N}$. ■

Definição 3.2.4. Sejam K um corpo e $f(x) \in K[x]$. Dizemos que $f(x)$ é fatorável, ou que se fatora, em $K[x]$ se $f(x)$ pode ser escrito como o produto de polinômios de grau 1 como abaixo com c, α_1, ..., $\alpha_n \in K$, n o grau de $f(x)$.

$$f(x) = c \cdot (x - \alpha_1) \dots (x - \alpha_n)$$

Definição 3.2.5. Sejam K e F corpos com F extensão de K. Então F é um corpo de decomposição para o polinômio $f(x) \in K[x]$ se $f(x)$ se fatora em F e todo corpo em que $f(x)$ seja fatorável contém F.

Proposição 3.2.6. Sejam K um corpo finito e F uma extensão finita de cardinalidade q. Então o polinômio $x^q - x \in K[x]$ é fatorável em $F[x]$ na forma

$$x^q - x = \prod_{a \in F} (x - a) \in F[x]$$

Demonstração. O polinômio $x^q - x$ possui no máximo q raízes, mas $a^q = a$, para todos os q elementos $a \in F$. Portanto, $a^q - a = 0 \; \forall a \in F$. Assim,

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

■

Proposição 3.2.7. Sejam K um corpo de cardinalidade q e $f(x) \in K[x]$ de grau d. Seja também o corpo $F = K[x]/\langle f(x) \rangle$, cujos elementos são dados por $\overline{g(x)}$, classes de equivalência de polinômios $g(x) \in K[x]$ sob o quociente $\langle f(x) \rangle$. Então ocorrem as seguintes propriedades:

a) $\{\overline{1}, \overline{x}, ..., \overline{x}^{d-1}\}$ é base de F sobre K.

b) $\overline{x}^{q^d} = \overline{x}$ em F.

c) $f(x) | (x^{q^d} - x)$ em $K[x]$.

d) Os elementos $\overline{1}, \overline{x}^{q^d}, ..., \overline{x}^{q^{d-1}}$ de F são distintos e são raízes de $f(x)$.

Demonstração.

a) De imediato, $\overline{1}$, $\overline{x^2} = \overline{x}^2$, ..., $\overline{x^{d-1}} = \overline{x}^{d-1}$ são LI sobre K.
Como $dim_K(K[x]/\langle f(x)\rangle) = d$, $\{\overline{1}, \overline{x}, ..., \overline{x}^{d-1}\}$ é base de F sobre K.

b) Da Proposição 3.2.3, $\overline{x}^{q^d} = (\overline{x})^{(\#K)^d} = (\overline{x})^{\#F} = \overline{x}$

c) Por (b) $\overline{x}$ é raiz de $x^{q^d} - x$. Como $f(\overline{x}) = \overline{f(x)} = \overline{0}$, segue que $f(x)$ divide $x^{q^d} - x$.

d) Considere o polinômio $g(y)$ fatorável em F como segue,

$$g(y) = (y - \overline{x})(y - \overline{x}^{q^d}) \dots (y - \overline{x}^{q^{d-1}}).$$

Do item (b),

$$\overline{a}^{q^d} = \overline{a},\ \forall a \in K/\langle f(x)\rangle$$

Assim,

$$\begin{aligned} g(y^q) &= (y^q - \overline{x})(y^q - \overline{x}^q) \dots (y^q - \overline{x}^{q^{d-1}}) \\ &= (y^q - \overline{x}^{q^d})(y^q - \overline{x}^q) \dots (y^q - \overline{x}^{d-1}) \end{aligned}$$

Pela proposição 3.1.17:

$$y^q - \overline{x}^{q^m} = y^q - (\overline{x}^{q^{m-1}})^q = (y - \overline{x}^{q^{m-1}})^q$$

Daí,

$$\begin{aligned} g(y^q) &= (y - \overline{x}^{q^{d-q}})^q (y - \overline{x})^q \dots (y - \overline{x}^{q^{d-2}})^q \\ &= (y - \overline{x})^q (y - \overline{x}^q)^q \dots (y - \overline{x}^{q^{d-1}})^q \\ &= g(y)^q \end{aligned}$$

Sejam $b_0, b_1, \dots b_d \in K$;

$$g(y) = \sum_{i=0}^{d} b_i y^i, \quad b_d = 1$$

então, pela generalização da proposição 3.1.17:

$$g(y)^q = (\sum_i b_i y^i)^q = \sum_i (b_i y^i)^q = \sum_i b_i^q y^{iq}$$

Mas como $g(y)^q = g(y^q)$,

$$\sum_i b_i^q y^{iq} = \sum_i b_i y^{iq}$$

Usando a identidade polinomial,

$$b_i^q = b_i, \quad \forall i$$

Como $b_i \in K$, $g(y) \in K[y]$,

$$\begin{aligned} f(\overline{x}) &= \overline{x}^{q^d} - \overline{x} \\ &= \overline{x} - \overline{x} = 0 \\ &\Rightarrow \overline{x} \text{ é raiz de } f \text{ em } F. \\ g(\overline{x}) &= (\overline{x} - \overline{x})(\overline{x} - \overline{x}^q) \dots (\overline{x} - \overline{x}^{q^{d-1}}) \\ &\Rightarrow \overline{x} \text{ é raíz de } g \text{ em } F. \end{aligned}$$

Como f é irredutível em $K[x]$ e $f(x)$ e $g(x)$ possuem raízes comuns em F, então $f(x)\Big|g(x)$. Mas os graus de $f(x)$ e $g(x)$ são iguais e ambos os polinômios são mônicos, portanto $f = g$.

Pela proposição 3.2.6, $x^{q^d} - x$ não possui raízes múltiplas. Como $f = g|(x^{q^d} - x)$, então $\overline{x}^{q^m}$, $m = 0, 1, \dots, d-1$, são todas raízes distintas, por serem raízes de f.

■

Segue da Proposição 3.2.7:

Corolário 3.2.8. Sejam o corpo K de cardinalidade q e o polinômio $f(x) \in K[x]$ irredutível de grau $\delta(f) = d$. Então $d = min\{j \in \mathbb{N}; \overline{x}^{q^j} = \overline{x}\}$ em que $\overline{x} \in K[x]/\langle f(x)\rangle$.

Proposição 3.2.9. Sejam $m, n \in \mathbb{N}\backslash\{0\}$. Então, $(x^m - 1)|(x^n - 1) \iff m|n$.

Demonstração. De fato, pelo algoritmo da divisão,

$$x^n - 1 = (x^m - 1)(x^{n-m} + x^{n-2m} + \dots + x^{n-km}) + (x^{n-km} - 1),$$

onde $n - km$ é o resto da divisão de n por m. Portanto, $x^{n-km} - 1 = 0$ se e somente se $n - km = 0$, isto é, se e somente se n é divisível por m. ■

Lema 3.2.10. Sejam K um corpo e $m, n \in \mathbb{N}\backslash\{0\}$. Temos que

$$mdc(x^m - 1, x^n - 1) = x^{mdc(m,n)} - 1$$

Demonstração. Pela observação anterior, caso $m|n$, $mdc(x^m - 1, x^n - 1) = x^m - 1$ e $m = mdc(m, n)$.

Caso $m \nmid n$, podemos encontrar $r_k = mdc(m, n)$ pelo algoritmo de Euclides:

$$\begin{aligned} n &= m \cdot q_1 + r_1 \\ m &= r_1 \cdot q_2 + r_2 \\ &\dots \\ r_{k-1} &= r_k \cdot q_k + r_{k+1} \\ &\qquad\qquad \text{com } r_{k+1} = 0. \end{aligned}$$

Apliquemos o algoritmo também para os polinômios, encontraremos os mesmos r_i:

$$\begin{aligned} x^n - 1 &= (x^m - 1)Q_1(x) + (x^{r_1} - 1) \\ x^m - 1 &= (x^{r_1} - 1)Q_2(x) + (x^{r_2} - 1) \\ &\dots \\ x^{r_{k-1}} - 1 &= (x^{r_k} - 1)Q_{k+1} + (x^{r_{k+1}} - 1) = x^{r_k}Q_{k+1} \end{aligned}$$

Assim, $mdc(x^n - 1, x^m - 1) = x^{mdc(n,m)} - 1$. ■

Corolário 3.2.11. Sejam K um corpo e $n, m, q \in \mathbb{N}\backslash\{0\}$. Então

$$mdc(x^{q^n} - x, x^{q^m} - x) = x^{q^{mdc(n,m)}} - x$$

Demonstração.

$$\begin{aligned} mdc(x^{q^n} - x, x^{q^m} - x) &= x \cdot mdc(x^{q^n - 1} - 1, x^{q^m - 1} - 1) \\ &= x(x^{mdc(q^n - 1, q^m - 1)} - 1) \\ &= x(x^{q^{mdc(n,m)} - 1} - 1) \\ &= x^{q^{mdc(n,m)}} - x \end{aligned}$$

■

Lema 3.2.12. Sejam $n, m, q \in \mathbb{N}\backslash\{0\}$. Então

$$(x^{q^m} - x) \Big| (x^{q^n} - x) \iff m | n$$

Demonstração.

$$\begin{aligned} (x^{q^m} - x) \Big| (x^{q^n} - x) &\iff (x^{q^m} - x) = mdc(x^{q^m} - x, x^{q^n} - x) \\ &\iff (x^{q^m} - x) = x^{q^{mdc(m,n)}} - x \\ &\iff q^m = mdc(q^m, q^n) \\ &\iff m = mdc(m, n) \\ &\iff m | n \end{aligned}$$

■

Teorema 3.2.13. Sejam K um corpo finito de cardinalidade q e $n \in \mathbb{N}\backslash\{0\}$. Seja $G_d(x)$ é o produto de todos os polinômios mônicos irredutíveis de grau d em $K[x]$. Em $K[x]$ vale a seguinte igualdade:

$$x^{q^n} - x = \prod_{d|n} G_d(x)$$

A demonstração pode ser encontrada em [3].

Definição 3.2.14. Seja K um corpo finito. Definimos $I(n)$ como o número de polinômios mônicos irredutíveis em $K[x]$ de grau n.

Corolário 3.2.15. Seja K um corpo de cardinalidade q. Então

$$q^n = \sum_{d|n} dI(d)$$

Demonstração. De 3.2.13, $q^n = \sum_{d|n} \delta(G_d(x))$.

$$G_d(x) = \prod_{g_i^{(d)} \text{ mônico}} g_i^{(d)}(x)$$

$$\Rightarrow \delta(G_d(x)) = \sum_{i=1}^{I(d)} \delta(g_i^{(d)}(x)) = \sum_{i=1}^{I(d)} (d) = dI(d)$$

$$\therefore\ q^n = \sum_{i=1}^{I(d)} dI(d)$$

■

Teorema 3.2.16. Seja K um corpo de cardinalidade q. Então para todo natural não nulo $n \in \mathbb{N}\backslash\{0\}$, existe f irredutível tal que o grau de $f(x)$ é n.

A demonstração deste teorema pode ser encontrada em [3].

Teorema 3.2.17 (Existência e unicidade de corpos finitos)**.** Para todo p primo e todo inteiro positivo n, existe um corpo finito com p^n elementos. Além disso, todo corpo finito com $q = p^n$ elementos é isomorfo ao corpo de decomposição do polinômio $x^q - x$ sobre $\mathbb{F}_p$.

Demonstração. Sejam $h(x) = x^q - x \in \mathbb{F}_p[x]$ e F um corpo de decomposição de $h(x)$ sobre $\mathbb{F}_p$. Temos que toda raiz de h está em F. Primeiramente, vejamos que h não possui raízes múltiplas. De fato:

$$\frac{dh}{dx}(a) = \underbrace{qa^{q-1}}_{q=p^n} - 1 = 0 - 1 = -1 \neq 0 \tag{3.1}$$

Defina o conjunto $S := \{a \in F; a^q - a = 0\}$. Pelo Teorema Fundamental da Álgebra e pela equação (3.1), temos $\#S = q$.

Ainda, S é subcorpo de F:

a) Temos

$$0^q - 0 = 0 \Rightarrow 0 \in S$$
$$1_F^q - 1_F = 1_F - 1_F = 0 \Rightarrow 1_F \in S$$

b) Sejam $a, b \in S$,

$$\begin{aligned}(a-b)^q - (a-b) &= a^q - b^q - a + b \\ &= (a^q - a) - (b^q - b) \\ &= 0 - 0 = 0 \\ &\Rightarrow a - b \in S\end{aligned}$$

c) Sejam $a, b \in S$, $b \neq 0$,

$$\begin{aligned}(ab^{-1})^q - (ab^{-1}) &= a^q b^{-q} - ab^{-1} \\ &= a^q (b^q)^{-1} \\ &= ab^{-1} - ab^{-1} = 0 \\ &\Rightarrow ab^{-1} \in S\end{aligned}$$

Desta forma, $S = F$, F um corpo finito de $q = p^n$ elementos.

Como já foi visto, existe F' subcorpo de F isomorfo a $\mathbb{F}_p$. Portanto, todo F pode ser visto como uma extensão de F_p. Logo, dois corpos finitos F_1, F_2 tais que $\#F_1 = \#F_2 = p^n$ são isomorfos. ■

Definição 3.2.18. Um elemento α de um corpo $\mathbb{F}_q$ é chamado primitivo se

$$\mathbb{F}_q \backslash \{0\} = \{\alpha^m\}_{m=0}^{q-2}.$$

3.3 EXTENSÕES DE CORPOS FINITOS

Proposição 3.3.1. Seja p um primo. Um corpo F de cardinalidade p^n contém outro, K, de cardinalidade p^m se, e somente se $m|n$. Nesse caso, existe um único subcorpo com esta propriedade e seus elementos são as raízes em F do polinômio $x^{p^m} - x$.

Demonstração. Sejam F, F' corpos tais que $\#F = p^n$, $\#F' = p^m$ e $F' \subset F$. Daí, $F = Z_F(x^{p^n} - x)$ e $F' = Z_F(x^{p^m} - x)$, definindo $Z_F(f) = \{a \in F; f(a) = 0\}$.

$$\begin{aligned}F' \subset F &\iff b \in F, \forall b \in F' \\ &\iff \left(x^{p^n} - x\right)(b) = 0, \forall b \in F; \left(x^{p^m} - x\right)(b) = 0 \\ &\iff (x^{p^m} - x) | (x^{p^n} - x) \\ &\iff m|n\end{aligned}$$

■

Corolário 3.3.2. Sejam $p, q, n, m \in \mathbb{N}\backslash\{0\}$ com p primo e q uma potência inteira de p. O corpo $\mathbb{F}_{q^n}$ contém um subcorpo isomorfo a $\mathbb{F}_{q^m}$ se, e somente se, $m|n$. Neste caso, tal subcorpo é único e seus elementos são raízes de $x^{q^m} - x$ em $\mathbb{F}_{q^m}$.

Demonstração.

$$q = p^k \quad \Rightarrow \quad \begin{cases} \mathbb{F}_{q^n} = \mathbb{F}_{p^{kn}} & \Rightarrow \#\mathbb{F}_{q^n} = p^{kn} \\ \mathbb{F}_{q^m} = \mathbb{F}_{p^{km}} & \Rightarrow \#\mathbb{F}_{q^m} = p^{km} \end{cases}$$

Ambos os corpos são extensões de $\mathbb{F}_p$, portanto

$$\mathbb{F}_{q^m} < \mathbb{F}_{q^n} \iff km|kn \iff m|n$$

■

Proposição 3.3.3. Sejam F um corpo finito, K um subcorpo de F e $\beta \in F$.

a) Se $m = \delta\Big(irr(\beta, K)\Big)$, então $1, \beta, \ldots, \beta^{m-1}$ é uma base de $K(\beta)$ sobre K. Em particular, $[K(\beta) : K] = m$.

b) Se K possui q elementos, então $\beta^{q^m} = \beta$ e $\beta^{q^i} \neq \beta^{q^j}$ para $i, j = 0, 1, \ldots, m-1$, $i \neq j$.

c) Existe $\alpha \in F$ tal que $F = K(\alpha)$.

Demonstração.

a) Temos:

$$\begin{aligned} \delta(\beta, K) = m \Rightarrow \sum_{k=0}^{m-1} c_k \beta^k \neq & \text{ desde que } c_k \neq 0 \text{ paa algum } k. \\ \Rightarrow \{\beta^k; k = 0, 1, \ldots, m-1\} & \text{ é base de } K(\beta). \\ \#\{\beta^k; k = 0, 1, \ldots, m-1\} = [K(\beta) : K] &= m \end{aligned}$$

b) Esta demonstração está inteiramente baseada nos itens *b)* e *c)* da *Proposição 3.2.7*:

$K(\beta) == K[x]/\langle f(x)\rangle$, com $f(x) = irr(\beta, K)$ e com isomorfismo $\psi : K[x]/\langle f(x)\rangle \to K(\beta)$:

$$\psi\Big(\sum_{k=0}^{m-1} a_k \overline{(x)}^k\Big) = \sum_{k=0}^{m-1} a_k \beta^k$$

Este isomorfismo está bem definido, uma vez que ambos são espaços vetoriais de mesma dimensão sobre o mesmo corpo e

$$\overline{x}^{k_1} \cdot \overline{x}^{k_2} = \overline{x}^{k_1+k_2} = \psi^{-1}\Big(\beta^{k_1+k_2}\Big) = \psi^{-1}\Big(\beta^{k_1}\Big) \cdot \psi^{-1}\Big(\beta^{k_2}\Big)$$

Assim, da *Proposição 3.2.7.b)*,

$$\begin{aligned} \overline{x}^{q^m} &= \overline{x} \\ &\Rightarrow \psi\Big(\overline{x}^{q^m}\Big) = \psi(\overline{x}) \\ &\beta^{q^m} = \beta \end{aligned}$$

Além disso, da *Proposição 3.2.7.d)*, para $0 \leq i < j < m$

$$\begin{aligned} \overline{x}^{q^j} \neq \overline{x}^{q^i} &\Rightarrow \psi\Big(\overline{x}^{q^j}\Big) \neq \psi\Big(\overline{x}^{q^i}\Big) \\ &\Rightarrow \beta^{q^j} \neq \beta^{q^i} \end{aligned}$$

Mais,

$$\begin{aligned} f(x) &= (x-\overline{x})(x-\overline{x}^q)\dots(x-\overline{x}^{q^{m-1}}) \\ \Rightarrow \psi(f(x)) &= \psi\Big((x-\overline{x})(x-\overline{x}^q)\dots(x-\overline{x}^{q^{m-1}})\Big) \\ &= (x-\beta)(x-\beta^q)\dots(x-\beta^{q^{m-1}}) \end{aligned}$$

c) Seja α um elemento primitivo de F. Como $\forall b \in F$ existe k tal que $\alpha^k = \beta$, então $K(\alpha) = F$, $\forall K < F$.

■

3.4 RAÍZES DA UNIDADE

Definição 3.4.1. Seja $\alpha \in F$, F corpo, raiz de $x^n - 1$. Dizemos que α é uma raiz n-ésima da unidade.

Proposição 3.4.2. Sejam F um corpo de cardinalidade q e $n \in \mathbb{N}\backslash\{0\}$ tal que $n|(q-1)$. Então existe um elemento $\gamma \in F$ tal que

$$x^n - 1 = (x-1)(x-\gamma)(x-\gamma^2)\dots(x-\gamma^{n-1})$$

onde $1, \gamma, \dots, \gamma^{n-1}$ são elementos distintos entre si.

Demonstração. Seja α um elemento primitivo de F e $\gamma = \alpha^m$, $m = \frac{q-1}{n}$. Então $\gamma^n = \alpha^{fracq-1nn} = \alpha^{q-1} = 1$. Ou seja, γ é raiz de $x^n - 1$.

