LUCIANO VIANNA FELIX

CLASSIFICAÇÃO DE CÓDIGOS RELATIVA ÀS ORDENS HIERÁRQUICAS E PROPRIEDADE DE EXTENSÃO

CAMPINAS
2014

UNIVERSIDADE ESTADUAL DE CAMPINAS

INSTITUTO DE MATEMÁTICA, ESTATÍSTICA
E COMPUTAÇÃO CIENTÍFICA

LUCIANO VIANNA FELIX

CLASSIFICAÇÃO DE CÓDIGOS RELATIVA ÀS ORDENS HIERÁRQUICAS E PROPRIEDADE DE EXTENSÃO

Tese apresentada ao Instituto de Matemática, Estatística e Computação Científica da Universidade Estadual de Campinas como parte dos requisitos exigidos para a obtenção do título de Doutor em Matemática.

Orientador: Marcelo Firer

ESTE EXEMPLAR CORRESPONDE À VERSÃO FINAL DA
TESE DEFENDIDA PELO ALUNO LUCIANO VIANNA FELIX
E ORIENTADA PELO PROF. DR MARCELO FIRER

MARCELO FIRER

CAMPINAS
2014

Ficha catalográfica
Universidade Estadual de Campinas
Biblioteca do Instituto de Matemática, Estatística e Computação Científica
Maria Fabiana Bezerra Muller - CRB 8/6162

F335c

Felix, Luciano Vianna, 1986-
Classificação de códigos relativa às ordens hierárquicas e propriedade de extensão / Luciano Vianna Felix. – Campinas, SP : [s.n.], 2014.

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

1. Códigos corretores de erros (Teoria da informação). 2. Métricas sobre ordens parciais. I. Firer, Marcelo,1961-. II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. III. Título.

Informações para Biblioteca Digital

Título em outro idioma: Classification of codes relative to hierarchical order and extension property
Palavras-chave em inglês:
Error-correcting codes (Information theory)
Poset metrics
Área de concentração: Matemática
Titulação: Doutor em Matemática
Banca examinadora:
Marcelo Firer [Orientador]
Sueli Irene Rodrigues Costa
Marcelo Muniz Silva Alves
Luciano Panek
Michel Marie Deza
Data de defesa: 16-09-2014
Programa de Pós-Graduação: Matemática

Tese de Doutorado defendida em 16 de setembro de 2014 e aprovada

Pela Banca Examinadora composta pelos Profs. Drs.

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

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

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

Prof(a). Dr(a). LUCIANO PANEK

Prof(a). Dr(a). MICHEL MARIE DEZA

Abstract

In this work we consider vector spaces over a finite field equipped with a metric induced by a partial order (poset) and study several aspects of codes embedded in those. Considering hierarchical posets, a canonical-systematic form for linear codes is determined. With this form it is possible to calculate the main metric invariants of coding theory, such as minimal distance, generalized weights, weight hierarchy and the packing radius. This canonical-systematic form also allows to classify MDS and perfect codes and to significantly decrease the complexity of syndrome decoding algorithm.

Considering generic posets, necessary and sufficient conditions are established to ensure the orbits of the group of linear isometries to be determined by the ideals isomorphisms classes (ideal extension property). Some families of posets that satisfy those conditions are presented, including posets that have as a Hasse diagram a level-wise regular rooted tree. In this particular case of trees, it is established an invariant that classifies those orbits. Considering classic operations over posets, it is proved that only ordinal sum preserves the ideal extension property.

Resumo

Neste trabalho são estudados diversos aspectos de códigos em espaços munidos de métricas poset. Considerando posets hierárquicos é determinada uma forma canônica-sistemática de um código linear. Esta forma permite calcular os principais invariantes métricos da teoria de códigos nestes espaços, incluindo distância mínima, pesos generalizados, hierarquia de pesos e o raio de empacotamento. Esta forma canônica-sistemática também permite, considerando métricas poset hierárquicas, classificar códigos MDS e códigos perfeitos e reduzir significativamente a complexidade do algoritmo de decodificação por síndrome.

Considerando posets genéricos, são estabelecidas condições necessárias e suficientes para que órbitas de grupos de isometrias lineares sejam determinadas pelas classes de isomorfismos de ideais (propriedade de extensão de ideais). São apresentadas algumas famílias de posets que satisfazem essa condição, incluindo posets cujo diagrama de Hasse é uma árvore uni-raiz, regular por nível. Neste caso específico de árvore, é determinada um invariante que caracteriza estas órbitas. Considerando as operações clássicas entre posets, é demonstrado que apenas a soma ordinal preserva a propriedade de extensão de ideais.

Sumário

Agradecimento

Gostaria de agradecer aos meus pais Amauri e Suely, à minha irmã Taiana e ao meu primo/irmão Anderson.

Agradeço ao Marcelo. Muito obrigado pelo apoio, paciência e ensinamentos (acadêmicos ou não) nesses anos.

Agradeço aos Professores Luciano, Marcelo, Sueli e Michel que compuseram a banca de avaliação. Suas correções e comentários me ajudaram muito com o encerramento deste texto.

Muito obrigado ao IMECC. Agradeço aos professores e funcionários deste instituto que tanto contribuiu com minha formação.

Aos amigos do Lab, em especial aos Marquinhos, Jerry e Chris que tanto me ajudaram na reta final deste trabalho e aos amigos da Rep Hostel .

Agradeço aos amigos de trabalho do Demat-UFRRJ.

Agradeço ao Professor Marcus Greferath, pela orientação durante o período de pesquisa na University College Dublin.

Agradeço aos órgãos de fomentos CNPq e CAPES pelo suporte financeiro.

Capítulo 1

Introdução

A teoria de Códigos Corretores de Erros considera a transmissão de informação através de um canal com ruído, que causa erros, ou seja, as mensagens recebidas podem diferir das mensagens enviadas. Um modelo de canal é essencialmente uma tripla $(\mathcal{X}, \mathcal{Y}, \mathbb{P})$, onde $\mathcal{X}$ é o conjunto de entrada, $\mathcal{Y}$ o conjunto de saída e $\mathbb{P}$ é modelo probabilístico que determina a probabilidade de se receber uma mensagem $y \in \mathcal{Y}$ dado que $x \in \mathcal{X}$ foi enviado. Um decodificador é um critério de decisão que estabelece uma maneira de interpretar uma mensagem recebida, eventualmente diferente da enviada. De modo geral, o critério de decisão ótimo é o critério de máxima verossimilhança, baseado no modelo probabilístico de canal e que minimiza a probabilidade de erros. De modo mais explícito, se consideramos $\mathcal{X}$ como o conjunto de entrada e de saída e um código como um subconjunto $\mathcal{C} \subseteq \mathcal{X}$, ao se transmitir uma palavra código $x \in \mathcal{C}$, recebe-se uma mensagem y, que eventualmente pode ter sido alterada pelo *ruído do canal*. O critério de máxima verossimilhança diz que devemos interpretar (decodificar) y como sendo o elemento $x' \in \mathcal{C}$ mais provável de ter sido enviado dado que y foi recebido.

Sob determinadas circunstâncias, o critério de máxima verossimilhança coincide com um critério métrico, de máxima proximidade, em outras palavras, considera-se uma métrica $d : \mathcal{X} \times \mathcal{X} \longrightarrow \mathbb{R}$ e sugere-se decodificar y como o elemento $a(y) \in \mathcal{C}$ mais próximo de y.

O caso mais paradigmático é o de um canal binário simétrico sem memória (BSMC na sigla em inglês) e da métrica de Hamming em que os critérios de decisão por máxima proximidade e máxima verossimilhança coincidem, assumindo-se que toda palavra-código $x \in \mathcal{C}$ tenha a

mesma probabilidade de ser enviada.

Os critérios métricos muitas vezes são interessantes por oferecer instrumentos que simplificam os algoritmos de decodificação, o que constatamos, por exemplo, nos algoritmos de síndrome para códigos lineares. Não obstante, o conjunto de métricas utilizadas na teoria manteve-se extremamente reduzida às métricas de Hamming e de Lee [23].

Em 1995, Brualdi [5] introduziu uma nova (e grande) família de métricas, definidas em espaços vetoriais sobre corpos finitos $\mathbb{F}_q$, a partir da definição de uma ordem parcial no conjunto dos índices $[n] = \{1, \ldots, n\}$ (partially ordered set, ou poset na sigla em inglês), chamadas de métricas poset. Esta família de métricas é interessante por admitir decodificação por síndrome de códigos lineares e por ter possíveis aplicações na modelagem de alguns tipos de ruído ([27],[13]), alguns modelos de canal ([21]) ou erros de decodificação com valores semânticos ([9]). Além de possíveis usos práticos, as métricas poset oferecem uma série de desafios, pois alguns conceitos que são trivializados pela métrica de Hamming têm sua diferença amplificada por estas métricas. A título de exemplo, estamos todos acostumados a pensar na "distância mínima" como sendo o parâmetro (de um código) a ser maximizado. Na realidade, o parâmetro realmente importante é o "raio de empacotamento", o qual é confundido com a distância mínima devido ao fato de ambos estarem relacionados, no caso da métrica de Hamming, pela famosa equação $R = \lfloor \frac{d-1}{2} \rfloor$, que aparece no primeiro capítulo de quase todos os livros sobre Códigos Corretores de Erros. As métricas poset questionam este e outros fatos, e colocam uma série de desafios que têm sido estudados nos últimos anos.