Tome agora γ^j, γ^i, $0 \leq i < j < n$.

$$\begin{aligned} (\gamma^j)^n = (\gamma^n)^j = 1^j = 1, \text{ ok, e} \\ \gamma^j - \gamma^i = \gamma^i(\gamma^{j-i} - 1), \\ Seja \gamma^i \neq 0, \\ \gamma^{j-i} - 1 = \alpha^{m\cdot(j-i)} = \alpha^{fracq-1n(j-i)} \end{aligned}$$

Como $0 < \frac{q-1}{n}(j-i) < q-1$,

$$\begin{aligned}\gamma^{j-i} = \alpha^{\frac{q-1}{n}(j-i)} &\in F\backslash\{1,0\}\\ &\Rightarrow \gamma^{j-i} - 1 \neq 0\\ &\Rightarrow \gamma^i(\gamma^{j-i}-1) = \gamma^j - \gamma^i \neq 0\\ &\Rightarrow \gamma^j = \gamma^i, 0 \leq i < j < n\end{aligned}$$

$\therefore 1, \gamma. \ldots . \gamma^{n-1}$, com $\gamma = \alpha^{\frac{q-1}{n}}$, são raízes distintas de $x^n - 1$.

■

Corolário 3.4.3. Seja K um corpo de cardinalidade q e n um número positivo tal que $mdc(q,n) = 1$. Então existem uma extensão $F \supset K$ e uma elemento $\gamma \in F$ tais que

$$x^n - 1 = (x-1)(x-\gamma)\ldots(x-\gamma^{n-1})$$

com $1, \gamma, \ldots, \gamma^{n-1}$ dois a dois distintos.

Demonstração.

$$K = Z(x^q - 1), n > 1$$

$$\begin{aligned}mdc(q,n) = 1 &\Rightarrow mdc(x^q-1, x^n-1) = x-1\\ &\Rightarrow x^n - 1 \text{ possui raízes fora de } K.\\ &\Rightarrow \exists F \supset K;\ Z(x^n-1) \subset F,\ \#F = q^m \text{ para algum } m \in \mathbb{N}\backslash\{0\}.\end{aligned}$$

Escolha $m; n\Big|(q^m - 1)$.

Isto ocorre porque $mdc(q,n) = 1$, então $\overline{q} \in \mathbb{Z}_n$ é inversível.

Desta forma, através da proposição anterior, $\exists \gamma \in F;\ 1, \gamma, \ldots, \gamma^{n-1}$ são raízes distintas de $x^n - 1$.

■

Observação 3.4.4. Se m for o menor inteiro para o qual $q^m \equiv 1(modn)$, então $\mathbb{F}_{q^m}$ é o menor corpo em que $x^n - 1$ se fatora.

Definição 3.4.5. Sejam $\mathbb{F}_{q^m}$ o menor corpo onde $x^n - 1$ se fatora. Chamamos tal corpo de corpo de raízes de $x^n - 1$.

Observação 3.4.6. Se n e $p = char(K)$ são primos entre si, podemos escrever $n = n'p^r$, para os quais $mdc(n,p) = 1$. Assim, $x^n - 1 = (x^n - 1)^{p^r}$, de forma que α é uma raiz n-ésima da unidade se, e somente se, α pe uma raiz n'-ésima da unidade.

Definição 3.4.7. Uma raiz n-ésima da unidade que não é raiz m-ésima da unidade para nenhum $m < n$ será chamada de raiz n-ésima primiticva da unidadde.

4 CÓDIGOS

Neste capítulo serão apresentados os fundamentos matemáticos para a utilização de códigos, em especial os códigos lineares, tendo como base [4].

4.1 MÉTRICA DE HAMMING

Definição 4.1.1. Um alfabeto A é um conjunto com um número finito de elementos.

Definição 4.1.2. Um código corretor de erros é um subconjunto próprio de A^n, para algum número natural n.

Definição 4.1.3. Dados dois elementos u e v em A^n, definimos a distância de Hamming entre eles como

$$d(u,v) = \#\{i;\ u_i \neq v_i,\ i \in [n]\}$$

Proposição 4.1.4. A distância de Hamming é uma métrica

Demonstração.

i)
$$d(u,v) \in \mathbb{N}\backslash\{0\},\ \forall u,v \in A^n \Rightarrow d(u,v) \geq 0,\ \forall u,v \in A^n$$

ii)
$$\begin{aligned} d(u,v) &= \#\{i;\ u_i \neq v_i,\ i \in [n]\} \\ &= \#\{i;\ v_i \neq u_i,\ i \in [n]\} \\ &= d(v,u) \end{aligned}$$

iii) Defina S:

$$\begin{aligned} S : A^n \times A^n :&\to \mathcal{P}([n]) \\ (u,v) &\mapsto \{i;\ u_i \neq v_i,\ i \in [n]\} \end{aligned}$$

de modo que $d(u,v) = \#S(u,v)$.

Daí, sejam $u,v,w \in A^n$.

$$\begin{aligned} i \in S(u,v) &\Rightarrow u_i \neq v_i \Rightarrow u_i \neq w_i \text{ ou } v_i \neq w_i \\ &\Rightarrow i \in S(u,w) \text{ ou } i \in S(v,w) \\ &\Rightarrow S(u,v) \subset S(u,w) \cup S(v,w) \\ &\Rightarrow \#S(u,v) \leq \#\Big(S(u,w) \cup S(v,w)\Big) \leq \#S(u,w) + \#S(v,w) \\ &\therefore d(u,v) \leq d(u,w) + d(v,w),\ \forall u,v,w \in A^n \end{aligned}$$

■

Definição 4.1.5. SEjam $a \in A^n$ e $r \in [n]$. Chamamos de disco e esfera, respectivamente, os conjuntos $D(a,r)$ e $S(a,r)$:

$$D(a,r) = \{u \in A^n;\ d(a,u) \leq r\}$$
$$S(a,r) = \{u \in A^n;\ d(a,u) = r\}$$

Lema 4.1.6. Para todo $a \in A$ e para todo $r \in [n]$, temos que

$$\#D(a,r) = \sum_{i=0}^{r} \binom{n}{i} (q-1)^i$$

Demonstração. É imediato que i é a união disjunta $D(a,r) = \bigcup_{i=0}^{r} S(a,i)$. Daí,

$$\#D(a,r) = \sum_{i=0}^{r} \#S(a,i)$$

Em partes, consideremos o número de coordenadas distintas entre $b \in S(a,i)$ e a. Há $\binom{n}{i}$ possíveis conjuntos de n-uplas com i coordenadas distintas entre a e b. Note que este não é o número total de elementos com i coordenadas distintas em relação a a. Fixando as coordenadas $b_{l_1}, b_{l_2}, \ldots, b_{l_i}$ diferentes de $a_{l_1}, a_{l_2}, \ldots, a_{l_i}$, respectivamente, e $b_j = a_j$, $\forall j \neq l_t$, $t \notin [i]$, temos a possibilidade de $q-1$ elementos para cada a_{l_t}.

Desta forma,

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

$$\therefore \#D(a,r) = \sum_{i=0}^{r} \binom{n}{i} (q-1)^i$$

■

Definição 4.1.7. Definimos a distância mínima de C, código, como

$$d = min\{d(u,v);\ u,v \in C,\ u \neq v\}$$

e também κ, a capacidade de correção de C, número máximo de erros que C pode corrigir.

$$\kappa = int\left(\frac{d-1}{2}\right)$$

em que $int(x)$ é a parte inteira de x.

Definição 4.1.8. Dizemos que a terna (n, M, d) são os parâmetros fundamentais de um código C de A^n, se reprentarem, na ordem, o comprimento de cada palavra de C, o número de elementos do código e sua distância mínima.

Definição 4.1.9. Dizemos que C é perfeito se

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

4.2 EQUIVALÊNCIA DE CÓDIGOS

Definição 4.2.1. Seja $n \in \mathbb{N}$. Dizemos que uma aplicação $F : A^n \to A^n$ é uma isometria de A^n se ela preserva distâncias de Hamming, ou seja,

$$d\Big(F(u), F(v)\Big) = d(x, y),\ \forall u, v \in A^n$$

Proposição 4.2.2. Toda isometria de A^n é uma aplicação bijetora.

Demonstração.

Sejam $x, y \in A^n$, $F : A^n \to A^n$ isometria. Suponha $F(x) = F(y)$.

$$0 = d\Big(F(x), F(y)\Big) = d(x, y) \Rightarrow x = y \Rightarrow F \text{ é injeção}$$

Como F é uma injeção de um conjunto finito sobre si mesmo, F é uma bijeção. ■

Proposição 4.2.3. Sejam F, G isometrias de A^n e $Id : A^n \to A^n$ a aplicação identidade. Então:

a) Id é uma isometria de A^n

b) F^{-1} é uma isometria de A^n

c) $F \circ G$ é uma isometria de A^n

Demonstração.

a) $d(x, y) = d\Big((Id(x), Id(y)\Big)$

b) Para todo $a, b \in A^n$, existem $x, y \in A^n$ tais que $a = F(x)$, $b = F(y)$. Então,

$$\begin{aligned} d(a, b) &= d\Big(F(x), F(y)\Big) \\ &= d(x, y) \\ &= d\left(F^{-1}\Big(F(x)\Big), F^{-1}\Big(F(y)\Big)\right) \\ &= d\Big(F^{-1}(a), F^{-1}(b)\Big) \end{aligned}$$

c) Sejam $x, y \in A^n$, F, G isometrias de A^n,

$$d(x, y) = d\Big(F(x), F(y)\Big) = d\Big(G(F(x)), G(F(y))\Big)$$

$$\therefore d(x, y) = d\Big(G \circ F(x), G \circ F(y)\Big),\ \forall x, y \in A^n$$

■

Definição 4.2.4. Dados C e C' códigos de A^n dizemos que eles são equivalentes se houver $F : A^n \to A^n$ isometria tal que $F(C) = C'$.

Proposição 4.2.5. A equivalência de códigos é uma relação de equivalência.

Demonstração.

a) A aplicação identidade $Id : A^n \to A^n$ é uma isometria. Como $Id(C) = C$, podemos afirmar que C é equivalente a si mesmo.

b) Sejam C e C' códigos tais que C é equivalente a C'. Então existe uma isometria T de A^n tal que $T(C) = C'$. Aplicando T^{-1}, $T^{-1}T(C) = T^{-1}(C)$, logo $T^{-1}(C') = C$. Sendo T^{-1} também uma isometria, podemos afirmar que C' é equivalante a C.

c) Sejam C, C', C'' códigos de A^n tais que C é equivalente a C' e C' é equivalente a C'' sob as isometrias T e S de A^n, respectivamente: $T(C) = C'$ e $S(C') = C''$. Então $C'' = S(T(C)) = S \circ T(C)$. Como a composição de isometrias é uma isometria, podemos afirmar que C é equivalente a C''.

■

Proposição 4.2.6. Dois códigos equivalentes possuem os mesmos parâmetros.

Demonstração. De fato, se dois códigos C e C' estão contidos em A^n, seus comprimentos são, necessariamente, n. Se estes códigos forem equivalentes, existe uma isometria (bijeção) de A^n que leva um ao outro e, por serem finitos, devem possuir a mesma cardinalidade M. Por fim, como existe uma isometria, a distância mínima d é expressa por

$$\begin{aligned} d &= min\{d(x,y);\ x,y \in C\} \\ &= min\{d(Tx,Ty);\ x,y \in C\} \\ &= min\{(a,b);\ a,b \in C'\} \end{aligned}$$

■

Definição 4.2.7. Sejam π uma permutação de $[n]$ e f uma aplicação de A e $u \in A^n$, $u = (u_1, \ldots, u_n)$. Definamos as aplicações T_π e T_f^j de A^n abaixo:

$$T_\pi(u) = (u_{\pi(1}, \ldots, u_{\pi(n)})$$

$$T_f^j(u) = (u_1, \ldots, u_{j-1}, f(u_j), u_{j+1}, \ldots, u_n)$$

Teorema 4.2.8. Seja $T : A^n \to A^n$ uma isometria. Então existem uma permutação π de $[n]$ e bijeções f_i, $i \in [n]$, de A^n tais que $T = T_\pi \circ T_{f_1}^1 \circ T_{f_2}^2 \circ \ldots T_{f_n}^n$

Demonstração. Sejam T uma isometria de A^n, $a, z \in A$, $e_i = (z, \ldots, z, \underbrace{a}_{i}, z, \ldots, z)$ e $o = (z, \ldots, z)$, com $T(o) = (z'_1, \ldots, z'_n)$.

$$d(Te_i, To) = d(e_i, o) = 1 \Rightarrow Te_j = (z'_1, \ldots, z'_{\pi(i)-1}, \underbrace{b}_{\pi(i)}, z'_{\pi(i)+1}, \ldots, z'_n)$$

Para e_j análogo a e_i:

$$d(Te_j, To) = d(e_j, o) = 1 \Rightarrow Te_i = (z'_1, \ldots, z'_{\pi(j)-1}, \underbrace{b'}_{\pi(j)}, z'_{\pi(j)+1}, \ldots, z'_n)$$

Num primeiro momento queremos mostrar que π é uma permutação sobre $[n]$. A seguir iremos mosrtrar que f_i e f_j são bijeções aplicadas sobre as coordenadas i e j, respectivamente.

Para o primeiro caso, tomemos e_i, e_j, Te_i e Te_j com $i \neq j$:

$$\begin{aligned} d(Te_i, Te_j) &= d(e_i, e_j) = 2 \\ &\Rightarrow \pi(i) \neq \pi(j),\ \forall i \neq j \\ &\Rightarrow \pi \text{ é uma permutação.} \end{aligned}$$

Para a segunda parte, sejam $\alpha, \beta \in A$, $\alpha \neq \beta$ e considere αe_i como a palavra e_i apresentada, trocando o elemento a por α:

$$d\Big(T(\alpha e_i), T(\beta e_i)\Big) = 1$$

Então, tratando a $\pi(i)$-ésima coordenada de $T(\alpha e_i)$ como uma função f_i da i-ésima coordenada da palavra de entrada, $f_i(\alpha) \neq f_i(\beta)$, se $\alpha \neq \beta$. Logo f_i é injeção de A sobre si mesmo e, então, f_i é uma bijeção.

Basicamente, o que fizemos até agora foi mostrar que $T\Big|_{\{xe_i;\, x \in A\}} = T_\pi \circ T^i_{f_i}$, com f_i bijeção. Isso é importante, pois deixa claro que a coordenada $\pi(i)$ de $T(u)$ é função exclusiva de u_i.

Desta forma,

$$T(u) = (f_{\pi(1)}(u_{\pi(1)}), \ldots, f_{\pi(n)}(u_{\pi(n)})) \tag{4.1}$$

$$\therefore T = T_\pi \circ T^1_{f_1} \circ T^2_{f_2} \circ \ldots \circ T^n_{f_n}$$

■

Corolário 4.2.9. Sejam C e C' dois códigos de A^n. Temos que C e C' são equivalentes se, e somente, existem uma permutação π de $[n]$ e bijeções f_i, $i \in [n]$ de A tais que

$$C' = \{(f_{\pi(1)}(u_{\pi(1)}), \ldots, f_{\pi(n)}(u_{\pi(n)}));\ (u_1, \ldots, u_n) \in C\}$$

Demonstração. Se C e C' são equivalentes, existem uma isometria T entre estes códigos. Do teorema anterior, na equação (4.1), existe uma expressão dessa isometria componente a componente como proposto no enunciado com as bijeções f_i. ■

Proposição 4.2.10. Dois códigos de comprimento n sobre um alfabeto A são equivalentes se, e somente se, um deles pode ser obtido do outro mediante uma sequência de operações dos tipos:

a) Substituição das letras numa dada posição fixa em todas as palavras do código por meio de uma bijeção de A.

b) Permutação das posições das letras em todas as palavras do código, mediante uma permutação fixa de $[n]$.

Demonstração. Estes passos estão implícitos no *Teorema 4.2.8* e no *Corolário 4.2.9*: as bijeções f_i são o primeiro passo: cada isometria $T^i_{f_i}$ substitui uma posição fixa em todas as palavras por meio da própria bijeção f_i. Por fim, se faz a permutação das posições por meio de T_π. ■

4.3 CÓDIGOS LINEARES

Definição 4.3.1. Um código $C \subseteq K^n$, K corpo, será chamado de código linear se for um subespaço vetorial de K^n.

Por se tratar de um espaço vetorial, podemos descrever um código C por sua base $\mathcal{B} = \{\alpha_1, \alpha_2, ..., \alpha_k\}$, resultando em $dim_K C = k$.

Desta forma,

$$C = \{\alpha_1 v_1 + \alpha_2 v_2 + ... + \alpha_k v_k;\ \alpha_i \in K,\ v_i \in \mathcal{B},\ \forall i = 1, 2, ..., k\}$$

donde $\#C = \prod_{i=0}^{k} \#K = \#K^k$, isto é, $\#C = (\#K)^{dim_K C}$.

Definição 4.3.2. Seja $u \in K^n$. Definimos o suporte de u como

$$supp(u) = \{i;\ u_i \neq 0\}$$

Definição 4.3.3. Seja $u \in K^n$. Definimos o peso (de Hamming) de u como $w(u)$:

$$w(u) = \#supp(u) = \#\{i; u_i \neq 0\}$$

Dependendo do contexto também podemos utilizar w_H para enfatizar que se trata do peso de Hamming.

Proposição 4.3.4. $w(u) = d(u, 0), \forall u \in K^n$

Demonstração.

$$\begin{aligned} w(u) =& \#\{i; u_i \neq 0\} \\ =& \#\{i; u_i - 0 \neq 0\} \\ =& d(u_i, 0) \end{aligned}$$

■

Definição 4.3.5. Seja C um subconjunto de K^n. Defina o suporte de C como

$$supp(C) = \bigcup_{u \in C} supp(u)$$

Definição 4.3.6. O peso de Hamming de um código linear C é

$$w(C) := min\{w(u); u \in C \backslash \{0\}\}$$

Proposição 4.3.7. Seja $C \subset K^n$ um código linear com distância mínima d. Temos que

a) Para quaisquer $x, y \in K^n$, temos $d(x, y) = w(x - y)$

b) $d = w(C)$

Demonstração.

a) Sejam $x, y \in K^n$, temos:

$$\begin{aligned} d(x, y) &= \#\{i; x_i \neq y_i\} \\ &= \#\{i; x_i - y_i \neq 0\} \\ &= w(x - y) \end{aligned}$$

b) Sejam $x, y \in C$ tais que $w(x - y) = d(x, y) = d$.

Assim, existe $z = x - y \in C$, pois C é linear. Logo, existe $zinC$ tal que

$$w(z) = d \tag{4.2}$$

Seja $s \in C$ tal que $w(s) = w(C)$. Então:

$$w(s) = min\{w(u); u \in C\} = min\{d(u, 0); u \in C\} \geq d$$

De (4.2), segue que $w(s) \leq d$, donde $w(C) = d$.

■

Definição 4.3.8. Seja $K = \mathbb{F}_q$ um corpo finito. Dois códigos lineares C e C' são ditos linearmente equivalentes se houver uma isometria linear T de K^n em K^n, tal que $T(C) = T(C')$.

Proposição 4.3.9. Dois códigos lineares C e C' são linearmente equivalentes se, e somente se, C pode ser obtido de C', e C' a partir de C, via operações descritas abaixo:

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

b) Permutação das posições de todas as palavras do cógido, mediante uma permutação fixa de $[n]$.