Além da métrica de Hamming (caso particular de uma métrica poset), uma outra família que foi adequadamente entendida é a de métricas definidas por uma ordem total (cadeia). Em [3] os autores descrevem uma forma canônica para códigos lineares em espaços munidos desta métrica. A partir desta forma canônica é possível descrever de maneira bastante simples os principais invariantes de um código (distância mínima, pesos generalizados, hierarquia de pesos, raio de empacotamento e raio de cobertura) assim como caracterizar famílias de códigos com propriedades especias (códigos MDS e códigos perfeitos). Por algum tempo, buscou-se generalizar estes resultados para posets determinados por família disjunta de cadeias (métricas NRT), como é o caso, por exemplo de Barg e Purkayastha ([4]). Neste trabalho, seguimos em outra direção e generalizamos os resultados de ([3]) para a família de posets hierárquicos. Esta é uma família grande de posets (essencialmente, a menos de escolha de um rótulo, temos 2^{n-1} posets hierárquicos sobre um conjunto com n elementos) e esta é a família que realmente

generaliza a "sensibilidade" da métrica de Hamming, no sentido que o raio de empacotamento é determinado pela distância mínima se, e somente se, o poset em questão é hierárquico. Mais ainda, esta família pode ser utilizada para determinar limitantes para os invariantes de códigos, ao se considerar métricas poset genéricas. Neste sentido, no Capítulo 3, considerando-se uma métrica definida por um poset hierárquico, é determinada uma decomposição canônica de um código linear e a forma canônica-sistemática da matriz geradora de um código. A partir da decomposição canônica de um código são apresentadas fórmulas simples para os invariantes (distância mínima, pesos generalizados, hierarquia de pesos, raio de empacotamento e raio de cobertura). Além disso, são caracterizados os códigos MDS e perfeitos.

No Capítulo 4, o ponto de partida são as métricas posets definidas por cadeias disjuntas, conforme trabalhado em Barg e Purkayastha ([4]), onde é determinada uma caracterização numérica de um vetor (chamada pelos autores de shape, ou formato, em português), a partir da qual é possível caracterizar uma série de invariantes da teoria. Apesar de não estar explicitado pelos autores, o formato de um vetor é uma característica da órbita pelo grupo de isometrias lineares, ou seja, dois vetores pertencem a mesma órbita se e somente se possuem o mesmo formato (ou shape). Adotando este ponto de vista, procuramos transferir do espaço vetorial $\mathbb{F}_q^n$ para o conjunto de coordenadas $[n] = \{1, \ldots, n\}$ o problema de caracterizar as órbitas distintas pelo grupo de isometrias lineares. Naturalmente, o conjunto de coordenadas é significativamente menor do que o espaço vetorial e, portanto, nem sempre esta caracterização é possível. Este problema é definido pela propriedade que chamamos de extensão de ideais que, essencialmente, afirma que um isomorfismo $\sigma : I \longrightarrow J$, entre ideais $I, J \subseteq [n]$ de um poset $P = ([n], \preceq)$, pode ser estendido a um automorfismo de P. Após demonstrar que a propriedade de extensão pode ser verificada através de uma propriedade do poset, mostramos que algumas famílias de poset satisfazem esta propriedade, incluindo as já mencionadas famílias de poset hierárquicos, NRT e também a família de posets definidos por árvores uni-raiz, regular por nível. Finalmente, mostramos como esta propriedade de extensão se comporta pelas quatro operações clássicas com posets (soma e produto diretos, soma e produto ordinais).

Capítulo 2

Códigos Corretores de Erros

Neste capítulo são apresentados alguns elementos básicos da Teoria de Códigos Corretores de Erros e de Códigos Posets. No que se refere aos códigos posets, são explorados alguns exemplos que ilustram as particularidades desta classe.

Na seção 2.1 são apresentadas as definições e resultados mais elementares sobre códigos corretores de erros. Como referência bibliográfica desta seção, destacam-se [11] e [12].

Na seção 2.2 são estudados os códigos poset, desde a definição de poset até a analise de alguns exemplos. A partir daí, define-se também as métricas poset e uma relação de equivalência entre os códigos posets através de isometrias lineares. Aqui, destacam-se os trabalhos [27], [5], [17] e [2].

2.1 Códigos lineares

Iniciaremos essa seção com alguns conceitos básicos sobre sistemas de comunicação.

Considere um alfabeto de entrada X e um alfabeto de saída Y. Estes alfabetos definem o *conjunto de entrada* $\mathcal{X} = X^n$ e o conjunto de saída $\mathcal{Y} = Y^n$. Sobre os conjuntos de entrada e saída, define-se uma função de probabilidade condicional $\mathbb{P} : \mathcal{X} \times \mathcal{Y} \longrightarrow \mathbb{R}^+$ tal que dados $x \in \mathcal{X}$ e $y \in \mathcal{Y}$, $\mathbb{P}(y|x)$ representa a probabilidade do símbolo y ser recebido, uma vez que o símbolo x foi enviado. Chamamos a tripla $(X, Y; \mathbb{P})$ de (modelo de) canal. Neste trabalho será

considerado sempre que $X = Y = \mathbb{F}_q$, onde $\mathbb{F}_q$ é um corpo finito com q elementos.

Um codificador é uma função (ou algoritmo) que transforma cada sequência de símbolos do alfabeto de mensagem A em elementos do conjunto de saída $\mathcal{X}$, de forma que a redundância é adicionada (para melhorar a proteção contra erros do canal).

Um decodificador é um critério de decisão, uma função que associa cada elemento de $\mathcal{Y}$ a um elemento de A. Como fixamos anteriormente que $Y = \mathbb{F}_q$, temos

$$a : \mathbb{F}_q^n \longrightarrow A.$$

O canal, o codificador, o decodificador, junto com a fonte e o receptor formam um *sistema de comunicação*, como ilustrado na figura seguinte:

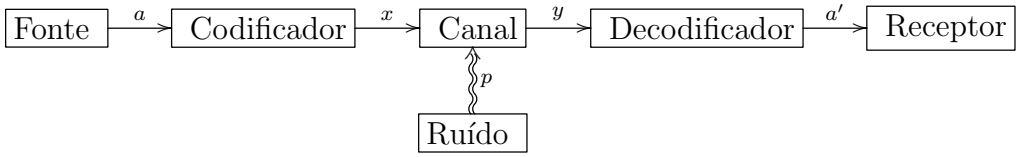


Figura 2.1: Sistema de comunicação

Aqui, a denota a mensagem de A, x um elemento de $\mathcal{X}$, y um elemento de $\mathcal{Y}$ e a' a mensagem final recebida e decodificada.

Um decodificador com a propriedade de sempre decodificar a mensagem recebida a' como a mais provável (em termos da probabilidade do canal) dado que recebeu y é chamado de *decodificador de máxima verossimilhança*.

Aqui serão apresentados apenas os elementos e resultados elementares da Teoria de Códigos Corretores de Erros que serão utilizados neste trabalho. Dentre os inúmeros livros onde esses elementos podem ser encontrados destacam-se [12] e [11].

Definição 2.1. *Seja $\mathbb{F}_q$ um corpo finito com q elementos e $n \in \mathbb{N}$. Um código $\mathcal{C}$ é um subconjunto de $\mathbb{F}_q^n$. Se $\mathcal{C} \subseteq \mathbb{F}_q^n$ for um subespaço vetorial de dimensão k, diremos que $\mathcal{C}$ é um $[n, k]_q$ código linear.*

Neste trabalho, serão considerados apenas códigos lineares.

Dado $x \in \mathbb{F}_q^n$, o *peso de Hamming de* x é a quantidade de entradas não nulas de x, isto é,

$$\omega_H(x) = |\{i; x_i \neq 0\}|.$$

A *métrica de Hamming sobre* $\mathbb{F}_q^n$ é dada por

$$d_H(x, y) = \omega_H(x - y)$$

para todo $x, y \in \mathbb{F}_q^n$. Note que a métrica de Hamming é invariante por translação, isto é, $d_H(x, y) = d_H(x + z, y + z)$ para quaisquer $x, y, z \in \mathbb{F}_q^n$.

2.1.1 Aspectos métricos dos códigos

A métrica de Hamming é uma dentre muitas métricas interessantes que podem ser introduzidas em $\mathbb{F}_q^n$. Aqui são apresentados alguns elementos dos códigos que dependem da métrica adotada.

Lembrando que um decodificador é uma função de $\mathbb{F}_q^n$ no código $\mathcal{C}$, considere a seguinte definição feita para qualquer métrica d.

Definição 2.2. (Decodificador de máxima proximidade) *Um decodificador* $a : \mathbb{F}_q^n \longrightarrow \mathcal{C}$ *é um decodificador de máxima proximidade se*

$$a(y) \in argmin\{d(y, c); c \in \mathcal{C}\},$$

isto é, $a(y)$ *é um elemento de* $\mathcal{C}$ *mais próximo (segundo a métrica* d*) de* y*. Nem sempre este elemento é único. Nestes casos, o decodificador pode escolher qualquer um dos elementos que satisfaça a condição de minimalidade da distância.*

Considere o seguinte exemplo de métrica em $\mathbb{F}_q^n$. Dados $x, y \in \mathbb{F}_q^n$

$$d_P(x, y) = \max\{i; x_i \neq y_i\}. \tag{2.1}$$

Esta métrica será chamada de *métrica cadeia* e é um caso particular das métricas poset (que serão apresentadas mais adiante). Note que, assim como a métrica de Hamming definida anteriormente, essa métrica também é invariante por translação. Os exemplos deste capítulo irão abordar o uso desta métrica e da métrica de Hamming d_H.

Vejamos agora como o decodificador de máxima proximidade se comporta nas diferentes métricas definidas anteriormente.

Exemplo 2.1. *Considere* $\mathcal{C} = \{0000, 1111\}$ *um código* $[4, 1]_2$ *e* $0001 \in \mathbb{F}_2^4$. *Note que* 0001 *e* 0000 *diferem em apenas uma coordenada, portanto,* $d_H(0001.0000) = 1$, *enquanto* 0001 *e* 1111 *diferem nas três primeiras coordenadas, então* $d_H(0001.1111) = 3$, *assim* $a_{d_H}(0001) = 0000$.

Considerando agora a métrica cadeia d_P, *a última coordenada em que* 0001 *e* 0000 *diferem é a quarta, portanto* $d_P(0001, 0000) = 4$ *mas, se compararmos* 0001 *a* 1111, *a última coordenada diferente é a terceira, logo* $d_P(0001, 1111) = 3$. *Com isso* $a_{d_P}(0001) = 1111$.

De maneira geral, para os elementos de $\mathbb{F}_2^4$ *temos a seguinte tabela de decodificação:*

y	a_{d_H}	a_{d_P}
0000	0000	0000
1000	0000	0000
0100	0000	0000
0010	0000	0000
0001	0000	1111
0011^*	$0000, 1111$	1111
0101^*	$0000, 1111$	1111
0110^*	$0000, 1111$	0000
1100^*	$0000, 1111$	0000
1010^*	$0000, 1111$	0000
1001^*	$0000, 1111$	1111
1110	1111	0000
1101	1111	1111
1011	1111	1111
0111	1111	1111
1111	1111	1111

Observe que os elementos da tabela acima, marcados com $*$, *têm mais do que um* a_{d_H}. *Assim, o algoritmo de decodificação pode escolher qualquer elemento deste conjunto.*

Distância mínima e peso de um código

Agora será apresentado um elemento métrico de um código linear $\mathcal{C}$ que determina o quanto as palavras de $\mathcal{C}$ estão dispersas em $\mathbb{F}_q^n$.

Definição 2.3. *Seja $\mathcal{C} \subseteq \mathbb{F}_q^n$ um código $[n,k]_q$ e $\mathbb{F}_q^n$ munido da métrica d. A distância mínima de $\mathcal{C}$ é dada por*

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

Dada uma métrica $d : \mathbb{F}_q^n \times \mathbb{F}_q^n \longrightarrow \mathbb{R}^+$, o peso induzido por d em $\mathbb{F}_q^n$ é dado por $\omega_d(x) = d(x,0)$. Com isso, também podemos definir o peso do código $\mathcal{C}$ induzido por d como

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

Das definições acima, segue que se $\mathcal{C}$ é um código linear então $\omega_d(\mathcal{C}) = d(\mathcal{C})$.

Exemplo 2.2. *Seja $\mathcal{C} = \{0000, 0101, 1010, 1111\}$. Considerando os pesos induzidos por d_H e d_P, os elementos de $\mathcal{C}$ têm os seguintes pesos:*

c	ω_{d_H}	ω_{d_P}
0000	0	0
0101	2	4
1010	2	3
1111	4	4

Como $\mathcal{C}$ é um código linear, segue que $d_H(\mathcal{C}) = \omega_{d_H}(\mathcal{C}) = 2$ e $d_P(\mathcal{C}) = \omega_{d_P}(\mathcal{C}) = 3$.

Raio de Empacotamento

O *raio de empacotamento* $R_d(\mathcal{C})$ de um código $\mathcal{C}$ é o raio máximo tal que as bolas métricas de raio $R_d(\mathcal{C})$ e centradas nos elementos do código não tenham nenhum elemento em comum. Em outras palavras,

Definição 2.4. *O Raio de empacotamento de um código $\mathcal{C}$ relativo à métrica d é:*

$$R_d(\mathcal{C}) := \max\{r \in \mathbb{R}; B_d(c,r) \cap B_d(c',r) = \emptyset \text{ para todo } c, c' \in \mathcal{C}, c \neq c'\},$$

onde $B_d(c,r) = \{x \in \mathbb{F}_q^n, d(x,c) \leq r\}$ é a bola métrica centrada em c de raio r.

Exemplo 2.3. *Considere $\mathcal{C} = \{0000, 0101, 1010, 1111\}$ o código linear apresentado no Exemplo 2.2. $R_{d_H}(\mathcal{C}) = 0$, uma vez que $1101 \in B_{d_H}(1111,1) \cap B_{d_H}(1010,1)$. Já no caso da métrica cadeia d_P tem-se os seguintes conjuntos disjuntos:*

c	$B_{d_P}(c,2)$
0000	$\{0000, 1000, 0100.1100\}$
0101	$\{0101, 1101, 1001, 0001\}$
1010	$\{1010, 0010, 1110, 0110\}$
1111	$\{1111, 0111, 0011, 1011\}$

Como $0000 \in B_{d_P}(1010,3) \cap B_{d_P}(0000,3)$*, segue que* $R_{d_P}(\mathcal{C}) = 2$.

Códigos Perfeitos

Uma importante classe de códigos é a família dos *códigos perfeitos.* Um código $\mathcal{C}$ é dito perfeito em $(\mathbb{F}_q^n, d)$ se a união das bolas métricas centradas nas palavras de $\mathcal{C}$ e raio $R_d(\mathcal{C})$ (o raio de empacotamento de $\mathcal{C}$) cobre $\mathbb{F}_q^n$, isto é, se

$$\mathbb{F}_q^n = \bigcup_{c \in \mathcal{C}} B_d(c, R_d(\mathcal{C})).$$

Códigos perfeitos são importantes porque num código qualquer, nem sempre é possível decodificar, de maneira única, uma palavra recebida.

Exemplo 2.4. *Considere* $\mathcal{C} = \{0000, 0101, 1010, 1111\}$ *o código linear apresentado no Exemplo 2.2. Conforme foi visto no Exemplo 2.3 o raio de empacotamento de* $\mathcal{C}$ *em* $(\mathbb{F}_2^4, d_P)$ *é* 2 *e, observando a tabela dada no mesmo exemplo, tem-se que* $\bigcup_{c \in \mathcal{C}} B_{d_P}(c,2) = \mathbb{F}_2^4$*. Portanto,* $\mathcal{C}$ *é perfeito em* $(\mathbb{F}_2^4, d_P)$.

Limitante de Singleton e códigos MDS

Em [25], R.C. Singleton enunciou e demonstrou o seguinte resultado para códigos com a métrica de Hamming:

Teorema 2.1. *Se* $\mathcal{C}$ *é um código* $[n,k]_q$ *com distância mínima* $d = d(\mathcal{C})$*, então* $d \leq n - k + 1$.

Em [14] os autores generalizam este resultado para qualquer código poset, isto é, tem-se:

Teorema 2.2. *Se P é um poset e $\mathcal{C} \subseteq (\mathbb{F}_q^n, d_P)$ é um $[n,k]_q$ código com distância mínima $d = d(\mathcal{C})$, então*

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

Estes resultados são conhecidos como *Limitante de Singleton*. Se um código atinge esta desigualdade, isto é, se $\mathcal{C}$ é um código tal que $d = n - k + 1$, dizemos que $\mathcal{C}$ é um código *MDS* (do inglês *Maximum-distance separable* [25],[14]). Estes códigos recebem este nome pois possuem a maior distância mínima possível para seus parâmetros (n e k) e, como foi visto anteriormente, a distância mínima determina o quanto as palavras do código estão dispersas no espaço.

Exemplo 2.5. *Seja $\mathcal{C} = \{0000, 0101, 1010, 1111\}$ o código linear apresentado no Exemplo 2.2. Note que $\mathcal{C}$ é um subespaço vetorial de $\mathbb{F}_2^4$ de dimensão 2, uma vez que $\{0101, 1010\}$ é uma base de $\mathcal{C}$. Segue do Exemplo 2.2 que o peso mínimo de $\mathcal{C}$, segundo o peso induzido pela métrica cadeia, é $\omega_{d_P}(\mathcal{C}) = 3$. Assim $d_P(\mathcal{C}) = \omega_{d_P} = 3 = n - k + 1 = 4 - 2 + 1$, ou seja, $\mathcal{C}$ é um código MDS em $(\mathbb{F}_2^4, d_P)$.*

2.1.2 Matriz geradora e de paridade

Seja $\mathcal{C}$ é um código $[n,k]_q$ tal que $\beta = \{v_1, \ldots, v_k\}$ é um conjunto de geradores de $\mathcal{C}$. A matriz G de dimensões $k \times n$ e cujas linhas são os elementos de β, é uma *matriz geradora* para $\mathcal{C}$.

É fato conhecido que as seguintes operações entre os elementos de uma base não alteram o espaço vetorial gerado por ela.

(i) Permutação de dois elementos da base;

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

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

Segue então que duas matrizes geradoras de um mesmo código podem ser obtidas, uma da outra, por uma sequência de operações do tipo:

($l1$) Permutação de duas linhas;

($l2$) Multiplicação de uma linha por um escalar não nulo;

($l3$) Adição de um múltiplo escalar de uma linha a outra.

Mais ainda, duas bases ordenadas, de um mesmo código, podem ser transformadas uma na outra por meio das transformações $(i), (ii)$ e (iii). Essencialmente $(l1), (l2)$ e $(l3)$ são as operações do escalonamento de matrizes e os equivalentes em termos matriciais das operações $(i), (ii)$ e (iii).

Definição 2.5. *Seja $\mathcal{C}$ é um código $[n,k]_q$. Uma matriz H de dimensões $(n-k)\times n$, de posto máximo, tal que $Hv^t = 0$ para todo $v \in \mathcal{C}$ é dita uma matriz de teste de paridade de $\mathcal{C}$.*

Seja $\mathcal{C}$ um código que admita G como matriz geradora. Para determinar se um elemento $y \in \mathbb{F}_q^n$ é um elemento de $\mathcal{C}$, é necessário resolver o sistema $Gx^t = y$, para algum $x \in \mathbb{F}_q^n$. Esse processo pode ter um alto custo computacional. Nesse sentido, a matriz de teste de paridade representa uma economia, uma vez que se H é uma matriz de teste de paridade de $\mathcal{C}$, para determinar se $y \in \mathcal{C}$, basta verificar se $Hy^t = 0$.

2.1.3 Isometrias e equivalências entre códigos

Nesta seção, será feito o estudo de uma relação de equivalência entre códigos, via isometrias lineares, de maneira que as propriedades métricas sejam preservadas.

Definição 2.6. *Sejam $\mathcal{C} \subseteq (\mathbb{F}_q^n, d_1)$ e $\mathcal{C}' \subseteq (\mathbb{F}_q^n, d_2)$ dois códigos. $\mathcal{C}$ e $\mathcal{C}'$ são ditos (d_1,d_2)-equivalentes se existe uma isometria linear $T : (\mathbb{F}_q^n, d_1) \longrightarrow (\mathbb{F}_q^n, d_2)$ tal que $T(\mathcal{C}) = \mathcal{C}'$. Se $d_1 = d_2 = d$, $\mathcal{C}$ e $\mathcal{C}'$ são ditos d-equivalentes.*

Exemplo 2.6. *Dados os espaços $(\mathbb{F}_2^2, d_H)$ e $(\mathbb{F}_2^2, d_P)$, os conjuntos das isometrias lineares são, respectivamente, $G_H = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\}$ e $G_P = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\}$.*

Considere os códigos $\mathcal{C}_1 = \{00, 10\}, \mathcal{C}_2 = \{00, 01\}$ e $\mathcal{C}_3 = \{00, 11\}$. Desta forma, $\mathcal{C}_1$ e $\mathcal{C}_2$ são d_H-equivalentes, mas não são d_P-equivalentes, enquanto $\mathcal{C}_2$ e $\mathcal{C}_3$ são d_P-equivalentes mas não são d_H-equivalentes.