Demonstração. Análoga à Proposição 4.2.10. ■

4.4 MATRIZ GERADORA DE UM CÓDIGO

Definição 4.4.1. Definimos como parâmetros de um código linear C a terna (n, k, d), em que k é a dimensão de C sobre $\mathbb{F}_q$, d é a distância mínima de C e n é o comprimento de um vetor em C.

Definição 4.4.2. Seja C um código linear de sobre $\mathbb{F}_q^n$ de dimensão k. Dizemos que C é um código $[n, k]_q$.

Definição 4.4.3. Sejam $C \subset \mathbb{F}_q^n$ um código linear e $\mathcal{B} = \{v^{(1)}, \ldots, v^{(k)}\}$ uma base ordenada de C. A matriz G construída abaixo é chamada de matriz geradora de C associada à base $\mathcal{B}$

$$G = [v^{(1)} \ldots v^{(k)}] = \begin{bmatrix} v_1^{(1)} & \ldots & v_1^{(k)} \\ v_2^{(1)} & \ldots & v_2^{(k)} \\ \vdots & \ldots & \vdots \\ v_n^{(1)} & \ldots & v_n^{(k)} \end{bmatrix} \tag{4.3}$$

Definição 4.4.4. Dizemos que uma matriz geradora G de um código $C \subset \mathbb{F}_q^n$ de dimensão k está na forma padrão se $G = \begin{bmatrix} Id_k \\ A \end{bmatrix}$, sendo Id_k a matriz identidade k por k e A é uma matriz de ordem $(n-k)$ por k.

Observação 4.4.5. A notação matricial adotada neste texto é a de que os vetores são colunas. Então o vetor $u = (u_1, \ldots, u_n) \in \mathbb{F}_q^n$ tem representação matricial $u = \begin{bmatrix} u_1 \\ \vdots \\ u_n \end{bmatrix}$.

Como é possível observar, a matriz geradora de um código linear é a matriz geradora de um subespaço vetorial. Dessa forma é possível construir o isomorfismo $\phi_G : \mathbb{F}_q^k \to C$ a seguir.

Definição 4.4.6. Seja C um código linear em $\mathbb{F}_q^n$ com dimensão k. Definimos o isomorfismo gerador de C associada a matriz geradora G como $\phi_G : \mathbb{F}_q^k \to C$ em que:

$$\phi_G(u) = G \cdot u$$

Como C é um subespaço vetorial e G sua matriz geradora, segue ϕ_G é uma isometria com $\phi_G(e_i) = v^{(i)}$, sendo $\{e_i\}_{i=1}^k$ a base canônica de $\mathbb{F}_q^k$.

4.5 CÓDIGOS DUAIS

Definição 4.5.1. Sejam $u = (u_1, \ldots, u_n)$ e $v = (v_1, \ldots, v_n)$ elementos de $\mathbb{F}_q^n$. Definimos o produto interno de u e v como sendo

$$\langle u, v \rangle = \sum_{i=0}^{n} u_i v_i,$$

com as propriedades usuais de produto interno (exceto $\langle u, u \rangle \geq 0$).

Definição 4.5.2. Sejam C um código linear. Definimos o seu código dual como

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

Lema 4.5.3. Seja $C \subset \mathbb{F}_q^n$ um código linear com matriz geradora G. Então

a) $C^\perp$ é um subespaço vetorial de $\mathbb{F}_q^n$;

b) $u \in C^\perp \iff u^T G = 0$.

Demonstração.

a) Note que $\langle 0, v \rangle = 0$ para todo elemento v de $\mathbb{F}_q^n$. Então $C^\perp$ nunca é vazio.
Sejam $u, u' \in C^\perp$ e $\alpha \in \mathbb{F}_q$ e $v \in C$.

$$\langle \alpha u + u', v \rangle = \alpha \langle u, v \rangle + \langle u', v \rangle = \alpha \cdot 0 + 0 \Longrightarrow \alpha u + u' \in C^\perp$$

b) Seja $u \in \mathbb{F}_q^n$. A i-ésima coordenada do produto $u^T G$ é dada por

$$u^T \cdot v^{(i)} = \langle u, v^{(i)} \rangle$$

Este resultado é nulo para todo i se, e somente se, $u \in C^\perp$.

■

Proposição 4.5.4. Sejam $C \in \mathbb{F}_q^n$ um código linear de dimensão k e matriz geradora na forma padrão $G = \begin{bmatrix} Id_k \\ A \end{bmatrix}$. Então,

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

b) $H = \begin{bmatrix} -A^T \\ Id_{n-k} \end{bmatrix}$ é uma matriz geradora de $C^\perp$.

Demonstração. a) Seja $u = [u_1, u_2, \ldots, u_n]^T \in \mathbb{F}_q^n$. Como vimos, $u \in C^\perp \iff u^T G = 0_{1,k}$. Desta forma,

$$\begin{aligned} u \in C^\perp &\iff \begin{bmatrix} u_1, \ldots, u_k, u_{k+1}, \ldots, u_n \end{bmatrix} \begin{bmatrix} Id_k \\ A \end{bmatrix} \\ &= \begin{bmatrix} u_1, \ldots, u_k \end{bmatrix} Id_k + \begin{bmatrix} u_{k+1}, \ldots, u_n \end{bmatrix} A \\ &= 0 \\ &\iff \begin{bmatrix} u_1, \ldots u_k \end{bmatrix} = \begin{bmatrix} u_{k+1}, \ldots, u_n \end{bmatrix} (-A) \end{aligned} \tag{4.4}$$

Note que para quaisquer valores de $u_{k+1}, \ldots, u_n$ existem valores únicos de $u_1, \ldots, u_k$ assegurando a consistência da equação (4.4). Por isso, podemos concluir que há exatamente q^{n-k} escolhas atendendo a $u \in C^\perp$, ou seja, $\#C^\perp = q^{n-k}$. Como $C^\perp$ é espaço vetorial sobre $\mathbb{F}_q^n$, temos

$$\begin{aligned} \#C^\perp &= (\#F_q)^{dim(C^\perp)} \\ q^{n-k} &= q^{dim(C^\perp)} \\ &\Rightarrow dim(C^\perp) = n - k \end{aligned}$$

b) Já que que $dim(C^\perp) = n - k$ e sabendo que as colunas da matriz H proposta são LI (por conta de Id_k), então basta mostrar que todas as suas colunas são ortogonais às de G.

Seja $h_j^T = v^T = [-a_{j,1} \ldots - a_{j,n-k} 0 \ldots \underbrace{1}_{j} \ldots 0]$. Tome o produto interno da j-ésima coluna de H com a i-ésima coluna de G:

$$\langle h_j, g_i \rangle = (a_{j,i}) \cdot 1 + 1 \cdot (-a_{j,i}) = 0$$

Portanto H é a matriz geradora de $C^\perp$.

■

Lema 4.5.5. Seja C um código linear em F_q^n. Para toda permutação σ de $[n]$, todo $\lambda \in F_q$ e todo $j \in [n]$ temos que

a) $T_\sigma(C)^\perp = T_\sigma(C^\perp)$

b) $T_\lambda^j(C)^\perp = T_{\lambda^{-1}}^j(C^\perp)$, onde
$T_\lambda^j\Big((u_1, \ldots, u_{j-1}, u_j, u_{j+1}, \ldots, u_n)\Big) = \Big((u_1, \ldots, u_{j-1}, \lambda u_j, u_{j+1}, \ldots, u_n)\Big)$

Demonstração.

a) Sejam $x' = T_\sigma(x)$, $x \in C^\perp$ e $c' = T_\sigma(c)$, $c \in C$.

Então, lembrando que toda permutação é uma bijeção,

$$\begin{aligned}
\langle x', c' \rangle &= \sum_{i=0}^{n} x'_i c'_i \\
&= \sum_{i=0}^{n} x_{\sigma^{-1}(i)} c_{\sigma^{-1}(i)} \\
&= \sum_{j=0}^{n} x_j c_j \\
&= 0 \\
&\Rightarrow x' \in T_\sigma(C)^\perp \\
&\Rightarrow T_\sigma(C^\perp) \subseteq T_\sigma(C)^\perp
\end{aligned}$$

Tome agora $y \in T_\sigma(C)^\perp$. Para $c' = T_\sigma(c)$, $c \in C$:

$$\begin{aligned}
0 &= \langle y, c' \rangle \\
&= \sum_{i=0}^{n} y_i c_{\sigma^{-1}(i)} \\
&= \sum_{i=0}^{n} y_{\sigma^{-1}(i)} c_{\sigma^{-1}(i)} \\
&= \sum_{j=0}^{n} y''_j c_j, \qquad y = T_\sigma(y'') \\
&\Rightarrow y'' \in C^\perp \\
&\Rightarrow y \in T(C^\perp) \\
&\Rightarrow T_\sigma(C)^\perp \subseteq T(C^\perp)
\end{aligned}$$

Portanto, $T_\sigma(C)^\perp = T(C^\perp)$

b) Sejam $x \in C^\perp$, $x' = T_{\lambda^{-1}}^j(x)$, $c' = T_\lambda^j(c)$, $c \in C$.

$$\begin{aligned}\langle x', c'\rangle &= \sum_{i\in[n]\setminus\{j\}} x_i c_i + \lambda x_j \lambda^{-1} c_j \\ &= \sum_{i\in[n]} x_i c_i \\ &= 0 \\ &\Longrightarrow x' \in T_\lambda^j(C)^\perp \Rightarrow T_{\lambda^{-1}}^j(C^\perp) \subseteq T_\lambda(C)^\perp\end{aligned}$$

Sejam agora $y \in T_\lambda^j(C)^\perp$, $c' = T_\lambda^j(c)$, $c \in C$.

$$\begin{aligned}0 &= \langle y, c'\rangle \\ &= \langle y, T_\lambda^j(c)\rangle \\ &= \sum_{i\in[n]\setminus\{j\}} y_i c_i + y_j(\lambda c_j) \\ &= \sum_{i\in[n]\setminus\{j\}} y_i c_i + (\lambda y_j) c_j \\ &= \sum_{i\in[n]\setminus\{j\}} y_i c_i + y_j'' c_j, \text{ em que } T_{\lambda^{-1}}^j(y'') = y \\ &= \sum_{i=0}^{n} y_i'' c_i \\ &= \langle c, y''\rangle \\ &\Rightarrow \exists\, y'' \in C^\perp; T_{\lambda^{-1}}^j(y'') = y \\ &\Rightarrow T_\lambda^j(C)^\perp \subseteq T_{\lambda^{-1}}^j(C^\perp)\end{aligned}$$

Portanto, $T_\lambda^j(C)^\perp = T_{\lambda^{-1}}^j(C^\perp)$

■

Teorema 4.5.6. Sejam C e D dois códigos lineares em $\mathbb{F}_q^n$. Se C e D são linearmente equivalentes, então $C^\perp$ e $D^\perp$ são linearmente equivalentes.

Demonstração. Seja $T = T_\pi \circ T_{c_1}^1 \circ \ldots \circ T_{c_n}^n$ uma isometria que leva C a D. Então,

$$
\begin{aligned}
D^{\perp} &= T(C)^{\perp} \\
&= T_{\pi} \circ T^{1}_{c_1} \circ \ldots \circ T^{n}_{c_n}(C)^{\perp} \\
&= T_{\pi}\Big((T^{1}_{c_1} \circ \ldots \circ T^{n}_{c_n}(C))^{\perp}\Big) \\
&= T_{\pi}\Big(T^{1}_{c_1^{-1}}(T^{2}_{c_2} \circ \ldots \circ T^{n}_{c_n}(C))^{\perp}\Big) \\
&= \ldots \\
&= T_{\pi} \circ T^{1}_{c_1^{-1}} \circ \ldots \circ T^{n-1}_{c_{n-1}^{-1}}\Big(T^{n}_{c_n}(C)^{\perp}\Big) \\
&= T_{\pi} \circ T^{1}_{c_1^{-1}} \circ \ldots \circ T^{n}_{c_n^{-1}}(C^{\perp}) \\
&\therefore D^{\perp} \text{ e } C^{\perp} \text{ são equivalentes.}
\end{aligned}
$$

■

Lema 4.5.7. Seja C um código linear de dimensão k em $\mathbb{F}_{\mathrm{q}}^{\mathrm{n}}$ com matriz geradora G. Uma matriz H de ordem $n \times (n-k)$ com coeficientes em $\mathbb{F}_{\mathrm{q}}^{\mathrm{n}}$ e com colunas linearmente independentes é uma matriz geradora de $C^{\perp}$ se, e somente se, $H^{T}G = 0$.

Demonstração. De fato, para H ser uma matriz geradora de $C^{\perp}$, todas as suas colunas devem ser ortogonais a C, levando a $H^{T}G = 0$.

Reciprocamente, se uma matriz apresenta $n-k$ colunas LI e ortogonais a uma matriz geradora $C_{n\times k}$, temos que estas colunas formam um subcódigo ortogonal a C, portanto, subcódigo de $C^{\perp}$. Como vimos, $dim(C^{\perp}) = n - dim(C) = n - k$ que é a dimensão do subcódigo gerado pelas colunas de H. Portanto, H é uma matriz geradora de $C^{\perp}$. ■

Corolário 4.5.8. Seja C um código linear. Então $\left(C^{\perp}\right)^{\perp} = C$.

Demonstração. Sejam G e H matrizes geradoras de C e $C^{\perp}$, respectivamente. Sob as perspectiva de $C^{\perp}$, um candidato a código dual deve ter matriz geradora L tal que $L^{T}H = 0_{k\times(n-k)}$. Assim,

$$
\begin{aligned}
G^{T}H &= (H^{T}G)^{T} \\
&= (0_{(n-k)\times k})^{T} \\
&= 0_{k\times(n-k)} \\
\therefore C &= (C^{\perp})^{\perp}
\end{aligned}
$$

■

Proposição 4.5.9. Sejam C um código linear e H uma matriz geradora de $C^{\perp}$.

$$v \in C \iff H^{T}v = 0$$

Demonstração. De fato, tome $v \in C$. Como cada coluna de H é um elemento de $C^{\perp}$, $\langle v, h_j \rangle = 0$, para toda coluna h_j de H. Disso, resulta que $H^T v = 0$. Em contrapartida, se $H^T v = 0$, então $v \in (C^{\perp})^{\perp}$ implica em $v \in C$. ■

Definição 4.5.10. Seja C um código linear. A matriz geradora H de $C^{\perp}$ é chamada de matriz teste de paridade de C.

Definição 4.5.11. Dados um código linear C com matriz de teste de paridade H, seja um elemento v de C. Definimos a síndrome de v como o resultado da operação $H^T v$.

Proposição 4.5.12. Seja H uma matriz teste de paridade de um código C. Temos que o peso de C é maior ou igual a s se, e somente se, quaisquer $s-1$ linhas de H são linearmente independentes.

Demonstração.

($\Longrightarrow$) Seja $C \subset \mathbb{F}_{\mathrm{q}}^{\mathrm{n}}$ um código linear de peso $w(C) > s$, $s \in [n]$. Suponha que H possua s linhas linearmente dependentes $h^{(i_1)}$, ... $h^{(i_s)}$. Dessa forma, existem c_{i_1}, ..., c_{i_s} $\in \mathbb{F}_q$, tais que

$$\sum_{j=1}^{s} h^{(i_j)} \cdot c_{i_j} = 0_{1,n-k}$$

Mas,

$$\sum_{j=1}^{s} {h^{(i_j)}}^T \cdot c_{i_j} = [{h^{(i_1)}}^T \dots {h^{(i_s)}}^T] \cdot \begin{bmatrix} c_{i_1} \\ \vdots \\ c_{i_s} \end{bmatrix} = 0_{n-k,1} \tag{4.5}$$

De (4.5) fica claro que, expandindo o conjunto $X = \{c_{i_l}\}_{l \in [s]}$,

$$H^T \cdot c = \left[{h^{(1)}}^T \mid {h^{(2)}}^T \mid \dots \mid {h^{(n)}}^T \right] \cdot \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{bmatrix} = 0$$

Com $c_j = 0$, se $j \notin X$.

Disso resulta que $c \in C$ e $w(c) \leq s$, necessariamente. Portanto, $w(C) \leq s$.

($\Longleftarrow$) Seja $c \in C$. Como H é a matriz teste de paridade de C,

$$H^T c = 0 \Longrightarrow \sum_{i=1}^{n} {h^{(i)}}^T c_i = 0_{n-k,1} \tag{4.6}$$

Como todo conjunto de s linhas de H é linearmente independente, qualquer que seja o elemento $c \in C$, não existe um conjunto de coordenadas $Y = \{c_{i_l}\}_{l=1}^{r}$ de elementos não nulos tal que $\sum_{l=1}^{r} {h^{(i_l)}}^T c_{i_l}$ que atenda a (4.6) com $r \leq s$. Levando a todo elemento c de C ter peso $w(c) > s$ e, portanto, $w(C) > s$. ■

Teorema 4.5.13. Seja H a matriz teste de paridade de um código linear C. Temos que o peso de C é igual a s se, e somente se, quaisquer $s-1$ linhas de H são linearmente independentes e existem colunas de H linearmente independentes.

Demonstração. Do resultado anterior, quaisquer linha$s-1$ linhas da matriz teste de paridade H são linearmente independentes se, e somente se, $w(C) > s$.

Por outro lado, pelo mesmo resultado, há s linhas de H linearmente dependentes se, e somente se, $w(C) < s+1$.

Concluímos, então que $w(C) = s$ se, e somente se, H possui s linhas linearmente dependentes, mas não $s-1$ linhas linearmente dependentes. ■

Corolário 4.5.14 (Cota de Singleton)**.** Os parâmetros (n, k, d) de um código linear C satisfazem à desigualdade $d \leq n - k + 1$.

Demonstração. Como $C^{\perp}$ possui dimensão $n-k$, H, uma matriz teste de paridade sua, possui no máximo $n-k$ linhas linearmente independentes. Por isso, pelo resultado anterior, $w(C) = d \leq (n-k)+1$ e atinge a cota se, e somente se, quaisquer $n-k$ linhas de H forem linearmente independentes. ■

5 CONJUNTOS PARCIALMENTE ORDENADOS

Esse capítulo expõe os resultados iniciais sobre conjuntos parcialmente ordenados, que chamaremos de posets, e conceitos da teoria de códigos corretores de erros relacionada a eles. Os resultados e definições aqui apresentados estão em [7] e [8], menos quando explicitado.

5.1 DEFINIÇÕES

Definição 5.1.1. Uma ordem parcial é uma relação binária $\preceq$ em X tal que valem as seguintes propriedades, $\forall a, b, c \in X$:

1. Reflexiva: $a \preceq a$;
2. Anti-simétrica: $a \preceq b, b \preceq a \Longrightarrow a = b$;
3. Transitiva: $a \preceq b, b \preceq c \implies a \preceq c$;

Exemplo 5.1.2. Sejam os conjuntos $\mathbb{R}$ e $\mathbb{C}$. Note que as condições para uma ordem parcial recaem também sobre um conjunto totalmente ordenado, como $\mathbb{R}$. Isto é, todo conjunto totalmente ordenado (em todo par de elementos está sujeito a uma relação de precedência) é parcialmente ordenado.

Já o conjunto dos números complexos não é (totalmente) ordenado. Podemos, entretando, definir a ordem parcial $\preceq$ tomando dois números $z = x + iy$ e $w = u + iv$, com $x, y, u, v \in \mathbb{R}$, como

$$w \preceq z \iff u \leq x \text{ e } v \geq y$$

Desta forma as três condições são atendidas. De fato, sejam $z_1 = x_1 + iy_1$, $z_2 = x_2 + iy_2$ e $z_3 = x_3 + iy_3 \in \mathbb{C}$.

1. Reflexiva:

   $x_1 \leq x_1$ e $y_1 \geq y_1$, $\forall z_1 \in \mathbb{C}$.