As classes de equivalência dependerão diretamente das métricas adotadas. No caso de códigos com a métrica de Hamming (d_H), permutações nas coordenadas dos elementos de $\mathbb{F}_q^n$

são isometrias. Assim, se $\mathcal{C} \subseteq (\mathbb{F}_q^n, d_H)$, onde d_H é a métrica de Hamming e G é uma matriz geradora de $\mathcal{C}$, efetuando sobre G as operações

$(c1)$ Permutação de duas colunas;

$(c2)$ Multiplicação de uma coluna por um escalar não nulo.

gera-se uma matriz G' de um código $\mathcal{C}'$ que é d_H-equivalente a $\mathcal{C}$.

Dessa maneira, realizando as operações $(l_1), (l_2), (l_3), (c_1)$ e (c_2) sobre a matriz geradora G, de $\mathcal{C}$, obtemos a equivalência entre $\mathcal{C}$ e um código cuja matriz geradora seja

$$G' = (id_k|A)\,,$$

onde id_k é a matriz identidade de dimensão k e A é uma matriz de dimensões $k \times (n-k)$. Esta matriz é chamada de *matriz geradora na forma sistemática de* $\mathcal{C}$.

Observação 2.1. *Se $G = (id_k|A)$ é uma matriz geradora de um código $\mathcal{C}$ em $\mathbb{F}_q^n$, então $H = (-A|id_{n-k})$ é uma matriz de teste de paridade de $\mathcal{C}$.*

2.1.4 Decodificação por Síndrome

Nesta seção será estudada uma importante etapa do sistema de comunicação, a *decodificação com correção de erros*. Apesar de existirem outros tipos de decodificadores, este trabalho concentra-se apenas nos decodificadores de mínima distância. Para isso, considere $\mathcal{C}$ um código $[n,k]_q$ e $\mathbb{F}_q^n$ munido da métrica d.

Aqui será utilizada a matriz de teste de paridade de um código para corrigir erros. Para isso será apresentado o *Algoritmo de Decodificação por Síndrome.*

Seja $\mathcal{C}$ um código que admita como matriz de teste de paridade uma matriz H de dimensões $(n-k) \times n$. Para todo $v \in \mathbb{F}_q^n$, a *síndrome de* v é definida por Hv^t. Considere a seguinte coleção de conjuntos:

$$v + \mathcal{C} = \{v + c; c \in \mathcal{C}\}.$$

Note que se $u, v \in \mathbb{F}_q^n$, são tais que $Hu^t = Hv^t$, então $H(u-v)^t = 0$, que implica que $u - v = c \in \mathcal{C}$. Isto é, u e v têm a mesma síndrome se, e somente se, $u \in v + \mathcal{C}$. Ainda mais, os conjuntos $v + \mathcal{C}$ têm as seguintes propriedades:

(i) $v + \mathcal{C} = u + \mathcal{C} \Leftrightarrow v - u \in \mathcal{C}$;

(ii) $(v + \mathcal{C}) \cap (u + \mathcal{C}) \neq \emptyset \Rightarrow v + \mathcal{C} = u + \mathcal{C}$;

(iii) $\bigcup_{v \in \mathbb{F}_q^n} (v + \mathcal{C}) = \mathbb{F}_q^n$;

(iv) $|v + \mathcal{C}| = |\mathcal{C}| = q^k$.

Cada conjunto da forma $v + \mathcal{C}$ é chamado de *classe lateral* de v segundo $\mathcal{C}$. Dos itens (ii) e (iii) acima segue que as classes laterais definem uma partição de $\mathbb{F}_q^n$ e do item (iv) que o número de classe laterais segundo $\mathcal{C}$ é q^{n-k}. Com isso, $\mathbb{F}_q^n$ pode ser escrito como a seguinte união disjunta

$$\mathbb{F}_q^n = (v_0 + \mathcal{C}) \dot{\cup} (v_1 + \mathcal{C}) \dot{\cup} \ldots \dot{\cup} (v_{q^{n-k}-1} + \mathcal{C})$$

Dada a classe lateral $v_i + \mathcal{C}$ o *elemento líder de* $v_i + \mathcal{C}$ é escolhido de forma que satisfaça:

$$\tilde{v_i} \in \operatorname{argmin}\{\omega_d(v_i + c); c \in \mathcal{C}\}.$$

Abaixo é apresentada uma proposição que auxilia na determinação dos elementos líderes das classes laterais de $\mathcal{C}$.

Proposição 2.1. *Seja $\mathcal{C}$ um código em $\mathbb{F}_q^n$, d uma métrica em $\mathbb{F}_q^n$ invariante por translação e $\tilde{v_i}$ um elemento líder de uma classe lateral de $\mathcal{C}$. Se $\omega_d(\tilde{v_i}) \leq R_d(\mathcal{C})$ então ele é o único elemento líder de $\tilde{v_i} + \mathcal{C}$.*

Demonstração: Suponha que $x, y \in \mathbb{F}_q^n$ são elementos líderes da mesma classe lateral de $\mathcal{C}$ tais que $\omega_d(x), \omega_d(y) \leq R_d(\mathcal{C})$.

Como x, y são elementos da mesma classe lateral, segue que $x - y = c \in \mathcal{C}$, logo $x = y + c$. Assim,

$d(x, 0) = \omega_d(x) \leq R_d(\mathcal{C})$, então $x \in B_d(0, R_d(\mathcal{C}))$.

$d(x, c) = d(y + c, c) = d(y, 0) = \omega_d(y) \leq R_d(\mathcal{C})$, então $x \in B_d(c, R_d(\mathcal{C}))$.

Então $x \in B_d(0, R_d(\mathcal{C})) \cap B_d(c, R_d(\mathcal{C}))$. Por definição de raio de empacotamento, tem-se que $B_d(0, R_d(\mathcal{C})) \cap B_d(c, R_d(\mathcal{C})) = \emptyset$ para todo $c \in \mathcal{C} \backslash \{0\}$. Segue que $c = 0$ portanto $x = y$ ■

Seja $r = c + e$, onde $r \in \mathbb{F}_q^n$ é a mensagem a ser decodificada, $c \in \mathcal{C}$ e e o erro. Calculando a síndrome da mensagem recebida tem-se

$$Hr^t = Hc^t + He^t = 0 + He^t = He^t,$$

ou seja, a mensagem a ser decodificada e o erro têm a mesma síndrome e, portanto, pertencem à mesma classe lateral de $\mathcal{C}$. Como o decodificador é um decodificador de máxima proximidade, é assumido que o erro é o elemento de menor peso possível. Como e está na mesma classe lateral de $\mathcal{C}$ que r, e é o elemento líder de $r + \mathcal{C}$.

Agora será apresentado um algoritmo de decodificação com correção de erros. A preparação deste algoritmo exige a determinação de todos os elementos $u \in \mathbb{F}_q^n$ tais que $\omega_d(u) \leq R_d(\mathcal{C})$. Em seguida, calcula-se as síndromes desses elementos e coloca-se esses valores numa tabela. Seja r a palavra recebida a ser decodificada.

Algoritmo 2.1. Decodificação por síndrome em códigos com a métrica de Hamming

(*i*) *Calcule a síndrome* $s^t = Hr^t$;

(*ii*) *Procure* s *na tabela. Seja* ℓ *o elemento líder da classe determinada por* s*. Troque* r *por* $r - \ell$;

Observação 2.2. *A complexidade do algoritmo de decodificação por síndrome em códigos com a métrica de Hamming é determinada, essencialmente, pela busca de elementos líderes das classes laterais. Como foi visto anteriormente, um código* $[n, k]_q$ *tem exatamente* q^{n-k} *classes laterais, portanto,* q^{n-k} *elementos líderes das classes laterais.*

2.2 Códigos Poset

Nesta seção serão apresentados alguns conceitos básicos sobre posets e códigos posets, apenas aqueles estritamente necessários para este trabalho. Como referência básica, sugere-se [8].

Uma *relação* R de X em Y é um subconjunto de $X \times Y$. Quando $X = Y$, dize-se simplesmente que R é uma relação em X.

Uma relação R em X é dita uma *relação de ordem parcial* se satisfaz as segintes propriedades:

Reflexiva Para todo $x \in X, (x, x) \in R$;

Transitiva Se (x, y) e $(y, z) \in R$, então $(x, z) \in R$;

Anti-simétrica Se (x, y) e $(y, x) \in R$, então $x = y$.

Se R é uma relação de ordem parcial em X e $(x, y) \in R$, x e y são ditos *comparáveis* e denota-se por $x \preceq y$.

Sejam X e $\preceq$ uma relação de ordem parcial em X. O par $P = (X, \preceq)$ é chamado de *conjunto parcialmente ordenado* ou *poset* (abreviação de *partially ordered set*, conjunto parcialmente ordenado, em inglês). Se quaisquer dois elementos de X são comparáveis, então $\preceq$ é uma *relação de ordem total* e $(X, \preceq)$ é um *conjunto totalmente ordenado.*

Um subconjunto I de X é um *ideal* se para todo $i \preceq j$ com $j \in I$ tem se $i \in I$. O conjunto de todos os ideais de P é denotado por $\mathcal{I}(P)$. Isto é,

$$\mathcal{I}(P) = \{Y \subseteq X | Y \text{ é um ideal em } X\}$$

Dado $Y \subseteq X$, o *ideal gerado por* Y é o menor ideal de P que contém Y, ou seja,

$$\langle Y \rangle = \bigcap_{\substack{I \in \mathcal{I}(P) \\ Y \subseteq I}} I$$

Um *diagramas de Hasse* de um poset $P = (X, \preceq)$ é um grafo orientado que tem X como conjunto de vértices e uma aresta (orientada) liga y a x se $x \prec y$ e se existe $z \in X$ tal que $x \preceq z \preceq y$, então $x = z$ ou $y = z$. Quando ilustrado no plano, convenciona-se que se $x \prec y$, então o ponto que representa y está "mais alto" que o que representa x, de modo que é possível omitir as setas na representação gráfica do grafo.

Definição 2.7. *Se $P = (X, \preceq)$ é um poset, $i \in X$ é um elemento minimal de P se não existe $j \in X$ tal que $j \prec i$. Um elemento $i \in X$ é um elemento maximal de P se não existe $j \in X$ tal que $i \prec j$.*

Uma cadeia em um poset é um subconjunto $Y \subseteq X$ totalmente ordenado. Isto é, dados $x, y \in Y$ temos que $x \preceq y$ ou $y \preceq x$. Neste caso, podemos rotular os elementos de Y como $i_1, i_2, \ldots, i_r$ de modo que $i_1 \prec i_2 \prec \ldots \prec i_r$. Se $Y = \{i_1, i_2, \ldots, i_r\}$ for uma cadeia, diz-se que r é o comprimento da cadeia.

Dado $i \in X$, a altura, $l(i)$, de i é o comprimento da maior cadeia que tem i como elemento maximal, ou seja,

$$l(i) = \max\{l; i_1 \prec i_2 \prec \ldots \prec i_l = i;\ i_1 \text{ é um elemento minimal de } P\}$$

O k-ésimo nível, H_k, do poset P é o conjunto de elementos de X de altura k, isto é,

$$H_k = \{i \in X; l(i) = k\}.$$

A altura de P é a maior altura que algum de seus elementos pode atingir, ou seja, a altura de P é dada por $l(P) = \max\{l(i); i \in X\}$.

Neste trabalho serão consideradas as relações de ordem parcial sobre o conjunto $[n] := \{1, \ldots, n\}$, onde $n \in \mathbb{N}$, e sobre esses posets, a menos que seja dito o contrário, será sempre considerado um *rotulamento natural*, isto é, se $n_i = |H_i|$ é a cardinalidade do i-ésimo nível de P, então

$$H_k = \left\{ \left(\sum_{1 \leq i \leq k-1} n_i \right) + 1, \left(\sum_{1 \leq i \leq k-1} n_i \right) + 2 \ldots, \left(\sum_{1 \leq i \leq k} n_i \right) \right\}.$$

No restante desta seção serão apresentadas algumas famílias importantes de posets sobre conjuntos finitos.

Exemplo 2.7. Poset anti-cadeia

Um poset anti-cadeia é um poset $P = ([n], \preceq)$ tal que $i, j \in P, i \preceq j$ se, e somente se, $i = j$, ou seja, dois elementos distintos nunca são comparáveis. Segue que em um poset anti-cadeia todos os elementos têm altura 1.

Figura 2.2: Diagrama de Hasse de um $([6], \preceq)$ poset anti-cadeia.

Exemplo 2.8. Poset cadeia

Seja $P = ([n], \preceq)$ um poset com uma relação de ordem total, ou seja, (assumindo o rotulamento natural) dados $i, j \in [n]$, $i \preceq j$ se, e somente se, $i \leq j$, onde $\leq$ é a relação de ordem usual dos inteiros.

Um poset cadeia sobre $[n]$ tem altura n e cada nível tem apenas um elemento.

Exemplo 2.9. Poset NRT

Posets NRT(Niederreiter, Rosenbloom, Tsfasman) foram apresentados em [27] e [17]. Um poset NRT é definido para cada decomposição $n = m.h$ colocando-se

$$i \preceq j \Leftrightarrow \text{ existe } 0 \leq l \leq m-1 \text{ tal que } lh < i \leq j \leq (l+1)h$$

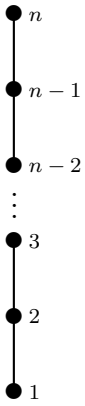


Figura 2.3: Diagrama de Hasse de um $([n], \preceq)$ poset cadeia.

Um poset NRT definido pela decomposição $n = m.h$ é a união disjunta de m posets cadeia, cada uma delas de altura h.

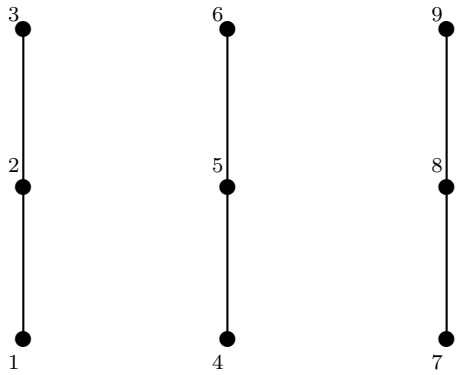


Figura 2.4: Diagrama de Hasse de um $([9], \preceq)$ poset NRT.

Exemplo 2.10. Árvores uni-raiz [1]

Um poset $P = ([n], \preceq)$ é uma árvore uni-raiz se :

(*i*) *Possui um único elemento minimal, que será chamado de raiz de P;*

(*ii*) *Para todo $i \in [n]$, exceto a raiz, existe um outro $j \in [n]$ tal que $j \prec i$;*

(*iii*) *Para todo elemento $i \in P$ o ideal gerado por $\{i\}$ é totalmente ordenado.*

Sejam $i,\ j \in P$ tais que $i \preceq j$ e $\nexists\ k \in [n]$ tal que $i \prec k \prec j$, então j é filho de i e i é pai de j. Segue do item (ii) que cada elemento (exceto a raiz) possui um pai e do item (iii) que esse pai é único.

Uma árvore uni-raiz de altura h é dita regular por nível, se todo elemento no k-ésimo nível de P possui exatamente q_k filhos, para $k = 1, \ldots, h-1$. Denotaremos uma árvore uni-raiz, regular por nível por $(n; q_1, q_2, \ldots, q_{h-1})$, onde q_i é a quantidade de filhos dos elementos do i-ésimo nível. Note que $n = 1 + q_1 + q_1q_2 + \ldots + q_1q_2 \ldots q_{h-1}$.

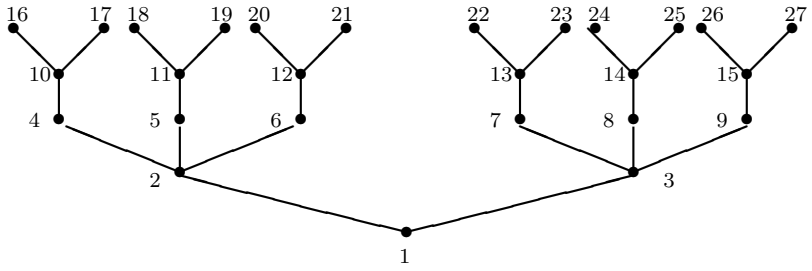


Figura 2.5: Diagrama de Hasse de uma $(27; 2, 3, 1, 2)$ árvore uni-raiz, regular por nível.

No exemplo da figura 2.5, o primeiro nível é composto apenas pelo elemento $\{1\}$. O segundo nível é composto por $\{2, 3\}$; o terceiro nível são os elementos $\{4, 5, 6, 7, 8, 9\}$; o quarto nível é $\{10, 11, 12, 13, 14, 15\}$ e o quinto nível é o conjunto $\{16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27\}$. Note também que todos os elementos do segundo nível têm exatamente 3 filhos, os elementos do terceiro nível apenas 1 filho e os elementos do quarto nível têm 2 filhos.

Exemplo 2.11. Poset Hierárquico

Um poset $P = ([n], \preceq)$ é um $(n; n_1, \ldots, n_h)$ poset hierárquico se existe uma partição

$$[n] = \overset{\circ}{\bigcup_{l=1,\ldots,h}} H_l$$

de $[n]$ tal que $i \preceq j$ se, e somente se $i = j$ ou $i \in H_{l_i}, j \in H_{l_j}$ e $l_i < l_j$. Cada classe H_i é o i-ésimo nível de P, $|H_i| = n_i$ e h é a altura do poset. Para evitar somatórios nas contas a seguir, defina $s_i = \sum_{j=1}^{i} n_j$, a quantidade de elementos de P até (incluindo) o nível i.

Note que o poset hierárquico é a generalização do poset cadeia e anti-cadeia, uma vez que o poset cadeia é um poset hierárquico com altura n e um poset anti-cadeia é um poset hierárquico com altura 1.

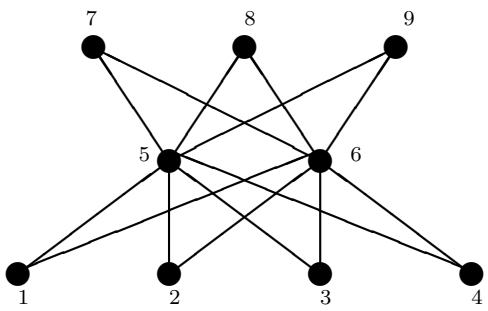


Figura 2.6: Diagrama de Hasse de um $(9; 4, 2, 3)$ poset hierárquico

Exemplo 2.12. Poset de posets

O conjunto de todos os posets sobre $[n]$ também é um poset com a seguinte relação de ordem: dados $P = ([n], \preceq_P)$ e $Q = ([n], \preceq_Q)$, $P \preceq Q$ se $i \preceq_P j \Rightarrow i \preceq_Q j$. Desta forma, assumindo apenas o rotulamento natural dos posets sobre $[n]$, os elementos minimal e maximal deste poset são os posets anti-cadeia e cadeia, respectivamente.

Exemplo 2.13. Poset dual

Dado um poset $P = ([n], \preceq_P)$, seja $P^\perp = ([n], \preceq_{P^\perp})$ um poset, tal que $i \preceq_{P^\perp} j \Leftrightarrow j \preceq_P i$. Com essa relação de ordem $P^\perp = ([n], \preceq_{P^\perp})$ é o poset dual de P.

Os ideais de $P^\perp$ serão chamados de filtros de P e o conjunto dos filtros de P será denotado por $\mathcal{F}(P)$. Isto é, $\mathcal{F}(P) = \mathcal{I}(P^\perp)$.

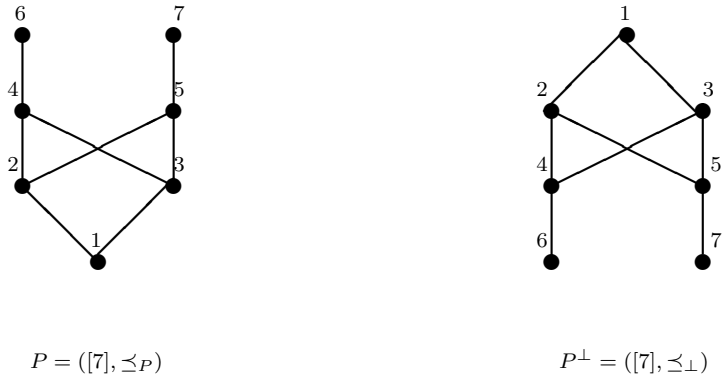


Figura 2.7: Diagrama de Hasse de P e de $P^\perp$, respectivamente.