2. Anti-simétrica:

   Se $z_1 \preceq z_2$ e $z_2 \preceq z_1$, então $x_1 \leq x_2$, $y_1 \geq y_2$, $x_2 \leq x_1$ e $y_2 \geq y_1$. Portanto $x_1 = x_2$ e $y_1 = y_2$. Logo, $z_1 = z_2$.

3. Transitiva:

$$
\begin{aligned}
& z_1 \preceq z_2 \text{ e } z_2 \preceq z_3 \\
\Rightarrow & \begin{cases} x_1 \leq x_2 \text{ e } y_1 \geq y_2 \\ x_2 \leq x_3 \text{ e } y_2 \geq y_3 \end{cases} \\
\Rightarrow & \begin{cases} x_1 \leq x_3 \\ y_1 \geq y_3 \end{cases} \\
\Rightarrow & z_1 \preceq z_3
\end{aligned}
$$

Portanto, $\preceq_{\mathbb{C}}$ é parcialmente ordenado com tal ordem parcial.

Definição 5.1.3. Seja X um conjunto dotado de única ordem parcial $\preceq$. O par ordenado $(X, \preceq)$ é chamado de poset (do inglês, parcially ordered set).

Exemplo 5.1.4. Seja o conjunto $\mathbb{N}^n$. Defina a relação $\preceq_{\mathbb{N}^n}$ entre quaisquer dois elementos $a = (a_1, ..., a_n)$ e $b = (b_1, ..., b_n)$ como

$$a \preceq_{\mathbb{N}^n} b \iff a_i \leq b_i, \forall i = 1, ..., n$$

Podemos verificar

i) $a_i \leq a_i, \forall i = 1, ..., n, a \in \mathbb{N}^n \Rightarrow a \preceq_{\mathbb{N}^n} a, \forall a \in \mathbb{N}^n$

ii) Sejam $a, b \in \mathbb{N}^n$:
$a \preceq_{\mathbb{N}^n} b$, $b \preceq_{\mathbb{N}^n} a \iff a_i \leq b_i, \forall i$ e $b_i \leq a_i, \forall i \iff a_i = b_i, \forall i \iff a = b$

iii) Sejam $a, b, c \in \mathbb{N}^n$; $a \preceq_{\mathbb{N}^n} b \preceq_{\mathbb{N}^n} c$:
$a_i \leq b_i \leq c_i, \forall i \Rightarrow a_i \leq c_i, \forall i \Rightarrow a \preceq_{\mathbb{N}^n} c$

Desta forma, podemos afirmar que $\preceq_{\mathbb{N}^n}$ é uma ordem parcial e o par $(\mathbb{N}^n, \preceq_{\mathbb{N}^n})$ é um poset.

Definição 5.1.5. Sejam dois elementos a, b de um poset $(X, \preceq)$. Dizemos que a e b são comparáveis se existir a relação $a \preceq b$ ou $b \preceq a$. Caso não exista nenhuma das relações, dizemos que a e b são incomparáveis.

Definição 5.1.6. Chamaremos o poset em que quaisquer elementos i, j, com $i \neq j$ são incomparáveis de poset de Hamming ou poset antilinear.

Sob esta definição, todos os espaços de coordenadas que utilizamos antes da construção de posets se tratavam de posets de Hamming. Enunciemos agora o caso oposto, em que todos os pares de elementos de um poset são comparáveis.

Definição 5.1.7. Seja P um poset completamente ordenado, ou seja, dados dois elementos i e j de P temos que $i \preceq_P j$ ou $j \preceq_P i$. A este poset chamaremos de poset linear.

Definição 5.1.8. Sejam dois posets P e Q com ordens $\preceq_P$ e $\preceq_Q$, respectivamente. Dizemos que $f : P \to Q$ é um homomorfismo ordem se:

$$a \preceq_P b \implies f(a) \preceq_Q f(b) \ \forall a, b \in P \tag{5.1}$$

Observação 5.1.9. Se f é um homomorfismo ordem, não necessariamente temos que f^{-1} é também um homomorfismo ordem. Veja o exemplo a seguir.

Exemplo 5.1.10. Sejam $f : (\mathbb{N}^n, \preceq_{\mathbb{N}^n}) \to (\mathbb{N}^n, \preceq_1)$, identidade sobre $\mathbb{N}$ e a relação parcial $\preceq_1$ definida como

$$a \preceq_1 b \iff a_1 \leq b_1$$

Desta forma, é fácil constatar que

$$a \preceq_{\mathbb{N}^n} b \Rightarrow a_1 \leq b_1 \Rightarrow f(a) \preceq_1 f(b)$$

Porém, considere $a', b' \in (\mathbb{N}^n, \preceq_1)$ tais que ${a'}_1 \leq {b'}_1$, mas ${a'}_i > {b'}_i$ para algum $i \neq 1$. Assim $a' \preceq_1 b'$, porém $f^{-1}(a') \not\preceq_{\mathbb{N}^n} f^{-1}(b')$.

Observação 5.1.11. A Figura 2 é uma representação em diagrama de Hasse. O diagrama de Hasse é uma forma gráfica de resumir as relações de precedência em um poset P sob a ordem $\preceq_P$ dada: os elementos ligados por uma aresta mantém uma relação de precedência um ao outro, sendo $i \preceq_P j$ se j estiver acima de j.

No poset representado sobre o conjunto $X = [4]$, temos a seguinte relação, $2n-1 \preceq 2m$, $n, m \in \{1, 2\}$, representada pelo diagrama de Hasse abaixo:

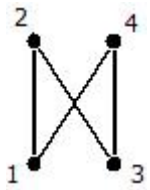

Figura 2 – Diagrama de Hasse

Definição 5.1.12. Um homomorfismo ordem é um isomorfismo se é bijeção e sua inversa também é um homomorfismo ordem. Um isomorfismo de um poset sobre si mesmo é um automorfismo.

Definição 5.1.13. Analogamente ao homomorfismo ordem, há o anti-homomorfismo ordem f:

$$a \preceq_P b \Rightarrow f(b) \preceq_Q f(a), \forall a, b \in X$$

Definição 5.1.14. Dado um poset $P = (X, \preceq_P)$, temos o seu poset oposto $\overline{P} = (X, \preceq_Q)$ tal que

$$i \preceq_P j \iff j \preceq_Q i, \forall i, j \in X$$

Proposição 5.1.15. Sejam P e Q posets e seja $\varphi : P \to Q$ um isomorfismo, então $\varphi : \overline{P} \to \overline{Q}$ também é isomorfismo.

Demonstração. Sejam $a, b \in X$, φ isomorfismo de P em Q e $b \preceq_{\overline{P}} a$.

$$\begin{aligned} b \preceq_{\overline{P}} a &\Rightarrow a \preceq_P b \\ &\Rightarrow \varphi(a) \preceq_Q \varphi(b) \\ &\Rightarrow \varphi(b) \preceq_{\overline{Q}} \varphi(a) \end{aligned}$$

■

Definição 5.1.16. Um ideal (ordem) de P é um subconjunto $I \subseteq P$ com a seguinte propriedade: se $u \in I$ e $v \preceq_{\mathrm{P}} u$, então $v \in I$.

Exemplo 5.1.17. Para o poset representado pelo diagrama de Hasse na Figura 2, temos que os subconjuntos $\{1\}$, $\{3\}$, $\{1, 2, 3\}$, $\{1, 3, 4\}$ e o próprio $[4]$ são todos os ideais ordem de X.

Definição 5.1.18. Dado $A \subseteq P$, denotamos por $\langle A \rangle_P$ o menor ideal de P contendo A, chamado ideal (ordem) de P gerado por A. Em outras palavras, $v \in \langle A \rangle \Rightarrow \exists a \in A$; $v \preceq_{\mathrm{P}} a$.

Definição 5.1.19. O elemento $a \in P$ é dito maximal em relação à ordem $\preceq_{\mathrm{P}}$ se $a \preceq_{\mathrm{P}} b$ implica em $b = a$. No sentido oposto, a é minimal se $b \preceq_{\mathrm{P}} a$, então $b = a$.

Exemplo 5.1.20. Seja o poset P sobre $[7]$ da Figura 3. Os elementos 1, 2 e 3 são minimais. Os elementos 5 e 7 são maximais. O elemento 6 não é minimal, nem maximal. E o elemento 4 é tanto maximal quanto minimal.

Definição 5.1.21. Definimos os seguintes conjuntos:

$$\mathcal{I}_P^r = \{J \subset P;\ \#J = r\}$$

$$\mathcal{M}(J) = \{x \in P;\ x \text{ é maximal no ideal } J \in P\}$$

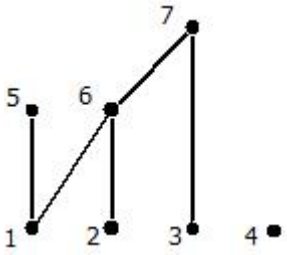

Figura 3 – Diagrama de Hasse de um poset P sobre [7]

Proposição 5.1.22. Sejam $0 \leq r \leq s \leq \#P$, e $I \in \mathcal{I}^r(P)$. Então, existe $J \in \mathcal{I}^s(P)$ tal que $I \subseteq J$.

Demonstração.

Se $s = r$ a demonstração é imediata.

Seja, então, $s > r$, $s = r + t$, $t \in \mathbb{N}^*$, $s \leq \#P$.

Para $t = 1$, seja $I' = P \backslash I$ e m_1 um elemento minimal de I'. Então $J_1 = \{m_1\} \cup I$ é um ideal de P com $\#J_1 = r + 1$.

Considere, então, haver $J_k \in \mathcal{I}^{r+k}(P)$. Sendo $J'_k = P \backslash \mathcal{I}^{r+k}(P)$, seja m_{k+1} um elemento minimal de J'_k. Portanto, $J_{k+1} := J_k \cup \{m_{k+1}\} \in \mathcal{I}^{r+k+1}(P)$. Logo, desde que $r + t \leq \#P$, existe $J \in \mathcal{I}^s(P)$, tal que $I \subseteq J$, $s = r + t$. ■

Proposição 5.1.23. Sejam $0 \leq s \leq r \leq \#P$ e $I \in \mathcal{I}^r(P)$. Então exite $J \in \mathcal{I}^s(P)$ tal que $J \subset I$.

Podemos demonstrar esta proposição de duas formas. A primeira é via maximais, análoga à demonstração da proposição anterior. A segunda é construindo tais conjuntos via minimais de cada poset.

Demonstração 1: via maximais. Analogamente à construção anterior, para todo ideal com cardinalidade positiva k podemos construir outro de cardinalidade $k - 1$ removendo um de seus maximais. ■

Demonstração 2: via minimais. Seja $I' = P \backslash I$. Podemos afirmar

1. $r' = \#I' = \#P - \#I = \#P - r$
2. I' é um ideal ordem de $\overline{P}$

A primeira afirmativa é imediata. Para a segunda, considere $a \in I'$ e $x \in \overline{P}$ tais que $x \preceq_{\overline{P}} a$. (Como será visto mais adiante, I' é o dual de I).

$$\begin{aligned} x \preceq_{\overline{P}} a &\Rightarrow a \preceq_{\mathrm{P}} x \\ &\Rightarrow x \notin I \\ &\Rightarrow x \in I' \end{aligned}$$

Retornamos ao caso da proposição anterior, trocando r por r' e I por I', temos que para $0 \leq r' \leq s' \leq \#\{\overline{P}\} = \#\{P\}$, existe $J' \in \mathcal{I}^{s'}(\overline{P})$, $s' = \#P - s$ satisfazendo $I' \subseteq J'$.

Desta forma, usando os mesmos argumentos, existe $J \in \mathcal{I}^{s}(P)$, $J = \#P \backslash J'$.

$$\begin{aligned} J =& \#P \backslash J' \\ \subseteq& \#P \backslash I' \qquad \Longrightarrow \qquad J \subseteq I \\ =& I \end{aligned}$$

■

Exemplo 5.1.24. Sejam o poset P sobre [9] representado pela Figura 4 e o ideal $I = \langle 8 \rangle_P$, $\#\langle 8 \rangle_P = 5$. Escolhendo números ao acaso em [9], como $s = 2$, 4, 6 e 8, encontramos sempre algum ideal contido ou que contenha I, em concordância com as Proposições 5.1.22 e 5.1.23.

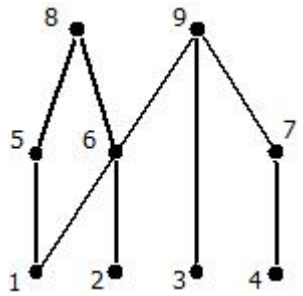

Figura 4 – Diagrama de Hasse de um poset P sobre [9]

Exemplos de ideais contidos em I que satisfazem as condições propostas são $J_2 = \langle 6 \rangle_P$, com $\#J_2 = 2$ e $J_4 = \langle 5, 6 \rangle_P$, com $\#J_4 = 4$.

Exemplos de ideais ordem contendo I com as cardinalidades 6 e 8 são $J_6 = I \cup \{3\}$ e $J_8 = P \backslash \{9\}$.

Proposição 5.1.25. Seja P um poset. Então, dois ideais I, J são iguais se, e somente se, $\mathcal{M}(I) = \mathcal{M}(J)$.

Demonstração. Se $I = J$, claramente $\mathcal{M}(I) = \mathcal{M}(J)$. Reciprocamente, se $\mathcal{M}(I) = \mathcal{M}(J)$, segue que:

$$\begin{aligned} x \in I &\Rightarrow \exists a \in \mathcal{M}(I); x \preceq a, a \in \mathcal{M}(I) \\ &\Rightarrow x \in J \\ &\Rightarrow I \subseteq J \end{aligned}$$

Analogamente, $J \subsetneq I$. Logo, $I = J$. ■

5.2 CÓDIGOS PONDERADOS POR ORDENS PARCIAIS

Definição 5.2.1. Dado um poset $P = ([n], \preceq_P)$, definimos o P-peso de $x \in \mathbb{F}_q^n$ como

$$w_P(x) := \ \#\langle supp(x)\rangle_P \tag{5.2}$$

A distância induzida em $\mathbb{F}_q^n$ por w_P é chamada de P-distância e é calculada como segue:

$$d_P(x, y) := w_P(x - y) \tag{5.3}$$

Teorema 5.2.2. Se P é um poset sobre $[n]$, então a P-distância

$$d_P(x, y) = w_P(x - y)$$

é uma métrica sobre $\mathbb{F}_q^n$.

Demonstração. Demonstremos as três condições para d_P ser uma métrica.

1.

$$\begin{aligned} d_P(x, y) &= w_P(x - y) \\ &= \#\{i; \exists j \in P, i \preceq_P j, x_j - y_j \neq 0\} \\ &= \#\{i; \exists j \in P, i \preceq_P j, y_j - x_j \neq 0\} \\ &= w_P(y - x) \\ &= d_P(y, x) \end{aligned} \tag{5.4}$$

2.

$$\begin{aligned} d_P(x, y) = 0 &\iff \#\{i;\ \exists\ j,\ i \preceq_P j,\ x_j - y_j \neq 0\} = 0 \\ &\iff \nexists i \in [n];\ x_i - y_i \neq 0 \\ &\iff x = y \end{aligned} \tag{5.5}$$

3.

$$\begin{aligned} d_P(x,z) &= \#\{\ i;\ \exists j \in P, i \preceq_P j,\ x_j - y_j \neq 0\} \\ &= \#\{\ i;\ \exists j \in P, i \preceq_P j,\ (x_j - y_j) + (y_j - z_j) \neq 0\} \\ &\leq \#\{\ i;\ \exists j \in P,\ i \preceq_P j, x_j - y_j \neq 0 \text{ ou } y_j - z_j \neq 0\} \\ &= \#\langle supp(x-y)\rangle \bigcup \langle supp(y-z)\rangle \\ &\leq w_P(x-y) + w_P(y-z) \\ &= d_P(x,y) + d_P(y,z) \end{aligned} \tag{5.6}$$

$$d_P(x,z) \leq d_P(x,y) + d_P(x,z) \tag{5.7}$$

Por fim, temos

$$d_P(x,y) := \#\{\ i; \exists j \in P,\ i \preceq_P j, x_j - y_j \neq 0\} \in \{0, ..., n\} \tag{5.8}$$

■

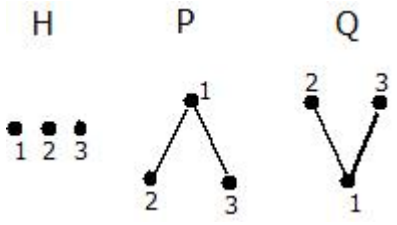

Figura 5 – Posets H, P e Q. Exemplo 5.2.4

Definição 5.2.3. Seja P um poset sobre $[n]$. Um código $C \subseteq \mathbb{F}_q^n$ é chamado r-corretor de erros P-perfeito se as P-bolas de raio r centradas nas palavras do código são disjuntas e a união destas é todo o espaço $\mathbb{F}_q^n$.

Exemplo 5.2.4. Seja o código $[3,2]_2$ $C = \{u_0 = 000, u_1 = 010, u_2 = 100, u_3 = 110\}$ e os posets H (de Hamming), P e Q da Figura 5.

Encontramos as seguintes distâncias no espaço $\mathbb{F}_2^3$ para cada um dos posets nas tabelas 1 para o poset H, 2 para o poset P e 3 para o poset Q.

Para uma melhor visualização, os pares distantes em uma unidade foram coloridos com amarelo. Repare que como a cardinalidade do espaço em que C se encontra tem $\#\mathbb{F}_2^3 = 2^3 = 8$, então para que C seja considerado perfeito, cada bola centrada nos elementos de C deve conter exatamente $\#\mathbb{F}_2^3/\#C = 8/4 = 2$ elementos e cada elemento de $\mathbb{F}_2^3$ deve ter uma distância mínima a apenas um dos elementos de C, estando os demais a uma distância superior.

Tabela 1 – Distâncias para o poset H

v	$d(v,u_0)$	$d(v,u_1)$	$d(v,u_2)$	$d(v,u_3)$
000	0	1	1	2
001	1	2	2	3
010	1	0	2	1
011	2	1	3	2
100	1	2	0	1
101	2	3	1	2
110	2	1	1	0
111	3	2	2	1

Tabela 2 – Distâncias para o poset P

v	$d_P(v,u_0)$	$d_P(v,u_1)$	$d_P(v,u_2)$	$d(v,u_3)$
000	0	2	2	3
001	1	2	2	3
010	2	0	3	2
011	2	1	3	2
100	2	3	0	2
101	2	3	1	2
110	3	2	2	0
111	3	2	2	1

Tabela 3 – Distâncias para o poset Q

v	$d_Q(v,u_0)$	$d_Q(v,u_1)$	$d_Q(v,u_2)$	$d(v,u_3)$
000	0	2	1	3
001	2	3	2	3
010	2	0	2	1
011	3	2	3	2
100	1	2	0	2
101	2	3	2	3
110	2	2	2	0
111	3	2	3	2

Porém, não é isso que se observa em Q. Para este, há elementos v que equidistam de dois elementos distintos de C e duas unidades, mas não em uma unidade. Já para o poset P, há exatamente um elemento distante em uma unidade de cada elemento de C, valendo para todos os elementos do espaço.

Note, então, que o mesmo código C é H-perfeito e P-perfeito, não sendo Q-perfeito.