2.2.1 Métrica poset

Nesta seção será apresentada uma família de métricas em $\mathbb{F}_q^n$ que generaliza tanto a métrica de Hamming quanto a métrica d_P introduzida na equação (2.1). Esta família de métricas foi apresentada pela primeira vez em [5] e desde então vem sendo largamente estudada.

Definição 2.8. *Dado $x = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$, o suporte de x é o conjunto dos índices das coordenadas não nulas desse vetor, ou seja,*

$$\operatorname{supp}(x) = \{i; x_i \neq 0\}$$

Definição 2.9. *Seja $P = ([n], \preceq)$ um poset e $x \in \mathbb{F}_q^n$. O P-peso de x é definido por:*

$$\omega_P(x) = |\langle \operatorname{supp}(x) \rangle|.$$

Isto é, $\omega_P(x)$ é a cardinalidade do ideal gerado por $\operatorname{supp}(x)$.

Assim como é feito no caso do peso de Hamming, o P-peso define uma métrica em $\mathbb{F}_q^n$ da seguinte maneira:

Definição 2.10. *Dados $x, y \in \mathbb{F}_q^n$, a métrica poset é dada por*

$$d_P(x, y) = \omega_P(x - y).$$

O espaço $\mathbb{F}_q^n$ munido da métrica d_P é dito um espaço poset ou P-espaço. Se $\mathcal{C} \subseteq (\mathbb{F}_q^n, d_P)$ é um código $[n, k]_q$, $\mathcal{C}$ é dito um código poset ou um P-código.

Note que se P é um poset anti-cadeia, então ω_P e d_P são os peso e a métrica de Hamming, respectivamente. Se P for um poset cadeia, então d_P é a métrica apresentada na equação (2.1). Nesse sentido, o peso e a métrica poset generalizam tanto o peso e métrica de Hamming quanto o peso e a métrica cadeia.

Exemplo 2.14. *Considere em $\mathbb{F}_2^{10}$ as P-métricas dadas pelos posets P, Q, R, S, onde P é um poset anti-cadeia, Q um poset cadeia, R um $(10; 3, 2)$ poset árvore uni-raiz, regular por nível, S um $(10; 3, 4, 3)$ poset hierárquico. Tome $v = (0000000010) \in \mathbb{F}_2^{10}$, ou seja,* $\operatorname{supp}(v) = \{9\}$. *Assim:*

Poset	$\langle \text{supp}(v) \rangle$	$\omega_P(v)$
P	$\{9\}$	1
Q	$\{1,2,3,4,5,6,7,8,9\}$	9
R	$\{1.4,9\}$	3
S	$\{1,2,3,4,5,6,7,9\}$	8

Distribuição de pesos

Dado D um subespaço de $\mathbb{F}_q^n$, denote por $\text{supp}(D)$ os elementos de $[n]$ que pertençam ao suporte de alguma palavra de D, isto é,

$$\text{supp}(D) = \{i \in [n]; x_i \neq 0 \text{ para algum } x \in D\}.$$

Em [28] Wei definiu o peso generalizado de Hamming de um código $\mathcal{C}$ da seguinte maneira:

Definição 2.11. *Seja $\mathcal{C}$ um código $[n,k]_q$ e $i = 1,\ldots,k$. O i-ésimo peso generalizado de Hamming de $\mathcal{C}$, denotado por δ_i, é definido por*

$$\delta_i := \delta_i(\mathcal{C}) = \min\{|\text{supp}(D)|; D \subseteq \mathcal{C} \text{ e } dim(D) = i\}.$$

A *hierarquia de pesos* de um código $\mathcal{C}$ é a k-upla

Generalizando as definições anteriores para o âmbito das métricas poset, tem-se que dado $i = 1,\ldots,k$, o *i-ésimo* P-peso generalizado de $\mathcal{C}$ é:

$$\delta_{P,i} := \delta_{P,i}(\mathcal{C}) = \min\{|\langle \text{supp}(D) \rangle|; D \subseteq \mathcal{C} \text{ e } dim(D) = i\}$$

Note que $\delta_{P,1} = \omega_{d_P}(\mathcal{C})$, é o peso do código $\mathcal{C}$.

A hierarquia de P-pesos generalizados de $\mathcal{C}$ é a k-upla $\{\delta_{P,i}(\mathcal{C}); i = 1,\ldots,k\}$.

2.2.2 Equivalência entre códigos poset

Na seção 2.1.3 foi introduzido o conceito de equivalência entre códigos dizendo que dois códigos são equivalentes se existir uma isometria linear entre eles. Considere agora a classificação das

isometrias em espaços com métricas poset. Para isso, é necessário introduzir o conceito de isomorfismo de ordem em posets.

Definição 2.12. *Sejam $P = ([n], \preceq_P)$ e $Q = ([n], \preceq_Q)$ dois posets e $T : [n] \longrightarrow [n]$ uma bijeção. T é um isomorfismo de ordem se $i \preceq_P j \Leftrightarrow T(i) \preceq_Q T(j)$. Se $P = Q$, então T é dito um automorfismos de posets.*

Em [2] Alves, Firer e Panek classificam o grupo das isometrias lineares de espaços bloco-poset, uma ideia ainda mais geral que a dos espaços poset. O grupo das isometrias lineares de $(\mathbb{F}_q^n, d_P)$ é denotado por $GL_P(n)$. O Teorema 4.11 de [2] afirma que:

$$GL_P(n) \cong \mathcal{U}(P) \rtimes Aut(P),$$

onde $Aut(P)$ denota o grupo dos automorfismos do poset P e $\mathcal{U}(P)$ é o grupo das matrizes triangulares superiores $A = (a_{ij})$, de ordem n, tais que $a_{ij} = 0$ se $i \not\preceq j$ e $a_{ii} \neq 0$.

Em [20] os autores estabelecem uma relação entre os automorfismos de um poset P e as isometrias do espaço $(\mathbb{F}_q^n, d_P)$. Estes estudos contribuíram substancialmente para o entendimento da essência das isometrias em espaços poset nos levando aos resultados do presente trabalho.

Considere agora os grupos de isometrias lineares de $(\mathbb{F}_q^n, d_P)$ para alguns casos particulares de posets.

Se P é o poset anti-cadeia (portanto, d_P é a métrica de Hamming) $\mathcal{U}(P) = \{id_n\}$ e $Aut(P) = S_n$, onde S_n é o grupo das permutações sobre $[n]$. Se P é o poset cadeia, $\mathcal{U}(P)$ é o grupo de todas as matrizes triangulares superiores e $Aut(P) = \{id\}$. Se P é um poset hierárquico do tipo $(n; n_1, \ldots, n_h)$, então $Aut(P) = S_{n_1} \otimes S_{n_2} \otimes \ldots \otimes S_{n_h}$ e $A \in \mathcal{U}(P)$ se, e somente se

$$A = \left(\begin{array}{c|c|c|c} id_{n_1} & * & * & * \\ \hline 0 & id_{n_2} & * & * \\ \hline \vdots & 0 & \ddots & * \\ \hline 0 & \cdots & 0 & id_{n_h} \end{array}\right),$$

onde $*$ pode assumir qualquer valor.

Capítulo 3

Estrutura e Classificação dos Códigos Poset Hierárquico

Métricas posets foram apresentadas por Brualdi, Graves e Lawrence em 1995 [5], generalizando tanto a métrica de Hamming quanto a métrica NRT (ver [17], [18] e [27]). Desde então códigos com esse tipo de métrica vêm sendo estudados em diferentes aspectos, incluindo um dos principais problemas da teoria de códigos que é determinar os principais parâmetros de um código, tais como distância mínima e a distribuição de pesos generalizada de Wei.

Em [3] Alves, Paneck e Firer classificaram os códigos em um espaço com a métrica bloco-cadeia, uma generalização da métrica cadeia. Esta classificação foi baseada em uma forma canônica para a matriz geradora do código, uma forma "mais limpa" que a forma sistemática usual e que é canônica no sentido de que é determinada pela hierarquia de P-pesos. Essa forma canônica é obtida considerando-se o conhecimento do grupo de isometrias lineares dos espaços com métrica poset, como pode ser visto na seção 2.2.2.

Este capítulo trata dos códigos poset hierárquico. A família dos códigos poset hierárquico, ou simplesmente códigos hierárquicos, é uma grande família entre os códigos posets. De fato, dado $n \in \mathbb{N}$, definir um poset hierárquico sobre $[n]$ é equivalente a determinar uma partição positiva $n = n_1 + \ldots + n_h, n_i > 0$. Considerando apenas os posets hierárquicos, com o rotulamento natural, tem-se 2^{n-1} posets distintos. Considerando rotulamentos quaisquer, o número de tais partições se comporta assintoticamente como $\frac{1}{4n\sqrt{3}} e^{\pi\sqrt{2n/3}}$ (ver [10]).

Uma outra boa razão para se estudar os códigos hierárquicos é que essa classe é a generalização tanto dos códigos com a métrica de Hamming quanto dos códigos cadeia. Comparando a quantidade de códigos hierárquicos com os códigos NRT tem-se que a primeira é maior, uma vez que fixado n, a quantidade de códigos hierárquicos é determinada pelo número de partições de n, enquanto a quantidade de códigos NRT é determinada pela quantidade de divisores de n.

Na seção 3.1 é mostrado que dado um código $\mathcal{C}$ é possível obter uma base ordenada de $\mathcal{C}$ tal que a sua matriz geradora apresente algumas características oriundas da sua hierarquia de P-pesos. A partir desta base e utilizando a classificação do grupo de isometrias lineares de espaços poset feito em [2] é construído um código equivalente ao inicial com uma matriz geradora com uma forma muito "mais limpa" que é chamada de *forma canônica-sistemática* da matriz geradora. Usando esta forma, é estabelecida uma decomposição do código poset como soma direta de sub-códigos que podem ser vistos como tendo a métrica de Hamming. Esta decomposição é chamada de *decomposição canônica* do código.