5.3 ISOMETRIAS EM ESPAÇOS POSET

Definição 5.3.1. Uma isometria entre dois espaços métricos (M, d_M) e (N, d_N) é uma aplicação $T : M \to N$ tal que

$$d_N(Tx, Ty) = d_M(x, y)$$

Definição 5.3.2. Uma isometria linear (ou P-isometria) T sobre o espaço métrico $(\mathbb{F}_q^n, d_P)$ é uma transformação linear $T : \mathbb{F}_q^n \to \mathbb{F}_q^n$ que preserva a P-métrica,

$$d_P(Tx, Ty) = d_P(x, y), \forall x, y \in \mathbb{F}_q^n$$

Equivalentemente, T é isometria linear se

$$w_P(Tx) = w_P(x), \forall x \in \mathbb{F}_q^n$$

Teorema 5.3.3. Seja P um poset sobre $[n]$. O conjunto de todas as isometrias lineares do espaço $(\mathbb{F}_q^n, d_P)$ é um grupo com a operção de composição de transformações lineares $\circ$.

Demonstração. O resultado é imediato, pois d_P é uma métrica. ■

Teorema 5.3.4. Sejam P um poset sobre $[n]$, $\{e_i\}_{i=1}^n$ a base canônica de $\mathbb{F}_q^n$ e T uma P-isometria. Então a aplicação $\phi_T : P \to P$ dada por

$$\phi_T(i) = max(\langle supp(Te_i)\rangle_P)$$

é um automorfismo de P.

Para este teorema serão feitas duas demonstrações diferentes, ambas tentando construir o conjunto $\phi_T(i)$. A primeira é "ascendente" e partirá de considerações sobre os elementos minimais, tentando chegar, ao final, à unicidade dos maximais dos $\langle supp(Te_i)\rangle_P$ e concluindo que i's diferentes levam a $\langle supp(Te_i)\rangle_P$ diferentes.

A outra é "descendente" e aborda os maximais de cada $\langle supp(Te_i)\rangle_P$. Também buscando a unicidade de maximais e maximais distintos para $\langle supp(Te_i)\rangle_P$ distintos.

Demonstração 1, Abordagem "ascendente".

i) Minimais levam a minimais.

$$\begin{aligned} w_P(e_i) &= d_P(e_i, 0) \\ &= d_P(Te_i, T0) \\ &= w_P(Te_i) \end{aligned}$$

Em particular, $w_P(e_i) = 1 \iff w_P(Te_i) = 1$.

Ou seja, $Te_i = \alpha e_k, \alpha \neq 0$, para algum $k \in [n]$ e k é minimal em P.

O mesmo vale para T^{-1}:

$$\begin{aligned} w_P(e_k) &= w_P(TT^{-1}e_k) \\ &= w_P(T^{-1}e_k) \end{aligned}$$

ii) Minimais distintos levam a minimais distintos

Sejam $i_1, i_2 \in [n]$ minimais em P, $i_1 \neq i_2$:

$$\alpha_1 e_{i_1} - \alpha_2 e_{i_2} \neq 0, \forall \alpha_1, \alpha_2 \neq 0$$

Suponha k, $\beta_1, \beta_2 \neq 0$; $Te_{i_1} = \beta_1 e_k$, $Te_{i_2} = \beta_2 e_k$.

$$\begin{aligned} &\beta_2 Te_{i_1} - \beta_1 Te_{i_2} = \beta_2\beta_1 e_k - \beta_1\beta_2 e_k \\ &T(\beta_2 e_{i_1} - \beta_1 e_{i_2}) = 0 \implies \beta_2 e_{i_1} - \beta_1 e_{i_2} = 0. \text{ Contradição.} \end{aligned}$$

Portanto, $\forall i_1, i_2, i_1 \neq i_2$ minimais, $Te_{i_1} = \beta_1 e_{k_1} \neq \beta_2 e_{k_2} = Te_{i_2}$, $k_1 \neq k_2$ minimais, $\beta_1, \beta_2 \neq 0$.

iii) $i \preceq_P j, i \neq j \implies \langle supp(Te_i)\rangle_P \subsetneq \langle supp(Te_j)\rangle_P$

$$\begin{aligned} \langle j\rangle_P &= \langle j, i\rangle_P \\ &= \langle supp(\alpha Te_i + e_j)\rangle_P, \ \forall \alpha \neq 0 \\ \implies w_P(Te_j) &= w_P(T(\alpha e_i + e_j)) \\ &= w_P(Te_j + \alpha Te_i), \ \forall \alpha \\ \implies \langle supp(Te_i)\rangle_P &\subseteq \langle supp(Te_j)\rangle_P \end{aligned}$$

Com $i \neq j$, então $\#\langle i\rangle_P < \#\langle j\rangle_P$ e

$$\begin{aligned} w_P(Te_i) = w_P(e_i) < w_P(e_j) = w_P(Te_j) \\ \therefore \langle supp(Te_i)\rangle_P \subsetneq \langle supp(Te_j)\rangle_P \end{aligned}$$

iv) Se j não é minimal, então $\exists k \in [n]$; $k \in \langle supp(Te_j)\rangle_P$, k não minimal

Seja $j \in [n]$ não minimal.

$$\begin{aligned} \#\langle j\rangle_P = w_P(e_j) > 1 \\ w_P(Te_j) = w_P(e_j), \langle supp(Te_j)\rangle_P \supseteq \langle supp(Te_i)\rangle_P, \forall i \preceq_P j \end{aligned}$$

Como a correspondência de ideais unitários e elementos minimais é biunívoca, há, no máximo, $w_P(e_j) - 1$ elementos minimais em $\langle supp(Te_j)\rangle_P$. Portanto, existe $k \in \langle supp(Te_j)\rangle_P$, tal que k não é minimal.

v) Defina a operação $\psi_T : P \to \mathcal{I}(P)$, $\mathcal{I}(P) :=$ ideais de P

$$\begin{aligned} \psi_T : P_0 &\to \mathcal{I}(P_0), \\ i &\mapsto \langle supp(Te_i)\rangle_P \end{aligned} \qquad P_0, Q_0 = P \tag{5.9}$$

Defina $M_0 := \{$ minimais de $P_0\}$.

Como foi visto, $T(e_i) = \alpha_k e_k, \alpha_k \neq 0, k \in M_0, \forall i \in M_0$.

Defina agora

$$\begin{aligned} \psi_T^{(1)} : P_1 &\to P_1, P_1 = P_0 \backslash M_0 \\ i &\mapsto \langle supp(Te_i)\rangle_P \end{aligned} \tag{5.10}$$

P_1 mantém todas as características de P_0 até agora descritas. Por indução, seguiremos construindo P_l e M_l até que atinjamos $m \in \mathbb{N}; P_{m+1} = \emptyset$.

Note que a cada etapa l atrelamos um elemento $i \in M_l$ a um outro $k \in M_l$ e a relação é biunívoca de forma que $\langle supp(Te_i)\rangle \backslash M_{l-1} = \{k\}$.

Observando de trás para a frente, vemos que cada k agora "adicionado" é, na verdade, o elemento maximal de $\langle supp(Te_i)\rangle_P$ a ele associado.

Sabemos que não é possível que i tenha outro maximal k' em $\langle supp(Te_i)\rangle_P$ eliminado na etapa anterior a l pois cada k' eliminado está em um único $\langle supp(Te_i)\rangle_P$, que é descartado também.

Portanto, $\forall i \in P$:

$$\exists!\ k;\ \langle k\rangle_P = \langle supp(Te_i)\rangle_P$$
$$i \neq j \implies \langle supp(Te_i)\rangle_P \neq \langle supp(Te_j)\rangle_P$$

$\therefore \phi_T$ está bem definida e é injetiva, logo, automorfismo.

■

Demonstração 2, Abordagem "descendente".

Sejam $i_1, i_2 \in P, i_1 \neq i_2$.

Defina $J_i := \langle supp(Te_i)\rangle_P$ e suponha $m \in P; m \in J_{i_1}, J_{i_2}$, m maximal.

$$\begin{array}{l} Te_{i_1} = \sum\limits_{l\in J_{i_1}\setminus\{m\}} \alpha_l e_l + \alpha e_m, \\ Te_{i_2} = \sum\limits_{k\in J_{i_2}\setminus\{m\}} \beta_k e_k + \beta e_m \end{array} \Longrightarrow T(\beta e_{i_1} - \alpha e_{i_2}) = \beta \sum_{l\neq m} \alpha_l e_l - \alpha \sum_{l\in J_{i_1}-\{m\}} \beta_k e_k \quad (5.11)$$

Defina $u := \beta e_{i_1} - \alpha e_{i_2}$ e $v := Tu$.

Mas $w_P(Tu) = \#\langle i_1, i_2\rangle_P = \#\left(\langle i_1\rangle_P \bigcup \langle i_2\rangle_P\right)$, para ideais ordem.

Entretanto, $w_P(v) \leq (\#(J_{i_1} \cup J_{i_2}\setminus\{m\}) < \#\left(J_{i_1} \bigcup J_{i_2}\right) = \#\left(\langle i_1\rangle_P \cup \langle i_2\rangle_P\rangle\right)$.

Daí, $w_P(v) \neq w_P(Tu)$. Contradição.

Portanto, $M(J_{i_1}) \cap M(J_{i_1}) = \emptyset$.

Como T é isometria, $\langle supp(Te_i)\rangle_P \neq \emptyset, \forall i$.

Portanto, $M(J_i) \neq \emptyset, \forall i$,

pelo princípio das casas dos pombos, $\#J_i = 1, \forall i$.

Por isso, ϕ_T está bem definida: todo maximal de $\langle supp(Te_i)\rangle_P$ é o máximo de $\langle supp(Te_i)\rangle_P$ sob a ordem $\preceq_{\mathrm{P}}$.

Além disso, ϕ_T é isometria de P sobre P.

$\therefore \phi_T$ é automorfismo.

■

Teorema 5.3.5. Sejam P um poset sobre $[n]$ e $\mathcal{B} = \{e_i\}_{i=1}^n$ a base canônica de $\mathbb{F}_{\mathrm{q}}^{\mathrm{n}}$. Então T é uma P-isometria se, e somente se,

$$Te_j = \sum_{i\preceq j} x_{ij} e_{\phi_T(i)}, x_{j,j} \neq 0, \forall j \in [n]. \quad (5.12)$$

em que $\phi_T : P \to P$ é um automorfismo associado com T como no teorema 5.3.4 e x_{ij} são constantes com $x_{jj} \neq 0, \forall j \in [n]$.

Demonstração.

Sejam $j, k \in P$:

$$Te_j = \sum_{i\in[n]} x_{ij} e_{\phi_T(i)} = x_{kj} e_{\phi_T(k)} + \sum_{i\in[n]\setminus\{k\}} x_{ij} e_{\phi_T(i)}, \text{ com } x_{kj} \neq 0$$

Então,

$$\begin{aligned}\phi_T(k) \in \langle supp(Te_j)\rangle_P &\Longrightarrow \langle supp(Te_k)\rangle_P \subset \langle supp(Te_j)\rangle_P \\ &\Longrightarrow k \preceq_{\mathrm{P}} j \\ &\Longrightarrow Te_j = \sum_{i \preceq_{\mathrm{P}} j} x_{ij} e_{\phi_T(i)}\end{aligned}$$

Mais ainda,

$$\begin{aligned}\phi_T(j) \in supp(Te_j) &\Longrightarrow x_{jj} e_{\phi_T(j)} \neq 0 \\ &\Longrightarrow x_{jj} \neq 0\end{aligned}$$

$$\therefore\ Te_j = \sum_{i \preceq_{\mathrm{P}} j} x_{ij} e_{\phi_{\mathrm{T}}(i)},\ x_{jj} \neq 0, \forall j \in [n]$$

■

Observação 5.3.6. Como ϕ_{T} é um automorfismo sobre $[n]$, $\phi_{\mathrm{T}}([n]) = [n]$.

Logo,

$$\sum_{i\in[n]} c_{ij} e_i = \sum_{l\in[n]} x_{lj} e_{\phi_{\mathrm{T}}(l)},\ \ x_{lj} = c_{\phi_{\mathrm{T}}(l)j}, \forall j \in [n] \tag{5.13}$$

Corolário 5.3.7. Seja P um poset sobre $[n]$. Dado T uma isometria linear de $(\mathbb{F}_{\mathrm{q}}^{\mathrm{n}}, d_P)$, existe uma ordenação $\beta = \{e_{i_1}, ..., e_{i_n}\}$ da base canônica tal que $[T]_{\beta,\beta}$ é dada por um produto $A \cdot U$, onde A é uma matriz triangular superior e U é uma matriz de permutação correspondente ao automorfismo induzido por T.

Demonstração. Seja $u : P \to P$ uma permutação da base canônica tal que $i_k \leq i_l$ sempre que $e_{i_k} = u(e_k) \preceq_{\mathrm{P}} u(e_l) = e_{i_l}$.

Como o resultado do Teorema 5.3.5, então

$$Te_{i_k} = \sum_{i \preceq_{\mathrm{P}} i_k} x_{ii_k} e_{\phi_{\mathrm{T}}(i)} = \sum_{i\in[n]} x_{ii_k} e_{\phi_{\mathrm{T}}(i)},\ \text{com } x_{ii_k} = 0 \text{ se } i \not\preceq_P i_k \tag{5.14}$$

Se $i \geq i_k$, então $i \not\preceq_P i_k$ e $x_{ii_k} = 0$. Ainda por 5.3.5, $x_{i_k i_k} \neq 0$.

Portanto, $[T]_{\beta,\beta} \in G_P := \{a_{ij} \in \mathbb{M}_n(\mathbb{F}_{\mathrm{q}}^{\mathrm{n}}); a_{ii} \neq 0, a_{ij} = 0,\ \text{se } i \not\preceq_P j\}$. ■

Definição 5.3.8. Um P-código $C \subset \mathbb{F}_{\mathrm{q}}^{\mathrm{n}}$ e um Q-código $C' \subset \mathbb{F}_{\mathrm{q}}^{\mathrm{n}}$ são equivalentes quando existe uma isometria linear $T : (\mathbb{F}_{\mathrm{q}}^{\mathrm{n}}, d_Q) \to (\mathbb{F}_{\mathrm{q}}^{\mathrm{n}}, d_P)$ tal que $T(C) = C'$.

Definição 5.3.9. Sejam P e Q posets isomorfos sob o isomorfismo $\phi : P \to Q$.

Definimos T_ϕ a transformação linear induzida por ϕ:

$$\begin{aligned} T_\phi : (\mathbb{F}_{\mathrm{q}}^{\mathrm{n}}, d_Q) &\to (\mathbb{F}_{\mathrm{q}}^{\mathrm{n}}, d_P) \\ x = (x_i)_{i=1}^n &\mapsto \sum_{i=1}^{n} x_i e_{\phi(i)} \end{aligned} \tag{5.15}$$

O resultado a seguir não se encontra nas referências [7] e [8]. No Teorema 5.3.4 afirmamos que ϕ_{T} é um automorfismo, mas não apresentamos a sua inversa. Isto é feito na proposição a seguir.

Proposição 5.3.10. Observamos que ${\phi_{\mathrm{T}}}^{-1} = \phi_{T^{-1}}$.

Demonstração. Seja i um elemento minimal em P. Pelo Teorema 5.3.5, $Te_i = x_i e_{\phi_{\mathrm{T}}(i)}$, $x_i \neq 0$.

$$\begin{aligned} \phi_{T^{-1}}(\phi_{\mathrm{T}}(i)) &= max\langle supp(T^{-1} e_{\phi_{\mathrm{T}}(i)})\rangle_P \\ &= max\langle supp(T^{-1}(x_{ii}^{-1} T e_i))\rangle_P \\ &= max\langle supp(x_{ii}^{-1} e_i)\rangle_P \\ &= max\langle i\rangle_P \\ &= i \end{aligned}$$

Com uma abordagem como a da *demonstração 1* do Teorema 5.3.4, defina o poset $P_1 = P \setminus \{\text{minimais de } P\}$ e repita o procedimento. Haverá novos elementos minimais para os quais $\phi_{T^{-1}}(\phi_{\mathrm{T}}(j)) = j$. Como P é finito, repetindo o procedimento para $P_2, P_3, ...$, chegaremos à mesma conclusão até que se atinja $m \in [n]; P_m = \emptyset$.

$$\therefore \phi_{T^{-1}} = {\phi_{\mathrm{T}}}^{-1}$$

■

Proposição 5.3.11. Seja $\phi : P \to Q$ um isomorfismo. Se C é um Q-código, então $C' = Im(T_\phi)$ é um P-código equivalente a C e o $\overline{Q}$-código $C^\perp$, conforme introduzido anteriormente, é equivalente ao $\overline{P}$-código $(C')^\perp$.

Demonstração. Primeiramente, provemos que $T_\phi x \cdot T_\phi y = x \cdot y$.

$$\begin{aligned} \mathrm{T}_\phi\, x &= \sum_{i=1}^{n} x_i e_{\phi(i)} \\ \mathrm{T}_\phi\, y &= \sum_{j=1}^{n} y_j e_{\phi(j)} \end{aligned} \quad \Longrightarrow Tx \cdot Ty = \sum_{i,j=1}^{n} x_i y_j e_{\phi(i)} e_{\phi(j)}$$

Como ϕ é automorfismo, $\phi(i) = \phi(j) \iff i = j$.

Portanto $e_{\phi(i)} \cdot e_{\phi(j)} = 1 \iff \phi(i) = \phi(j) \iff i = j \iff e_i e_j = 1$.

Daí,

$$\begin{aligned} Tx \cdot Ty &= \sum_{i,j=1}^{n} x_i y_j e_{\phi(i)} e_{\phi(j)} \\ &= \sum_{i,j=1}^{n} x_i y_j e_i e_j \\ &= x \cdot y \end{aligned}$$

Seja agora $v \in C^{\perp\prime}$. Existe $u \in C^\perp$ tal que $\mathrm{T}_\phi\, u = v$.

Sejam a e b, com $a \in C$ e $b = Ta \in C'$.

$$\begin{aligned} v \cdot b &= Tu \cdot Ta \\ &= u \cdot a \quad \Longrightarrow v \in C'^{\perp} \Longrightarrow C^{\perp\prime} \subset C'^{\perp} \\ &= 0 \end{aligned}$$

Seja $v \in C'^{\perp}$.

$v \cdot b = 0, \forall b \in C'$.

Sejam $u = T^{-1}v$, $a \in C$,

$$\begin{aligned} u \cdot a &= Tu \cdot Ta \\ &= v \cdot Ta \implies u \in C^\perp \Longrightarrow v \in C^{\perp\prime} \\ &= 0 \end{aligned}$$

$\therefore C^{\perp\prime} = C'^{\perp}$ ■

Corolário 5.3.12. Se dois P-códigos C e C' são equivalentes por uma transformação induzida então os $\overline{P}$-códigos $C^\perp$ e $(C')^\perp$ são equivalentes pela mesma transformação.

5.4 P-PESOS GENERALIZADOS

Definição 5.4.1. Seja $D \subseteq \mathbb{F}_{\mathrm{q}}^{\mathrm{n}}$ um subespaço. O P-Peso generalizado de D é a cardinalidade

$$w_P(D) := \#\langle supp(D)\rangle_P$$

do menor ideal de P que contém o suporte de D, lembrando que

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

Definição 5.4.2. Definimos também o r-ésimo P-peso mínimo generalizado do código linear $C \subset \mathbb{F}_q^n$ como

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

Definição 5.4.3. Define-se ainda a hierarquia de P-pesos de C, como a sequência

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

Em que k é a dimensão de C sobre $K = \mathbb{F}_q^n$.

Teorema 5.4.4. Para um $[n,k]_q$ P-código linear C com $k > 0$, a hierarquia de P-pesos é crescente:

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

Demonstração.

$$\begin{aligned} d_1^{(P)}(C) &= min\{w_P(D); D \subseteq C, dim_K(D) = 1\} \\ &= min\{w_P(x); x \in C, x \neq 0_{\mathbb{F}_q^n}\} \\ &\geq min\{w_P(x); x \in \mathbb{F}_q^n, x \neq 0_{\mathbb{F}_q^n}\} \\ &= 1 \end{aligned}$$

Seja D_{r+1} subcódigo de C tal que $dim_K(D_{r+1}) = r+1$ e $w_P(D_{r+1}) = d_{r+1}^{(P)}(C)$.

Para todo D_r, subcódigo de C, $dim_P(D_{r+1}) = r$, $D_r \subset D_{r+1}$, tem-se

$$\begin{aligned} w_P(D_r) &\leq d_{r+1}^{(P)}(C) \\ supp(D_r) &\subset supp(D_{r+1}) \\ \Rightarrow d_r^{(P)}(C) \leq w_P(D_r) &\leq w_P(D_{r+1}) = d_{r+1}^{(P)}(C) \\ \Rightarrow d_r^{(P)}(C) &\leq d_{r+1}^{(P)}(C) \end{aligned}$$

Suponha então que exista $D_{r+1} \subset C$ subcódigo tal que $dim(D_{r+1}) = r+1$

$$w_P(D_{r+1}) = d_{r+1}^{(P)}(C) = d_r^{(P)}(C)$$

Seja $D \subset D_{r+1}$ subcódigo, $dim_P D = r$.

$$\begin{aligned} d_r^{(P)}(C) &\leq w_P(D), \text{mas} \\ supp(D) &\subseteq supp(D_{r+1}) \\ \Rightarrow d_r^{(P)}(C) \leq w_P(C) &\leq d_{r+1}^{(P)}(C) \\ \Rightarrow w_P(D) = w_P(D_{r+1}), &\forall D \subset D_{r+1}, dim_K(D) = r \end{aligned}$$

Sejam $\mathcal{B}_{r+1} = \{u^{(1)}, u^{(2)}, ..., u^{(r+1)}\}$ uma base de D_{r+1} e m um elemento maximal de $\langle suppD_{r+1}\rangle_P$.

$\mathcal{B}_r = \left\{ v^{(i)} = u^{(i)} - \frac{u_m^{(i)}}{u_m^{(j)}} u^{(j)} \right\}_{i\in[n]}^{i\neq j}$ para algum j tal que $u_m^{(j)} \neq 0$ também é uma base de $D \subseteq D_{r+1}$, para algum $D; dim_P(D) = r$.

Dessa forma, $m \in \langle supp(D_{r+1})\rangle_P \backslash \langle supp(D_r)\rangle_P$

Como $\langle supp(D_r)\rangle_P \subsetneq \langle supp(D_{r+1})\rangle_P$, então $w_P(D_r) < w_P(D_{r+1})$, contradição.

$$\therefore d_r^{(P)}(C) < d_{r+1}^{(P)}(C), \forall r$$

■

Corolário 5.4.5 (Limitante de Singleton generalizado)**.** Para um $[n,k]_q$ P-código linear C, temos

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

Demonstração. A distância entre dois quaisquer vetores em um espaço poset de dimensão n é o próprio valor n.

$$\begin{array}{l} d_{k-1}^{(P)}(C) \leq d_k^{(P)}(C) - 1 \\ \quad ... \\ d_r^{(P)}(C) \leq d_{r+1}^{(P)}(C) - 1 \end{array} \quad \Longrightarrow \quad \begin{array}{l} d_r^{(P)}(C) \leq d_k^{(P)}(C) + (-1)\cdot(k-(r-1)+1) \\ \qquad\qquad \leq n - (k-r) \\ \qquad\qquad \leq n - k + r \end{array}$$

Analogamente,

$$\begin{array}{r} 1 \leq d_1^{(P)}(C) \\ d_1^{(P)}(C) + 1 \leq d_2^{(P)}(C) \\ ... \\ d_{r-1}^{(P)}(C) + 1 \leq d_r^{(P)}(C) \end{array} \quad \Longrightarrow \quad r \leq d_r^{(P)}(C)$$

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

■

5.5 REFINAMENTO DE UM POSET

Definição 5.5.1. Sejam P e Q posets sobre o mesmo conjunto $[n]$ tais que $x \preceq_Q y \Rightarrow x \preceq_P y$. Dizemos que P é um refinamento de Q e denotamos por $Q \subseteq P$.

Proposição 5.5.2. Sejam P, Q posets com $Q \subseteq P$. Seja C um código linear com $dim(C) = k$. Então, para $r \in [k]$:

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

Demonstração.

Como P é um refinamento de Q:

$$\begin{aligned}
\langle j\rangle_Q \subseteq \langle j\rangle_P, \forall j \in [n] &\implies \langle supp(x)\rangle_Q \subseteq \langle supp(x)\rangle_P, \forall x \in \mathbb{F}_{\mathrm{q}}^{\mathrm{n}} \\
&\implies \langle \bigcup_{x\in D} supp(x)\rangle_Q \subseteq \langle \bigcup_{x\in D} supp(x)\rangle_P \\
&\implies \#\langle supp(D)\rangle_Q \leq \#\langle supp(D)\rangle_P, \forall D \subseteq \mathbb{F}_{\mathrm{q}}^{\mathrm{n}} \\
&\implies w_Q(D) \leq w_P(D), \forall D \subseteq \mathbb{F}_{\mathrm{q}}^{\mathrm{n}} \\
&\implies \min\, w_Q(D_r) \leq \min\, w_P(D_r)
\end{aligned}$$

Com $D_r \subseteq C; dim D_r = r, D_r$ subcódigo.

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

■

Corolário 5.5.3. Sejam P um poset e C um código linear com $dim(C) = k$. Então $d_r^{(H)}(C) \leq d_r^{(P)}(C)$, H poset de Hamming e $r \in [k]$.

Demonstração. H e P são posets sobre o mesmo conjunto $[n]$, então $H \subseteq P$ e, por isso, $d_r^{(H)}(C) \leq d_r^{(P)}(C), \forall P$. ■

Os dois resultados a seguir foram obtidos neste trabalho e não aparecem em [7] ou [8].

Proposição 5.5.4. Seja P um poset qualquer. Para dois elementos quaisquer i, j de P não comparáveis entre si sempre existirão os refinamentos Q e Q' de P em que $i \preceq_Q j$ e $j \preceq_{Q'} i$.

Demonstração.

Em outras palavras, o que queremos mostrar é que tomando dois elementos $i, j \in P$ não comparáveis, podemos criar um refinamento Q em que, sem perda de generalidade, $i \preceq_Q j$ e todas as demais potenciais relações introduzidas por esta relação não contradizem nenhuma já estabelecida por $\preceq_{\mathrm{P}}$. Esta constradição aconteceria se a nova relação de precedência provocasse a relação $s \preceq_Q r$ a dois elementos de P em que $r \preceq_{\mathrm{P}} s$.

Este caso só pode ser introduzido na situação de $i \preceq_Q j$ acarretar na nova relação pela transitividade das comparações entre dois elementos de um poset. Neste caso, deveríamos ter $s \preceq_Q i \preceq_Q j \preceq_Q r$. Sendo as relações $s \preceq_Q i$ e $j \preceq_Q r$ não introduzidas por Q, mas herdadas de P, teríamos, na verdade, $s \preceq_P i$ e $j \preceq_P r$, portanto, $j \preceq_P r \preceq_P s \preceq_P i$, o que contraria a hipótese.

A demonstração é análoga para o refinamento Q'.

■

Proposição 5.5.5. Todo poset finito pode ser refinado até um poset linear.

Demonstração.

Seja P um poset sobre $[n]$, $n \in \mathbb{N}\backslash\{0\}$. No total, existem $m = \binom{n}{2} = \frac{n!}{(n-2)!\cdot 2} < \infty$ pares de elementos de P. Ordene estes pares em uma lista e construa a sequência de posets $Q_1 \subset Q_2 \subset \ldots \subset Q_m$, em que o poset Q_1 é o refinamento de P julgando o primeiro par $(i, j) \in P$ da lista: caso os elementos já tenham relação de comparação, $Q_1 = P$, caso não, Q_2 é o refinamento de Q_1 sob a introdução da relação $i \preceq_{Q_1} j$ ou $j \preceq_{Q_1} i$.

Adotando passos análogos para os posets Q_{r+1} em relação a Q_r, ao construirmos Q_m já teremos que, para todo par (i, j) em Q_m, estes elementos são comparáveis, tornando Q_m um conjunto totalmente ordenado, ou seja, um poset linear. ■

Vale observar que apesar de sempre podermos obter posets lineares, estes posets resultantes não são únicos. De fato, em cada interação na sequência de refinamentos, a escolha entre fazer $i \preceq_{Q_{r+1}} j$ ou $j \preceq_{Q_{r+1}} i$ para um par (i, j) incomparável em Q_r apresenta a possibilidade de duas comparações distintas que não poderão ser revertidas em um passo adiante.

Sob o algoritmo apresentado na demonstração, sempre haverá passos em que o refinamento não introduz nova comparação, podendo-se otimizar a construção de um poset linear. Recomenda-se priorizar criar relações com um maximal e um minimal cujos ideais gerados sejam disjuntos, fazendo este maximal inferior ao minimal no novo refinamento. Isto maximiza as comparações implicitamente introduzidas.

Além disso, é possível chegar ao mesmo poset linear (ou qualquer refinamento) alterando-se a ordem das comparações, alterando possivelmente também o número de passos.

Exemplo 5.5.6. Seja o poset P da Figura 6. Podemos construir o mesmo poset linear pelas sequências das figuras 7 e 8.

Para a sequência da figura 7 as comparações introduzidas foram, na ordem, $2 \preceq_{Q_1} 3$ e $3 \preceq_{Q_2} 4$, seguindo a recomendação dada no primeiro passo.

Já para a sequência da figura 8, as comparações foram, também na ordem, $1 \preceq_{Q'_1} 4$, $2 \preceq_{Q'_2} 3$, $2 \preceq_{Q'_3} 3$ e $3 \preceq_{Q'_4} 4$.

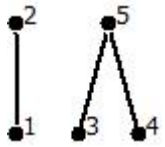

Figura 6 – Poset sobre [5]

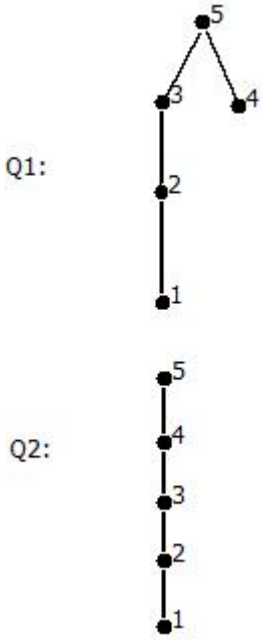

Figura 7 – Opção "rápida"de refinamento a um poset linear.

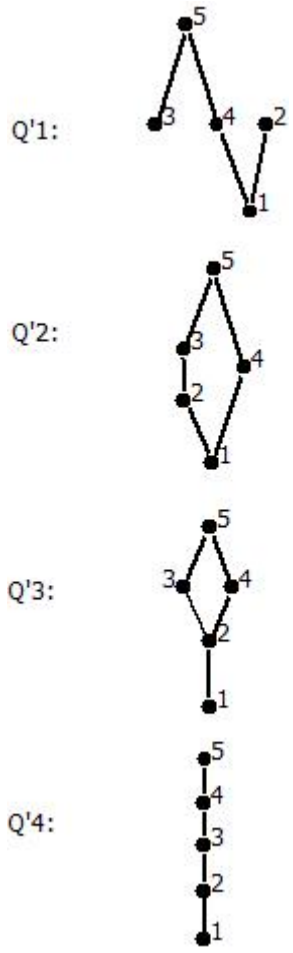

Figura 8 – Opção "lenta"de refinamento a um poset linear.

5.6 CÓDIGOS P-MDS

Definição 5.6.1. Um código C é chamado *MDS* (*maximum distance separable*) se $d_H^{(C)}$ atinge o limitante de Singleton.

Definição 5.6.2. Dizemos que um $[n,k]_q$ P-código C é (P,r)-MDS quando

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

Proposição 5.6.3. Seja C um código (P,r)-MDS. Então, C também é (P,s)-MDS, $\forall s \geq r$.

Demonstração. Analogamente à demonstração do Limitante de Singleton:

$$\begin{array}{r} \text{n-k} + \text{r} = \text{d}_\text{r}^{(\text{P})}(\text{C}) \\ \text{d}_\text{r}^{(\text{P})}(\text{C}) + 1 \leq d_{r+1}^{(P)}(C) \\ \vdots \\ d_{k-1}^{(P)}(C) + 1 \leq d_s^{(P)}(C) \end{array} \quad \Longrightarrow \quad \begin{array}{r} \text{n-k} + \text{r} + 1 \cdot (s-r) \leq d_s^{(P)}(C) \\ n - k + s \leq d_s^{(P)}(C) \end{array}$$

Mas $d_s^{(P)}(C) \leq n - k + s$ pelo Limitante de Singleton.

$\Rightarrow d_s^{(P)}(C) = n - k + s$.

$$\therefore C \text{ é (P,s)-MDS, } \forall s \leq r$$

■

Proposição 5.6.4. Sejam os posets P, Q sobre $[n]$ tais que $Q \subseteq P$ e C subespaço de $\mathbb{F}_\text{q}^\text{n}$. Se C é (Q,r)-MDS, então é (P, r)-MDS. Em particular, se for MDS, então C é (P,r)-MDS, $\forall P$ poset sobre $[n]$.

Demonstração.

$$\begin{aligned} \text{n-k} + \text{r} = d_r^{(Q)}(C) \leq \text{d}_\text{r}^{(\text{P})}(\text{C}) &\leq \text{n-k} + \text{r} \\ \Rightarrow \text{d}_\text{r}^{(\text{P})}(\text{C}) &= \text{n-k} + \text{r} \\ \Rightarrow C \text{ é (P,r)-MDS.} & \end{aligned}$$

Como $H \subseteq P, \forall P$ poset sobre $[n]$, então, C é (P,r)-MDS, $\forall P$ poset sobre $[n]$ se for MDS. ■

Teorema 5.6.5. Para todo código linear C sobre $\mathbb{F}_\text{q}^\text{n}$ e $r \leq dimC$, existe um poset P sobre $[n]$ tal que C é (P,r)-MDS.

Demonstração.

Seja H o poset de Hamming sobre n. Se $\text{d}_\text{r}^{(\text{P})}(\text{C}) = 1$, não há o que demonstrar.

Caso não seja, seja o peso generalizado $d_r^{(H)}(C) < n - k + 1$.

Seja $D \subseteq C$, $dim_{\mathbb{F}_q} C = r$; $w_H(D) = d_r^{(H)}(C)$.

Seja também $V = [n] \setminus \langle supp(D) \rangle_H = [n] \backslash supp(D)$

$$\begin{aligned} \#V &= n - supp(D) \\ &> n - (n - k + r) \\ &= k - r \end{aligned}$$

Escolha n-k + r $-d_r^{(H)}(C)$ elementos de V e componha o poset Q em que $supp(D) \subset Q$ e se $i \in Q \cap V$, então existe $j \in supp(D)$ tal que $i \preceq_{\mathrm{P}} j$.

Dessa forma, $\#\langle supp(D) \rangle_Q = w_H(D) + \text{n-k} + \text{r} - d_r^{(H)}(C) = \text{n-k} + \text{r}$.

Caso não haja outro subcódigo $D^{(1)} \subset C$, $dim_Q D^{(1)} = r$, com $w_Q(D^{(1)}) < \text{n-k} + \text{r}$, então $d_r^{(Q)}(C) = w_Q(D) = \text{n-k} + \text{r}$ e C é (Q,r)-MDS.

Caso haja tal $D^{(1)}$, defina o poset $Q^{(1)}$ a partir de $D^{(1)}$ e $supp(D^{(1)})$ assim como foi feito com Q a partir de D. Repita o procedimento enquanto não for atingido o limitante de Singleton.

Como C é finto, $I^{(r)}(C)$ também é. Assim podemos garantir que com uma quantidade m finita de passos,

$$d_r^{(Q^{(m+l)})}(C) > d_r^{(Q^{(l)})}(C),\ \forall l;\ d_r^{(Q^{(l)})}(C) \neq \text{n-k} + \text{r}$$

Como $d_r^{(Q')}(C) \leq \text{n-k} + \text{r}, \forall Q'$ poset, então $\exists s \in \mathbb{N}$;

$$d_r^{(Q)}(C) \leq d_r^{(Q^{(s)})}(C) = \text{n-k} + \text{r}$$

$\therefore$ Dado um código linear C de $\mathbb{F}_{\mathrm{q}}^{\mathrm{n}}$, existe um poset $P(= Q^{(s)})$ tal que $\mathrm{d}_{\mathrm{r}}^{(\mathrm{P})}(\mathrm{C}) =$ n-k + r. ■

6 MULTICONJUNTOS

O presente capítulo apresenta o conceito de Multiconjunto, coleção de elementos em que cada um pode apresentar mais de uma ocorrência. Multiconjuntos apresentam a interessante ideia de multiplicidade, que é o número de ocorrências de um elemento no multiconjunto referido. Um conjunto como conhecemos poderia ser interpretado como um multiconjunto com multiplicidades 1 para elementos que o componham e 0 para elementos não presentes.

Estes conceitos serão importantes para a demonstração do Teorema da Dualidade no próximo capítulo e podem ser encontrados em [7] e [8], fonte de todas as definições e proposições deste capítulo, com exceção das proposições 6.2.2 e 6.3.3.

6.1 MULTICONJUNTOS

Definição 6.1.1. Chamamos uma coleção $\mathcal{L}$ não ordenada de elementos não necessariamente distintos de um conjunto S de multiconjunto.

Definição 6.1.2. Chamamos de multiplicidade de um multiconjunto $\mathcal{L}$ sobre S a função $\gamma : S \to \mathbb{N}$ em que $\gamma(s)$ é o número de ocorrências de s em $\mathcal{L}$. Neste texto, cada multiconjunto $\mathcal{L}$ será identificado com sua multiplicidade γ e ambos serão chamados de multiconjunto.

Definição 6.1.3. Dois multiconjuntos γ_1 e γ_2 são ditos equivalentes se, e somente se, há uma há uma bijeção $\sigma : S_1 \to S_2$ tal que

$$\gamma_2 = \gamma_1 \circ \sigma$$

Definição 6.1.4. Um código é dito degenerado se existe uma matriz geradora com linha nula. Do contrário, é dito não degenerado.

Definição 6.1.5. Seja C um código com matriz geradora G e a aplicação $m_C : \mathbb{F}_q^k \to [n]$, onde $m_C(v)$ é o número de vezes que o vetor v aparece como uma linha de G. Chamamos tal m_G de multiconjunto induzido pelo código G.

Proposição 6.1.6. Sejam $C \subseteq \mathbb{F}_q^n$ um código e w o peso de Hamming. Dado um subespaço D de C, existe um código $U \subseteq \mathbb{F}_q^k$ tal que

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

Demonstração.

Dada uma matriz geradora G de C:

$$C = \phi_C(\mathbb{F}_q^k)$$
$$D \subseteq C \Rightarrow V = \phi^{-1}(D) \subseteq \mathbb{F}_q^k$$

$$i \in supp(D) \iff \exists v \in V; \qquad g_i \cdot v \neq 0$$
$$\iff g_i \notin V$$

Dai

$$\begin{aligned} w(D) &= \#\{i; \exists v \in V, g_i \cdot v \neq 0\} \\ &= \#\{i; g_i \notin V^\perp\} \\ &= \#\{g_i; g_i \notin V^\perp\} \\ &= n - \#\{g_i; g_i \in V^\perp\} \\ &= n - m_C(V^\perp) \end{aligned}$$

Definindo $U = V^\perp \subset \mathbb{F}_q^k$, $dimU = dimV^\perp = dim\,\mathbb{F}_q^k - dimV = k - dimD$,

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

■

Definição 6.1.7. Seja $\{A_1, ..., A_s\}$ uma coleção de subconjuntos de um espaço vetorial. Denotaremos por $[A_1, ..., A_s]$ o espaço gerado pela interseção de subespaços contendo $\bigcup_{i=1}^{s} A_i$.