Na seção 3.2 usando a decomposição canônica de um código são determinados sua distância mínima, seus P-pesos generalizados e seu raio de empacotamento. Também são classificados os códigos hierárquicos MDS e P-perfeitos.

Por fim, é apresentado um algoritmo de decodificação por síndrome que tem um ganho (que pode ser até) exponencial na complexidade, se comparado ao algoritmo de decodificação usual por síndrome.

3.1 Forma Canônica-sistemática

Nesta seção, dado um código hierárquico $\mathcal{C}$ definiremos uma forma canônica-sistemática para a matriz geradora de um código $\mathcal{C}'$ equivalente a $\mathcal{C}$, no sentido estabelecido na seção 2.1.3.

O conjunto dos posets sobre n também é um poset onde os elementos minimais e maximais são, respectivamente, o poset anti-cadeia e o poset cadeia (Exemplo 2.12). Como na ordem parcial entre os posets, os posets hierárquicos estão entre o poset cadeia e o anti-cadeia, a forma canônica-sistemática para sua matriz geradora é algo intermediário entre a forma canônica dos códigos cadeia (apresentada em [3]) e a forma sistemática dos códigos anti-cadeia.

Nas métricas poset o peso de um elemento é determinado pela cardinalidade do ideal gerado

pelo seu suporte, assim, se uma coordenada não é maximal no suporte, ela não contribui para a determinação do peso de um elemento, portanto, considere a seguinte definição.

Definição 3.1. *Seja $v \in \mathbb{F}_q^n$, definimos*

$$M(v) = \{i; j \in \text{supp}(v) \ e \ i \preceq j \Rightarrow i = j\}$$

o conjunto dos elementos maximais do suporte de v, segundo a ordem parcial $\preceq$. Dessa forma, $\omega_P(v) = |\langle M(v)\rangle|$.

É válido lembrar que se $P = ([n], \preceq)$ é um $(n; n_1, \ldots, n_h)$ poset hierárquico, então existe uma partição

$$[n] = \overset{\circ}{\bigcup_{l=1,\ldots,h}} H_l$$

de $[n]$ de forma que $|H_l| = n_l$ e $i \preceq j$ se, e somente se, $i = j$ ou $i \in H_{l_i}, j \in H_{l_j}$ e $l_i < l_j$. Com isso, temos que se P é um poset hierárquico e $0 \neq v \in \mathbb{F}_q^n$, existe um único $l \in \{1, \ldots, h\}$ tal que $M(v) \subseteq H_l$.

Defina $\widehat{C}_0 := \{0\}$ (**o vetor nulo**) e $\widehat{C}_i$ como o conjunto dos elementos de $\mathcal{C}$ cujos elementos maximais de seu suporte estejam exatamente no nível i de P, isto é,

$$\widehat{C}_i := \{v \in \mathcal{C} | M(v) \subseteq H_i\}.$$

Note que, em geral, $\widehat{C}_i$ não é um subespaço vetorial (uma vez que se $M(u) = M(v)$, então $\omega_{d_P}(u+v) \leq \omega_{d_P}(u)$), mas $C_i = \cup_{j=0}^{i} \widehat{C}_j$ (o conjunto de todas as palavras de $\mathcal{C}$ tais que os elementos de seus suporte estejam até o nível i de P) é, já que se $u, v \in C_i$, então $M(u) \subseteq H_{i_u}, M(v) \subseteq H_{i_v}$ com $i_u, i_v \leq i$. Logo, $M(u+v) \subseteq M_{i_m}$ onde $i_m = \max\{i_u, i_v\} \leq i$ e se $k \in \mathbb{F}_q, k \neq 0$, então $M(kv) = M(v)$. Note também que

$$C_0 \subseteq C_1 \subseteq C_2 \subseteq \ldots \subseteq C_h \tag{3.1}$$

é uma cadeia de sub-espaços. Seja $\Lambda(\mathcal{C}) := \{t_1, \ldots, t_s\}$ o conjunto dos níveis de P tais que $\widehat{C}_{t_j} \neq \emptyset$, com $t_1 < t_2 < \ldots < t_s$.

Tome $d_j := \dim(C_{t_j}) - \dim(C_{t_{j-1}})$ para $j > 1$ e $d_1 := dim(C_{t_1})$. Com isso, $\dim(C_{t_j}) = d_1 + \ldots + d_j$.

Os vetores da base canônica de $\mathbb{F}_q^n$ serão denotados por $e_i = (0, \ldots, 0, \underbrace{1}_{i}, 0, \ldots, 0)$, o vetor que tem como suporte o conjunto $\{i\}$ e a i-ésima entrada igual a 1.

A seguir será apresentado um teorema que dá uma forma para a matriz geradora de $\mathcal{C}$ onde é possível ver como a construção dos sub-códigos C_{t_i} já separa os elementos de $\mathcal{C}$ com relação aos seus pesos sem usar, diretamente, nenhuma informação sobre o poset.

Teorema 3.1. *Seja P um $(n; n_1, \ldots, n_h)$ poset hierárquico e $\mathcal{C} \subseteq \mathbb{F}_q^n$ um código poset. Então, $\mathcal{C}$ admite como matriz geradora uma matriz $G = (G_{k,j})$ constituída de blocos $G_{k,j}$ e $0_{k,j}$, onde $G_{k,j}$ são matrizes de dimensões $d_k \times n_j$ e $0_{k,j}$ são matrizes nulas de dimensões $d_k \times n_j$. Ou seja, $\mathcal{C}$ admite como matriz geradora uma matriz da seguinte forma*

$$G = \begin{pmatrix} G_{s,1} & \ldots & & \ldots & \ldots & & G_{s,t_s} & 0_{s,t_s+1} & \ldots & 0_{s,h} \\ \vdots & & \vdots & & & \vdots & & \vdots & & \vdots \\ G_{2,1} & \ldots & & \ldots & G_{2,t_2} & 0_{2,t_2+1} & & \ldots & & 0_{2,h} \\ G_{1,1} & \ldots & G_{1,t_1} & 0_{1,t_1+1} & & \ldots & & \ldots & & 0_{1,h} \end{pmatrix}$$

Demonstração: A ideia principal da demonstração desse teorema é usar a cadeia de sub-espaços dada na equação (3.1) e tomar a base de cada um desses subespaços de forma que a base de um subespaço contenha a base do subespaço imediatamente anterior a ele na cadeia.

Para tal, tomemos bases de C_{t_j} de forma que se β_{j-1} é uma base de $C_{t_{j-1}}$ e β_j é uma base de C_{t_j}, tem-se que $\beta_j = \hat{\beta}_j \cup \beta_{j-1}$, para algum completamento $\hat{\beta}_j$. Assim, temos que $\beta_j = \widehat{\beta}_1 \cup \widehat{\beta}_2 \cup \ldots \cup \widehat{\beta}_j$, para $j = 1, \ldots, s$, e que $\beta := \widehat{\beta}_1 \cup \widehat{\beta}_2 \cup \ldots \cup \widehat{\beta}_s$ é uma base de $\mathcal{C}$.

Observe que se $v = \sum_{i=1}^{n} e_i v_i \in \widehat{\beta}_j$, com $v_i \in \mathbb{F}_q$, então $M(v) \subseteq H_j$, o que implica que $v_i = 0$ para todo $i \in H_{t_r+1} \cup \ldots \cup H_h$, isto é, $v = \sum_{i=1}^{s_{t_j}} e_i v_i$.

Assim, obtém-se uma base ordenada $\beta := \beta_s = \widehat{\beta}_1 \cup \ldots \cup \widehat{\beta}_s$ para $\mathcal{C}$ tal que a matriz geradora de $\mathcal{C}$ que tem como linhas os elementos de β_s ordenados de baixo para cima satisfaz as condições do enunciado do teorema. ■

Note que esta forma pode ser obtida através das operações $(l1), (l2)$ e $(l3)$ apresentadas na seção 2.1.2 numa matriz geradora G qualquer de $\mathcal{C}$ uma vez que sempre é possível obter uma base a partir de outra apenas realizando estas operações. Em termos matriciais: se duas matrizes representam bases do mesmo espaço, é possível obter uma delas a partir do escalonamento da outra.

Exemplo 3.1. *Considere* $(\mathbb{F}_2^{16}, d_P)$ *onde* P *é um* $(16; 2, 3, 2, 4, 2, 1, 2)$ *poset hierárquico e* $\mathcal{C}$ *é um* $[16, 5]_2$ *código com a seguinte matriz geradora:*

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

Fazendo o escalonamento na matriz acima, temos que $\mathcal{C}$ *admite a seguinte matriz geradora*

$$G' = \left(\begin{array}{cc|ccc|cc|c|cc} 0&1 & 0&1&1 & 0&1 & 1&0&0&1 & 1&0 & 1 & 0&0 \\ \hline 1&0 & 1&1&1 & 1&1 & 1&1&0&1 & 0&0 & 0 & 0&0 \\ 1&1 & 1&1&0 & 0&0 & 1&1&1&1 & 0&0 & 0 & 0&0 \\ \hline 0&1 & 0&0&1 & 0&0 & 0&0&0&0 & 0&0 & 0 & 0&0 \\ 0&1 & 0&1&0 & 0&0 & 0&0&0&0 & 0&0 & 0 & 0&0 \end{array}\right)$$

As duas primeiras linhas, de baixo para cima, de G' *são os elementos de* $\widehat{\beta}_1$*, os dois seguintes são de* $\widehat{\beta}_2$ *e o primeiro, de cima para baixo, é o elemento de* $\widehat{\beta}_3$ *e* $\Lambda(\mathcal{C}) = \{2, 4, 6\}$.

Seja $W = W_1 \oplus W_2 \oplus \ldots \oplus W_n$ uma decomposição de um espaço vetorial como soma direta de sub-espaços. Assim, cada elemento $v \in W$ pode ser escrito de forma única como $v = v_1 + v_2 + \ldots + v_n$ com $v_i \in W_i$. Denote a projeção de v em W_i por $p_i(v) = v_i$ e por $q_i(v) = v - v_i = v - p_i(v)$.