Definição 6.1.8. Sejam um $[n,k]_q$ P-código não-degenerado C de dimensão k e uma matriz geradora sua G. O multiconjunto induzido por C é o multiconjunto sobre $\mathcal{P}(\mathbb{F}_q^k)$ dado por

$$m_C^P := \{U_1, ..., U_n\}, \qquad \text{onde } U_i = [\{g_j; i \preceq_P j\}]$$

Em que g_j é a j-ésima coluna de G.

Proposição 6.1.9. Sejam C um $[n,k]_q P$-código e D um subcódigo de C. Então existe um subespaço $U \subseteq \mathbb{F}_q^k$ em que

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

Demonstração.

$$\begin{aligned} w_{\overline{P}}(D) &= \#\{i \in [n]; \quad j \preceq_{\mathrm{P}} i, \exists x \in D, x_j \neq 0\} \\ &= \#\{i \in [n]; \quad j \preceq_{\mathrm{P}} i, \exists v \in \phi^{-1}(D), g_j \cdot v \neq 0\} \\ &= \#\{i \in [n]; \quad j \preceq_{\mathrm{P}} i, g_j \notin V^{\perp} = \phi^{-1}(D) \subseteq \mathbb{F}_{\mathrm{q}}^{\mathrm{k}}\} \\ &= n - \#\{i \in [n]; \forall j \preceq_{\mathrm{P}} i, g_j \in V^{\perp}\} \\ &= n - \#\{i; [g_j; j \preceq_{\mathrm{P}} i] \subseteq V^{\perp}\} \\ &= n - \#\{i; U_i \subseteq V_{\perp}\} \\ &= n - m_C^P(V^{\perp}) \end{aligned}$$

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

■

6.2 LEVANTAMENTO

Definição 6.2.1. Definimos o epimorfismo natural $\mu_C : \mathbb{F}_{\mathrm{q}}^{\mathrm{n}} \to \mathbb{F}_{\mathrm{q}}^{\mathrm{n}}/C^{\perp}$, C código linear sobre $\mathbb{F}_{\mathrm{q}}^{\mathrm{n}}$, por

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

Proposição 6.2.2. Existe uma bijeção

$$\psi_C : \mathbb{F}_{\mathrm{q}}^{\mathrm{n}}/C^{\perp} = \mu_C(\mathbb{F}_{\mathrm{q}}^{\mathrm{n}}) \to C$$

Demonstração.

$$\begin{aligned} \mathbb{F}_{\mathrm{q}}^{\mathrm{n}} &= C \oplus C^{\perp} \\ \Rightarrow \forall x \in \mathbb{F}_{\mathrm{q}}^{\mathrm{n}}, \exists! c \in C, c' \in C^{\perp} \\ x &= c + c' \end{aligned}$$

Definindo ϕ_C como a projeção de $\mathbb{F}_{\mathrm{q}}^{\mathrm{n}}$ sobre C:

$$\begin{aligned} \psi_C(x + C^{\perp}) &= \psi_C(c + c' + C^{\perp}) \\ &= \psi_C(c + C^{\perp}) \\ &= c \end{aligned}$$

Em contrapartida, ψ_C^{-1} é óbviamente definida sobre todo $c \in C$.

Portanto, ψ_C é uma bijeção entre $\mathbb{F}_{\mathrm{q}}^{\mathrm{n}}/C^{\perp}$ e C. ■

Definição 6.2.3. Para um $[n,k]_q P$-código C, o seu multiconjunto associado é o multiconjunto $m_C^{\overline{P}} = \mu_C(B_{\overline{P}})$ definido sobre $\mathcal{P}(\mathbb{F}_q^n / C^{\perp})$.

Definição 6.2.4. Dados os gerados $V_i = [g_j; j \in \langle i \rangle_P]$, definimos o conjunto $B_P := (V_i)_{i=1,...,n}$ como o conjunto de cobertura ortogonal.

6.3 SUBMULTICONJUNTO

Definição 6.3.1. Um submulticonjunto $\gamma' \subseteq \gamma$ é um multiconjunto tal que $\gamma'(s) \leq \gamma(s), \forall s \in S$, sobre o mesmo conjunto S.

Lema 6.3.2. Sejam $C \subseteq \mathbb{F}_q^n$ um P-código e $m_C^{\overline{P}}$ o seu multiconjunto associado. Dado $J \subseteq \{1,...,n\}$ considere $B_J := \{V_j; j \in J\}$ com $V_j = [\{e_i; i \in \langle j \rangle_{\overline{P}}\}]$, então $m_J := \mu_C(B_J)$ é um submulticonjunto de $m_C^{\overline{P}}$ e, mais ainda, todo submulticonjunto de $m_C^{\overline{P}}$ pode ser dado dessa forma.

Demonstração.

$$\begin{aligned} J \subseteq \overline{P} \Rightarrow m_J &= \{\mu(V_i)\}_{i \in J} \subseteq \{\mu(V_i)\}_{i \in \overline{P}} = m_{\overline{P}} \\ &\Rightarrow m_J \subseteq m_{\overline{P}} \end{aligned}$$

■

Proposição 6.3.3. A partir da demonstração da *proposição 6.1.8*, obtemos que o P-peso de um subcódigo $D \subseteq C$ está associada a um submulticódigo $m_J = \mu_C(B_J)$, onde

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

Mais ainda, J é ideal de $\overline{P}$.

Demonstração. Sejam $j \in J$ e $i \in \overline{P}$, $i \preceq_P j \Rightarrow j \preceq_{\overline{P}} i \Rightarrow i \in J$. ■

Proposição 6.3.4. Sejam C um $[n,k]_q$ P-código e $D \subseteq C$ um subcódigo de dimensão r. Então, existe um ideal J de $\overline{P}$ tal que a codimensão de $[\mu_C(B_J)] \subseteq \mathbb{F}_q^k$ é r e

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

Demonstração.

$$\begin{aligned} w_{\overline{P}}(D) &= \#\{i \in \overline{P}; \exists x \in D, j \in \overline{P}, i \preceq_{\overline{P}}, x_j \neq 0\} \\ &= n - \#\{i \in \overline{P}; \forall x \in D, j \in \overline{P}, i \preceq_{\overline{P}} j, x_j = 0\} \\ &= n - \#\{i \in P, \forall x \in D, j \preceq_P i, x_j = 0\} \end{aligned}$$

Faça $J := \{i \in P, \forall x \in D, j \preceq_P i, x_j = 0\}$.

$$\#J = \#\{V_i\}_{i \in J} = \#B_J \Longrightarrow w_{\overline{P}} = n - \#J = n - \#B_J$$

■

Proposição 6.3.5.

$$[B_J] = [\{e_j; j \in \langle J \rangle_{\overline{P}}\}], \forall J \subseteq [n]$$

Demonstração.

$$[B_J] = [(V_i)_{i \in J}] = [\{e_j; k \in \langle i \rangle_{\overline{P}}\}_{i \in J}] = [\{e_j; j \in \langle J \rangle_{\overline{P}}]$$

■

Proposição 6.3.6.

$$dim[B_J] \geq \#B_J \text{ e } dim[B_J] = \#B_J \iff J \text{ é ideal de } \overline{P}.$$

Demonstração.

$$\begin{aligned} dim[B_j] &= dim[e_j]_{j \in \langle J \rangle_{\overline{P}}} \\ &= \#\langle J \rangle_{\overline{P}} \qquad \Longrightarrow dim[B_J] \geq \#B_J \\ &\geq \#B_J \end{aligned}$$

$$\begin{aligned} dim[B_J] = \#B_J &\iff \#\langle J \rangle_{\overline{P}} = \#J \\ &\iff \langle J \rangle_{\overline{P}} = J \end{aligned}$$

■

7 TEOREMA DA DUALIDADE PARA CÓDIGOS POSET

Este capítulo apresenta e demonstra o resultado mais importante em [7], o Teorema da Dualidade para Códigos Poset. Para isto enuncaremos um resultado auxiliar, a proposição 7.1.1. Todos os demais podem ser encontrados em [7].

7.1 DUALIDADE POSET

Proposição 7.1.1. Sejam C um $[n,k]_q$ P-código e $D \subseteq C$ um subcódigo tal que $dimD = r$ e $w_P(D) = \mathrm{d}_{\mathrm{r}}^{(\mathrm{P})}(\mathrm{C})$, então:

$$D = [B_I] \cap C$$

com $I = suppD$.

De fato. Sejam D e I como enunciados.

Suponha $x \in [B_I] \cap C \backslash D$.

Como $x \notin D$, $\{x\} \cup \mathcal{B}_D$ é LI. ($\mathcal{B}_D$ uma base de D)

Daí, $dim[\{x\} \cup \mathcal{B}_D] = r+1$ e $[\{x\} \cup \mathcal{B}_D] \subseteq [B_I] \cap C \subseteq C$.

Portanto,

$$\begin{aligned} & w_P([\{x\} \cup \mathcal{B}_D] = \mathrm{d}_{\mathrm{r}}^{(\mathrm{P})}(\mathrm{C})\,,\ dim[\{x\} \cup \mathcal{B}_D] = r+1 \\ & \Rightarrow \mathrm{d}_{\mathrm{r}}^{(\mathrm{P})}(\mathrm{C}) \geq d_{r+1}^{(P)}(C) \qquad \text{Contradição.} \\ & \Rightarrow [B_I] \cap C \backslash D = \emptyset \\ & \Rightarrow [B_I] \cap C \subseteq D \end{aligned}$$

Por outro lado,

$$D \subseteq C, [B_I] \Rightarrow D \subseteq [B_I] \cap C$$

$$\therefore D = [B_I] \cap C$$

■

Esse resultado mostra ainda que ao identificar um subcódigo D de C com suporte I, este é o único com estas características.

Teorema 7.1.2. Sejam P um poset em $[n]$, C um $[n,k]_q$ P-código em $\mathrm{m}_{\mathrm{C}}^{\overline{\mathrm{P}}}$ o multiconjunto associado a C. Considerando μ o epimorfismo natural de $\mathbb{F}_{\mathrm{q}}^{\mathrm{n}}$ em $\mathbb{F}_{\mathrm{q}}^{\mathrm{n}}/C^{\perp}$, então

$$d_r^{(\overline{P})}(C^{\perp}) = min\{\#B_J; J\text{é ideal de } \overline{P}, \#B_J - dim[\mu_C(B_J)] \geq r\}$$

Demonstração. Seja J um ideal de menor cardinalidade possível de $\overline{P}$ que satisfaz

$$\#B_J - dim[\mu_C(B_J)] \geq r \tag{7.1}$$

Então fazendo $\mu = \mu_C|_{[B_J]}, D' \subseteq C^\perp \cap [B_J] \Rightarrow D' \subseteq N(\mu)$.

Mais,

$$\begin{aligned} \#B_J - dim[\mu_C(B_J)] = \\ dim[B_J] - dimIm(\mu) = \\ dim(N(\mu)) \geq dimD' = r \end{aligned}$$

Além disso,

$$\begin{aligned} D' \subseteq [B_J] \Rightarrow & suppD' \subseteq J \\ \Rightarrow & \langle suppD' \rangle_{\overline{P}} \subseteq J \end{aligned}$$

Suponha $\langle suppD' \rangle_{\overline{P}} \subsetneq J$.

Seja $I = \langle suppD' \rangle_{\overline{P}} \subsetneq J$, $\#I < \#J$.

Faça agora $\mu' = \mu|_{[B_I]}$:

$$\begin{aligned} \#B_I - dim[\mu_C(B_I)] = \\ dim[B_I] - dimIm(\mu') = \\ dimN(\mu') \geq \\ dimD' = r \end{aligned}$$

$\Rightarrow J$ não é o menor ideal de $\overline{P}$ a atender (7.1), contrariando a hipótese inicial.

$\Rightarrow \langle suppD' \rangle_{\overline{P}} = J$.

$\Rightarrow \#B_J = \#J = w_{\overline{P}}(D') = d_r^{\overline{P}}(C^\perp)$.

$\therefore d_r^{\overline{P}}(C^\perp) = min\{\#B_J; \#B_J - dim[\mu_C(B_J)] \geq r, J \text{ é ideal de } \overline{P}\}$.

■

Teorema 7.1.3 (Teorema da Dualidade)**.** Seja C um $[n,k]_q$ P-código e $C^\perp$ o seu código dual. Considere a hierarquia de P-pesos de C

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

e o conjunto

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

Então

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

Demonstração. Pelo resultado anterior, existe um ideal J de $\overline{P}$ tal que $\#B_J = d_r^{\overline{P}}(C^{\overline{P}})$, $r \leq n-k$, $k = dimC$.

$$\#B_J - dim[\mu(B_J)] \leq \#B_J - r = d_r^{(\overline{P})}(C^{\perp}) - r$$

$$\begin{aligned} dim[\mu_C] &= dim[\mu(B_J)] \\ &\geq \#B_J - r \\ &= d_r^{(\overline{P})}(C^{\perp}) - r \end{aligned}$$

$$\begin{aligned} t =& codim[\tau_C(B_J)] \\ =& k - dim[\mu_C(B_J)] \\ \leq& k - d_r^{(\overline{P})}(C^{\perp}) + r \end{aligned}$$

Pela proposição 6.3.4, existe D, $dimD = t$, $w_P(D) = n - \#B_J$ tal que

$$w_P(D) = n - d_r^{(P)}(C^{\perp}) \geq d_t^{(P)}(C)$$

Suponha que haja $s > 0$ para o qual

$$d_{t+s}^{(P)}(C) = n + 1 - d_r^{(P)}(C)$$

Então existe $I \subseteq \overline{P}$ tal que

$$\begin{aligned} [\tau_C(B_I)] \subseteq U \subseteq \mathbb{F}_{\mathrm{q}}^{\mathrm{n}}\text{, com} \\ \#B_I = n - d_{t+s}^{(P)}(C) \end{aligned}$$

e

$$\begin{aligned} dim(U) &= k - (t+s) \\ \Rightarrow dim[\mu_C(B_I)] &= k - t - s \\ &\leq k - (k - d_r^{(\overline{P})}(C^{\perp}) + r) - s \\ &= d_r^{(\overline{P})}(C^{\perp}) - r - s \end{aligned}$$

Aplicando a hipótese,

$$\begin{aligned}\#B_I &= n - d_{t+s}^{(\overline{P})}(C) \\ &= n - (n+1-d_r^{(\overline{P})})(C^\perp) \\ &= d_r^{(\overline{P})}(C^\perp) - 1\end{aligned}$$

Daí,

$$\begin{aligned}\#B_I - dim[\mu_C(B_I)] &\geq \left(d_r^{(\overline{P})}(C^\perp) - 1\right) - \left(d_r^{\overline{P}}(C^\perp) - r - s\right) \\ &= r + s - 1 \\ &\geq r\end{aligned}$$

$$\Rightarrow \#B_I \geq d_r^{\overline{P}}(C^\perp)$$

Mas

$$\#B_I = d_r^{\overline{P}}(C^\perp) - 1$$

Contradição.

$$\begin{aligned}\Rightarrow \nexists d \in [n];& \\ d &= d_t^{(P)}(C) = d_r^{\overline{P}}(C^\perp) \\ t &\in [k], r \in [n-k]\end{aligned}$$

Logo,

$$X \cap Y = \emptyset$$

Como $\#X = k$, $\#Y = n - k$, $X \cap Y = \emptyset$, e $X, Y \subseteq [n]$, segue que

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

■

7.2 CÓDIGOS MDS

Definição 7.2.1. Definimos a $\underline{P\text{-discrepância}}$ de um $[n,k]_q$-código C como o menor inteiro s que satisfaz $d_{s+1}^{(P)}(C) > n - k$. Denotaremos a P-discrepância de um código C como $\delta_P(C)$.

Teorema 7.2.2. Dado um $[n,k]_q$ P-código, então

(1) $\delta_P(C) = \#\left([n-k] \cap \{d_r^{(P)}; r \in [k]\}\right)$

(2) $\delta_P(C) = \delta_{\overline{P}}(C^{\perp})$

Demonstração. .

(1) Pela monotonia da hierarquia de pesos de um P-código sabemos que se $\delta_P^{(P)} = s$, então $d_i^{(P)} \leq n-k$, $\forall i \in [s]$, e também que $d_j^{(P)} > n-k$, $\forall j > s$. Portanto,

$$[n-k] \cap \{d_l^{(P)}(C)\}_{l \leq k} = \{d_l^{(P)}(C)\}_{l \leq \delta_P(C)}$$

E

$$\begin{aligned}
&\#\{d_l^{(C)}\}_{l \leq \delta_P(C)} = \delta_P(C) \\
&\Rightarrow \delta_P(C) = \#\left([n-k] \cap \{d_l^{(P)}(C)\}_{l \leq k}\right) \\
&\Rightarrow \delta_P(C) = \#\left(\{[n-k] \cap \{d_l^{(P)}(C); l \in [k]\}\right)
\end{aligned}$$

(2) Sejam

$$\begin{aligned}
X &= \{d_l^{(P)}(C)\} \\
Y &= \{n+1-d_l^{\overline{P}}(C^{\perp})\}_{l \leq n-k}
\end{aligned}$$

como no teorema da dualidade.

Seja também $r_0 = \delta_P(C)$, então

$$\begin{aligned}
&\#\left(X \cap [n-k]\right) = r_0 \\
&\Rightarrow \#\left([n-k] \setminus X\right) = n-k-r_0 \\
&\text{Existem } n-k-r_0 \text{ elementos } y \text{ de } Y \text{ que satisfazem } y \leq n-k.
\end{aligned}$$

Mas cada $y \in Y$ é da forma $y = n+1-d_s^{(\overline{P})}(C^{\perp})$. Então há $n-k-r_0$ elementos de $\{d_1^{(\overline{P})}(C^{\perp}), ..., d_{n-k}^{(\overline{P})}(C^{\perp})\}$ que satisfazem

$$\begin{aligned}
&n+1-d_s^{\overline{P}}(C^{\perp}) \leq n-k \\
&\Rightarrow d_s^{(\overline{P})} \geq k+1, \text{ para } n-k-r_0 \text{ elementos da hierarquia de } C^{\perp}. \\
&\Rightarrow d_s^{(\overline{P})}(C^{\perp}) \geq k+1, \text{para } n-k-(n-k-r_0) = r_0 \text{ elementos da hierarquia de } C^{\perp}. \\
&\Rightarrow \delta_{\overline{P}}(C^{\perp}) = \delta_P(C)
\end{aligned}$$

■

Proposição 7.2.3. Seja P um poset sobre $[n]$. Um $[n,k]_q$ P-código C é $(P,r) - MDS$ se, e somente se,

$$d_1^{(\overline{P})} \geq k + 2 - r$$

Demonstração.

$$\begin{aligned}
d_1^{(\overline{P})} &\geq k+2-r \\
&\iff \forall s > n+1-k-2+r = n-k+r-1; s \leq n, \\
&\quad s \in X = \{d_i^{(P)}(C)\}_{i\leq k}, X \text{ hierarquia de } C. \\
&\iff n-k+r, n-k+r+1, ..., n \in X \\
&\iff d_k^{(P)} = n, \\
&\quad d_{k-1}^{(P)} = n-1, \\
&\quad\quad ... \\
&\quad d_r^{(P)} = n-k+r \\
&\iff C \text{ é MDS.}
\end{aligned}$$

■

Corolário 7.2.4. Seja P um poset sobre $[n]$. Para um $[n,k]_q$ P-código C, seja $r = n-k+2-d_1^{(P)}(C)$. Então $C^\perp$ é um código $(\overline{P},r)$-MDS com dimensão $n-k$.

Demonstração. .

$$\begin{aligned}
dim(C) = k \Rightarrow dim(C^\perp) &= n-k \\
r = n-k+2-d_1^{(P)} \Rightarrow d_1^{(P)} &= n-k+2-r \\
&= dimC^\perp + 2 - r
\end{aligned}$$

Aplicando a proposição anterior, $C^\perp$ é $(\overline{P},r)$-MDS. ■

8 CÓDIGOS DO TIPO CADEIA

Como será apresentado na primeira definição desta seção, códigos do tipo P-cadeia são aqueles com a propriedade de que há uma sequência de subcódigos D_i aninhados com dimensões $i = 1, \ \ldots, \ k$, sendo k a dimensão do código original, tais que para cada um destes D_i ocorra $w_P(D_i) = d_i^{(P)}(C)$. Esta propriedade é interessante sob o ponto de vista de compactação de informação, se assemelhando aos espaços de escala.

Aqui se concentram as principais contribuições deste trabalho, apresentadas como proposições neste capítulo. Definições, teoremas e corolários podem ser também encontrados em [7].

Definição 8.1.1. Dizemos que um código P $[n,k]_q$ é um código cadeia se existe uma sequência de subespaços lineares D_i, $i = 1, 2, ..., k$ tais que

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

Com

$$w_P(D_i) = d_i^{(P)}(C)$$
$$dim D_i = i$$

Também dizemos que C satisfaz a condição P cadeia.

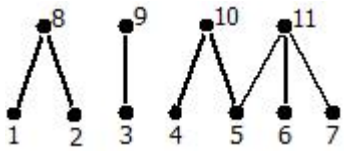

Figura 9 – Poset sobre [11]

Exemplo 8.1.2. Sejam o poset P da Figura 9 e o $[11, 3]_2$-código $C = [v_1 = e_5 + e_{10}e_5 + e_{10} = 00001000010, v_2 = e_3 + e_8 = 00100001000, v_3 = e_1 + e_2 + e_9 = 11000000100]$ sobre P.

Tentemos encontrar uma sequência de subcódigos $\{0\} = D_0 \subsetneq D_1 \subsetneq D_2 \subsetneq D_3 = C$ atendendo à condição P-cadeia. A Tabela 4 exibe os pesos de cada elemento de C.

Da figura, temos que o único candidato possível a D_1 é $[v_1]$. Logo, o código D_2 deve conter D_1, logo,$v_1 \in D_2$. Porém, qualquer subcódigo de C de duas dimensões contendi v_1 tem pelo menos peso 7, enquanto $[v_2, v_3] \subset C$ tem peso 5. Por isso, C não é um código do tipo P-cadeia.

Exemplo 8.1.3. Seja agora o código $D = [u_1 = e_9 = 00000000100, \ u_2 = e_6 + e_7 + e_{11} = 01000110001, \ u_3 = e_2 + e_3 + e_{10} = 01100000010]$. D não apenas é do tipo P-cadeia, como tem duas opções de cadeia: $\{0\} \subsetneq [u_1] \subsetneq [u_1, u_2] \subsetneq D$ e $\{0\} \subsetneq [u_1] \subsetneq [u_1, u_3] \subsetneq D$, com hierarquia $\{2, 4, 9\}$.

Tabela 4 – Pesos de C para o poset P da Figura 9

v	$w_P(v)$
0	0
v_1	3
v_2	4
v_3	4
$v_1 + v_2$	7
$v_1 + v_3$	7
$v_2 + v_3$	5
$v_1 + v_2 + v_3$	8

Proposição 8.1.4. Sejam P um poset em $[n]$ e $1 \leq j_1 < j_2 < ... < j_k \leq n$ uma sequência de números inteiros. Então existe uma sequência de códigos $C_1 \subsetneq C_2 \subsetneq ... \subsetneq C_k = C$ tais que $w_P(C_i) = j_i$.

Demonstração. Pela proposição 5.1.23, considerando P um ideal de si mesmo, podemos encontrar um ideal J_k com $\#J_k = j_k$, $j_k < \#P$.

Podemos então construir C_k como

$$C_k = [B_{J_k}] \cap \mathbb{F}_{\mathrm{q}}^{\mathrm{n}}$$

Seguindo este padrão, podemos definir cada C_i recursivamente, como

$$C_{i-1} = [B_{J_{i-1}}] \cap supp\langle C_i \rangle_P$$

Desta forma, $w(C_i) = \#J_i = j_i$ e $C_i \subseteq C_{i+1}$, $\forall i = 1, ..., k$. ■

É preciso notar, porém, que não necessariamente a sequência de códigos $C_1 \subsetneq C_2 \subsetneq ... \subsetneq C_k$ atende à condição P-cadeia, como verificaremos.

Exemplo 8.1.5. Seja H o poset antilinear sobre $\mathbb{F}_2^6$ e a sequência $\{3, 4\}$.

Temos que

$$3 = d_1^{(H)}(C) = w_H(v_1), [v_1] = D_1$$

Sem perda de generalidade, seja $v_1 = 111000 \in C_1 \subsetneq C_2 = C$.

Para a construção de C_2:

$$4 = d_2^{(H)}(C) = w_P(D_2) = \#supp[v_1, v_2]$$

Como $w(v_1) = 3$, $\#(supp(v_2) \setminus supp(v_1)) = 1$.

Sem perda de generalidade novamente,

$$v_2 = (x_1, x_2, x_3, 1, 0, 0)$$

Como $d_1^{(H)}(C) = 3$

$$
\begin{aligned}
& w_P([v_2]) \geq 3 \\
& \Rightarrow w_P(v_2) \geq 3 \\
& \Rightarrow \text{No máximo, uma componente } x_1, x_2 \text{ ou } x_3 \text{ é nula.} \\
& \Rightarrow d(v_1, v_2) \leq 2 \\
& \Rightarrow \exists v \in C_2; v = v_2 - v_1, w_P(v) \leq 2 < d_1(C_1)
\end{aligned}
$$

Portanto, não existe código C que atenda à condição P-cadeia com a sequência de pesos $\{3, 4\}$.

Exemplo 8.1.6. Seja o poset P da Figura 10. Este poset também não admite códigos P-cadeia de hierarquia $\{3, 4\}$.

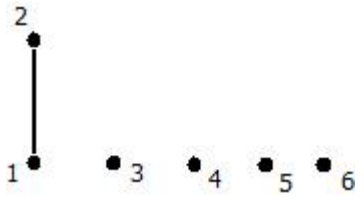

Figura 10 – Poset P sobre [6].

Exemplo 8.1.7. Em contrapartida, tome o poset Q como na Figura 11. Naturalmente, Q é um refinamento do poset P do exemplo anterior, que é um refinamento do poset antilinear H. Escolha $v_1 = 110000$ e $v_2 = 000100$ e construa $E = [v_1, v_2]$.

Como estamos sobre o corpo binário $\mathbb{F}_2$, E tem $2^2 - 1 = 3$ elementos não nulos:

$$
\begin{aligned}
v_1 = 110000 & \qquad & w_P(v_1) = 3 \\
v_2 = 000110 & \Longrightarrow & w_P(v_2) = 3 \\
v_1 + v_2 = 110110 & & w_P(v_1 + v_2) = 4
\end{aligned}
$$

Como podemos notar, $d_1^{(Q)}(E) = 3$, com $E_1 = [v_1]$, por exemplo, e $d_2^{(Q)}(E) = w_Q(E) = 4$ e E é um código do tipo Q-cadeia com sequência $\{3, 4\}$.

Este é um caso a ser retornado mais adiante: para qualquer poset Q existe um refinamento P do tipo P-cadeia.

Proposição 8.1.8. Seja uma sequência de ideais $J_1 \subsetneq J_2 \subsetneq ... \subsetneq J_k$ tal que $\#J_i \leq \#\langle J_{i+1} \backslash J_i \rangle_P$. Então existe uma sequência de códigos lineares sobre $\mathbb{F}_{\mathrm{q}}^{\mathrm{n}}$, $\{0\} = D_0 \subsetneq D_1 \subsetneq D_2 \subsetneq ... \subsetneq D_k = C$, tais que $d_i^{(P)} = w_P(D_i) = \#J_i$.

Demonstração. Construa a base de um código C como $\mathcal{B}_C = \{v_i\}_{i=1,..,k}^k$ tal que $v_i = (x_j)_{j \in [n]}$, $x_j = 1$ se $j \in J_i$ e $x_j = 0$, se $j \notin J_i$.

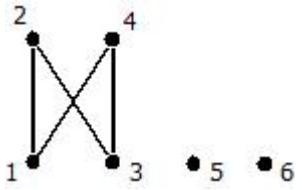

Figura 11 – Poset P. Exemplo 8.1.7

Construa também cada D_i como $D_i = [v_j]_{j \leq i}$.

$$suppD_i = \bigcup_{j=1}^{i} supp(v_i) = \bigcup_{j=1}^{i} J_j = J_i$$

Daí,

$$w_P(D_i) = \#J_i$$

Sejam $s > 0$, D_{i+s}, D_i. Suponha $D' \subset D_{i+s}$; $w_P(D') < w_P(D_i)$, $dimD' = i$. Dessa forma, $D' \cap (D_{i+s} \backslash D_i) = D' \backslash D_i \neq \emptyset$.

Seja $u \in D' \backslash D_i$. Como $D_{i+s} = [v_j]_{j \leq i+s}$, então $\exists \alpha_1, \alpha_2, ..., \alpha_{i+s} \in \mathbb{F}_q$ tais que

$$u = \underbrace{\sum_{l=1}^{s} \alpha_{i+l} v_{i+l}}_{\notin D_i} + \underbrace{\sum_{j=1}^{i} \alpha_j v_j}_{\in D_i}$$

Como $u \notin D_i$, existe $t, 0 < t < s$, tal que $\alpha_{i+t} \neq 0$. Da construção de cada v_i, temos que $J_{i+t} \backslash J_{i+t-1} \subset suppD'$.

Logo,

$$\begin{aligned} w_P(D') = \#\langle suppD' \rangle_P &\geq \#\langle J_{i+t} \backslash J_{i+t-1} \rangle_P \\ &\geq \#J_{i+t-1}, \quad \text{(Pela suposição)} \\ &\geq ... \\ &\geq \#J_i \\ &= w_P(D_i) \end{aligned}$$

$$\Rightarrow w_P(D') \geq w_P(D_i), \forall D', dimD' = i$$
$$\therefore w_P(D_i) = d_i^{(P)}(C)$$

■

Teorema 8.1.9. Se o suporte de um P-código C é um subconjunto de P totalmente ordenado então C satisfaz a condição P-cadeia.

Demonstração. Seja $X = \{\max_{v \in C}(supp(v))\} = \{t_i\}$, com $t_{i-1} < t_i$.

Construa $\mathcal{B}_X = \{v^{(i)}\}_{i \in [\#X]}$; $v^{(i)} = \left(v_j^{(i)}\right)_{j \in [n]}$,

$$\begin{cases} v_j^{(i)} = 1, \text{se } j = t_i \\ v_j^{(i)} = 0, \text{se } t_i \not\preceq_P j \end{cases}$$

Queremos provar por agora que $\#X = k$.

Claramente $\mathcal{B}_X$ é LI $\Rightarrow \#X \leq k$.

Seja então $v \in C$ e faça $u^{(0)} = v$ e

$$\begin{aligned} u^{(1)} &= u^{(0)} - u^{(0)}_{t_{\#X}} v^{(\#X)} \\ u^{(2)} &= u^{(1)} - u^{(1)}_{t_{\#X}} v^{(\#X-1)} \\ &... \\ u^{(\#X-1)} &= u^{(\#X-2)} - u^{(\#X-2)}_{t_2} v^{(2)} \\ u^{(\#X)} &= u^{(\#X-1)} - u^{(\#X-1)}_{t_1} v^{(1)} \end{aligned}$$

Note que em cada iteração a componente $t_{(\#X-i)}$ de $u^{(i)}$ é anulada e não está presente em nenhum $v^{(\#X-j)}$, $j > i$, e, por conseguinte, em nenhum $u^{(j)}, j > i$. Portanto, $u^{(\#X)} = 0$.

Caso $u^{(\#X)} \neq 0$, então haveria $j \in [n]$ tal que $j = max(supp(u^{(\#X)})$, mas como $u^{(\#X)} \in C, j \in X \Longrightarrow u^{(\#X)} = 0$. $\lightning$

Logo,

$$C = [\mathcal{B}_X] \Rightarrow \#X \geq k \Rightarrow \#X = k$$

Resta agora apenas provar que os subcódigos $D_i = [u^{(j)}]_j$ correspondem a uma P-cadeia.

Obviamente, $D_{i-1} \subsetneq D_i$, ok!

Seja $D' \subsetneq C$, $dim(D') = i < k$; $D' \neq D_i$

Para $v \in D' \backslash D_i$, $\exists \alpha_1, \alpha_2, ..., \alpha_k \in \mathbb{F}_q$;

$$v = \underbrace{\sum_{j=i+1}^{k} \alpha_j v^{(j)}}_{\notin D_i} + \underbrace{\sum_{j=1}^{i} \alpha_i v^{(i)}}_{\in D_i}$$

Então, como $v \in D_i$, $\exists s \in [k]$, $i < s \leq k, \alpha_s \neq 0$.

Assim,

$$\begin{aligned} d_s \in supp D', d_i \preceq_P d_s, d_s \not\preceq_P d_i \\ \Rightarrow w_P(D') \geq \#\langle d_s \rangle_P > \#\langle d_i \rangle_P = w_P(D_i) \\ \therefore w_P(D_i) = d_i^{(P)}, \forall i \in P, \\ \{0\} = D_0 \subsetneq D_1 \subsetneq D_2 \subsetneq ... \subsetneq D_k = C, dim D' = i \end{aligned}$$

■

Teorema 8.1.10. Seja um poset P. Um código C satisfaz a condição P-cadeia se, e somente, se $C^{\perp}$ satisfaz a condição P-cadeia também.

A demonstração deste teorema pode ser encontrada em [7]

Proposição 8.1.11. Em um poset totalmente ordenado a relação

$$\begin{aligned} \psi : P &\to [n] \\ i &\mapsto w_P(e_i) \end{aligned}$$

é uma bijeção.

Demonstração. Sejam $i, j \in P$, P linear. Como o poset é totalmente ordenado, $i \preceq_{\mathrm{P}} j$ ou $j \preceq_{\mathrm{P}} i$, necessariamente. Para $i \neq j$, isso significa $\langle i \rangle \subsetneq \langle j \rangle$ ou $\langle j \rangle \subsetneq \langle i \rangle$, respectivamente. Logo, para $i \neq j$, $\psi(i) = w_P(e_i) \neq w_P(e_j) = \psi(j)$ e ψ é injeção. Como $\#P = \#[n] < \infty$, temos que ψ é bijeção. ■

Proposição 8.1.12. Seja P um poset e S um poset linear subconjunto de P. Então

$$\begin{aligned} \psi|_S : S &\to \psi(S) \\ i &\mapsto \psi(i) \end{aligned}$$

é bijeção.

Demonstração.

Sejam $i_1, i_2, \ldots, i_{\#S} \in S$ tais que $i_j \preceq_{\mathrm{P}} i_{j+1}$. Então $\psi|_S$ é injeção. Como o contradomínio foi restrito, segue que $\psi|_S(i)$ é bijeção. ■

Proposição 8.1.13. Sejam P um poset qualquer sobre $[n]$ e $X = \{d_1, d_2, \ldots, d_k\} \subset [n]$. Existe um refinamento Q de P para o qual é possível encontrar um código C do tipo P-cadeia com hierarquia X.

Demonstração.

Do resultado de 5.5.5 temos que o conjunto P pode ser refinado até Q, para o qual X se torna um poset linear. Do *Teorema 8.1.9* resulta que qualquer código de suporte em X é Q-cadeia. Pode-se, então construir subcódigos C_i da forma $C_i = [e_j]_{j \in \mathcal{B}_i}$, $\mathcal{B}_{i+1} = \mathcal{B}_i \cup \{e_{(\psi|_X)^{-1}(d_i)}\}$. Assim, $C_{i+1} \subset C_i$ e $w_P(C_i) = w_P(\mathcal{B}_i) = d_i$. ■

Corolário 8.1.14. Se o suporte de um P-código é um subconjunto de P totalmente ordenado, então $C^{\perp}$ é um código do tipo P-cadeia.

Demonstração.

$$\textit{suppC} \text{ é totalmente ordenado} \implies C \text{ é do tipo } P\text{-cadeia} \iff C^{\perp} \text{ é do tipo } P\text{-cadeia.}$$

■

Corolário 8.1.15. Qualquer $[n, n-1]_q$, $[n, n-2]_q$ código é do tipo P-cadeia para qualquer poset P em $[n]$.

Demonstração.

Pelo Teorema da Dualidade, temos que se a hierarquia de um código C é X, com $\#X = n-1$ ou $n-2$, então a hierarquia de $C^{\perp}$ é $Y = [n]\backslash X$ com $\#Y = 1$ ou 2, respectivamente.

Como todo código de dimensões 1 ou 2 é do tipo cadeia ($\overline{P}$-cadeia, no caso), então $C^{\perp}$ é do tipo $\overline{P}$-cadeia, pelo *Corolário* 8.1.10, C é do tipo P-cadeia. ■

REFERÊNCIAS

[1] SHANNON, C. E. *A Mathematical Theory of Communication*. Bell System Tech. J. **27**, 379-423, 623-656, 1948.

[2] HAYKIN, S. *Sistemas de Comunicação*, quarta edição. Bookman, 2004.

[3] COUTINHO, M. *Corpos finitos e códigos corretores de erros*. Trabalho de Conclusão do Curso de Matemática. Juiz de Fora: UFJF, 2014.

[4] HEFEZ, A; VILLELA, M. *Códigos corretores de erros*. Rio de Janeiro: Série de Computação e Matemática, SBM, 2002.

[5] LIDL, R.; NIEDERREITER, H. *Introduction to Finite Fields and their Applications*. Cambridge: Cambridge University Press, 1986.

[6] MOON, T. *Error Correction Coding: Mathematical Methods and Algorithms*. Wiley, 2005.

[7] MOURA, A. *Dualidade em espaços Poset.* Tese de Doutorado em Matemática. Campinas: UNICAMP, 2010.

[8] MOURA, A; FIRER, M. *Duality for Poset codes*. IEEE TRANSACTIONS ON INFORMATION THEORY, **56**(7), 3180–3186, 2010.

ANEXO A – Teorema de Shannon-Hartley

A informação apresentada neste anexo está toda contida em [1], Teorema 17.

O Teorema de Shannon-Hartley, como enunciado em seu artigo marco da Teoria da Informação estabelece a taxa máxima de informação que pode ser transmitida por um canal com taxa de erro arbitrariamente baixo (denominada capacidade do canal, C) sob as condições de banda W ocupada pelo sinal transmitido (faixa de frequências em que a representação de Fourier do sinal está contida) e relação sinal/ruído, S/N, razão entre a potência do sinal transmitido e o ruído, no caso de te resultado, branco.

A expressão enunciada pelo teorema é:

$$C = Wlog(1 + S/N)$$

A base do logaritmo varia com a unidade utilizada para informação (2 para bits, e para nats e 10 para Hartleys.