Assumindo o rotulamento natural do poset, consideremos a seguinte decomposição de $\mathbb{F}_q^n$:

$$\mathbb{F}_q^n = V_1 \oplus V_2 \oplus \ldots \oplus V_h, \tag{3.2}$$

onde $\mathrm{supp}(V_i) = H_i$, isto é, $V_i \simeq \mathbb{F}_q^{n_i}$, ou seja, $\mathbb{F}_q^n$ é decomposto de acordo com os níveis de P. Isso implica que $C_i \subseteq V_1 \oplus V_2 \oplus \ldots \oplus V_i$. Esta decomposição de $\mathbb{F}_q^n$ é explicitada no Teorema 3.1 pelas linhas verticais desenhadas na matriz geradora de $\mathcal{C}$ no sentido que as dimensões de V_i determinam quantas colunas têm cada parte desta divisão. Note também que $x \in V_1 \oplus \ldots \oplus V_{t_j}$ se, e somente se, $\mathrm{supp}(x) \subset \bigcup_{l=1}^{t_j} H_l$.

Lema 3.1. *Seja* $\beta_j = \bigcup_{l=1}^{j} \widehat{\beta}_l = \{v_{11}, \ldots, v_{1d_1}, \ldots, v_{j1}, \ldots, v_{jd_j}\}$ *a base de* C_{t_j} *determinada no Teorema 3.1. Então* $p_{t_j}(\widehat{\beta}_j) := \{p_{t_j}(v_{j1}), \ldots, p_{t_j}(v_{jd_j})\}$ *é um conjunto linearmente independente.*

Demonstração: Suponha que $\sum_{i=1}^{d_j} a_i p_{t_j}(v_{ji}) = 0$. Seja $u = \sum_{i=1}^{d_j} a_i v_{ji} \in \langle \widehat{\beta}_j \rangle$. Então

$$\begin{aligned}
\sum_{i=1}^{d_j} a_i v_{ji} &= \sum_{i=1}^{d_j} a_i (p_{t_j}(v_{ji}) + q_{t_j}(v_{ji})) \\
&= \sum_{i=1}^{d_j} a_i p_{t_j}(v_{ji}) + \sum_{i=1}^{d_j} a_i q_{t_j}(v_{ji}) \\
&= \sum_{i=1}^{d_j} a_i q_{t_j}(v_{ji}).
\end{aligned}$$

Uma vez que $M(v_{ji}) \subseteq H_j$, segue que $M(q_{t_j}(v_{ji})) \subseteq H_l$ para algum $l < j$. Então, como $u \in \mathcal{C}$ e $u = \sum_{i=1}^{d_j} a_i q_{t_j}(v_{ji})$, segue que $u \in C_{t_{j-1}} = \langle \beta_{j-1} \rangle$. Como $\beta_j = \beta_{j-1} \cup \widehat{\beta}_j$ é uma base de C_{t_j} então, $\langle \widehat{\beta}_j \rangle \cap \langle \beta_{j-1} \rangle = \{0\}$. Logo $u = \sum_{i=1}^{d_j} a_i v_{ji} = 0$, o que implica que $a_i = 0 \; \forall \; i \in \{1, \ldots, d_j\}$. Portanto,

$$p_{t_j}(\widehat{\beta}_j) = \{p_{t_j}(v_{j1}), \ldots, p_{t_j}(v_{jd_j})\}$$

é um conjunto linearmente independente. ■

Essencialmente, o que o lema que acabamos de demonstrar faz, é criar um conjunto de vetores linearmente independentes (portanto, base de um código) a partir de β_s tomando a projeção de cada vetor no nível maximal de seu suporte, portanto, mantendo os pesos. Segue o enunciado de um lema trivial mas que será necessário para futuras referências.

Lema 3.2. *Seja* $W = W_1 \oplus \ldots \oplus W_m$ *a decomposição de um espaço vetorial. Se* $A_1, \ldots, A_m$ *são, cada um, conjuntos linearmente independentes com* $A_i \subset W_i$ *para cada* $i = 1, \ldots, m$ *então* $A_1 \cup \ldots \cup A_m$ *é um conjunto linearmente independente.*

No Teorema 3.1 foi determinada uma base β_s para $\mathcal{C}$ que carrega algumas informações sobre a distribuição de pesos de $\mathcal{C}$. Segue agora uma sequência de resultados que possibilitará a construção, no Teorema 3.2, de um código $\mathcal{C}'$ equivalente a $\mathcal{C}$ com uma representação mais clara, porém preservando as principais propriedades métricas de $\mathcal{C}$. A sequência começa com o Lema 3.3 que introduz a base β_s determinada no Teorema 3.1 numa base de $\mathbb{F}_q^n$.

Denotando a base de V_l composta pelos elementos da base canônica de $\mathbb{F}_q^n$ que tenham seus suportes contidos em H_l por $\widehat{\Gamma}_l$, tem-se o seguinte resultado.

Lema 3.3. *Dado um $\mathcal{C}$ código $[n,k]_q$, para cada $j=1,\ldots,s$ existe uma base α_j de $V_1\oplus\ldots\oplus V_{t_j}$ tal que $\alpha_j=\Gamma_j\cup\beta_j\cup\Delta_j$, onde:*

- *β_j é a base de C_{t_j} determinada no Teorema 3.1,*
- $\Gamma_j=\bigcup\limits_{\substack{l=1\\ l\notin\Lambda(\mathcal{C})}}^{t_j}\widehat{\Gamma}_l$
- $\Delta_j=\bigcup\limits_{l=1}^{j}\widehat{\Delta}_l$ *é tal que se $v\in\widehat{\Delta}_l$, então $M(v)\subset H_{t_l}$.*

Demonstração: Esta demonstração será feita por indução.

Seja Γ_1 conforme estabelecido anteriormente. $\beta_1\cup\Gamma_1$ é um sub-conjunto linearmente independente de $V_1\oplus\ldots\oplus V_{t_1}$. De fato, se $\sum_{i=1}^{d_1}a_iv_{1i}+\sum_{\gamma\in\Gamma_1}b_\gamma\gamma=0$, então

$$w:=\sum_{i=1}^{d_1}a_iv_{1i}=-\sum_{\gamma\in\Gamma_1}b_\gamma\gamma.$$

Note que $w\in\mathcal{C}$, já que $w\in\langle\beta_1\rangle$. w também é um elemento de $\langle\Gamma_1\rangle$. Com isso $M(w)\subset H_i$ para algum $i\leq t_1-1$. Logo $w=0$ pois t_1 é o primeiro nível de P tal que $M(x)\subset H_{t_1}$ para algum $x\in\mathcal{C},\ x\neq 0$. Mas tanto Γ_1 quanto β_1 são conjuntos linearmente independentes, logo, $a_i=0=b_\gamma$ para todo $i\in\{1,\ldots,d_1\}$ e $\gamma\in\Gamma_1$.

Com isso, existe um conjunto Δ_1 tal que $\Gamma_1\cup\beta_1\cup\Delta_1$ é base de $V_1\oplus\ldots\oplus V_{t_1}$. Agora, basta mostrar que $M(v)\subset H_{t_1}$ para todo $v\in\Delta_1$. Isso será feito por absurdo. Para tal, considere $v\in\Delta_1$ e suponha que $M(v)\not\subset H_{t_1}$, então, $\mathrm{supp}(v)\subset\bigcup_{l=1}^{t_1-1}H_l$, ou seja, $v\in V_1\oplus\ldots\oplus V_{t_1-1}$. Como Γ_1 é uma base de $V_1\oplus\ldots\oplus V_{t_1-1}$, segue que $v\in\langle\Gamma_1\rangle$. Mas $v\in\langle\Delta_1\rangle$ e $\Gamma_1\cup\Delta_1$ é um conjunto linearmente independente, logo $v=0$.

Considere agora $V_1\oplus\ldots\oplus V_{t_{j-1}}\oplus V_{t_{j-1}+1}\oplus\ldots\oplus V_{t_j-1}\oplus V_{t_j}$ e suponha que $\Gamma_{j-1}\cup\beta_{j-1}\cup\Delta_{j-1}$ é uma base de $V_1\oplus\ldots\oplus V_{t_{j-1}}$. Pelo Lema 3.2, $\Gamma_j\cup\beta_{j-1}\cup\Delta_{j-1}$ é um conjunto linearmente independente. Note também que $\Gamma_j\cup\beta_{j-1}\cup\Delta_{j-1}$ gera $V_1\oplus\ldots\oplus V_{t_{j-1}}\oplus\ldots\oplus V_{t_j-1}$, e portanto, é uma base de $V_1\oplus\ldots\oplus V_{t_{j-1}}\oplus\ldots\oplus V_{t_j-1}$.

Tome $v_{jl}\in\widehat{\beta_j}\subset\widehat{C}_{t_j}$. Assim $M(v_{jl})\subset H_{t_j}$ e como P é hierárquico $M(v_{jl})\not\subset H_{t_j-1}$. Segue que

$$v_{jl} \in \left(V_1 \oplus \ldots \oplus V_{t_j}\right) \setminus \left(V_1 \oplus \ldots \oplus V_{t_j-1}\right).$$

Note que

$$\Gamma_j \cup \beta_{j-1} \cup \Delta_{j-1} \cup \widehat{\beta}_j = \Gamma_j \cup \Delta_{j-1} \cup \beta_j$$

é um subconjunto linearmente independente de $V_1 \oplus \ldots \oplus V_{t_j}$. De fato, suponha que

$$w := \sum_{i=1}^{d_j} a_i v_{ji} + \sum_{v \in \beta_{j-1}} a_v v + \sum_{\gamma \in \Gamma_j} b_\gamma \gamma + \sum_{\delta \in \Delta_{j-1}} c_\delta \delta = 0.$$

Considere p_{t_j} a projeção em V_{t_j}.

$$\begin{aligned} p_{t_j}(w) &= p_{t_j}\left(\sum_{i=1}^{d_j} a_i v_{ji}\right) + p_{t_j}\left(\sum_{v \in \beta_{j-1}} a_v v\right) + p_{t_j}\left(\sum_{\gamma \in \Gamma_j} b_\gamma \gamma\right) + p_{t_j}\left(\sum_{\delta \in \Delta_{j-1}} c_\delta \delta\right) \\ &= \sum_{i=1}^{d_j} a_i p_{t_j}(v_{ji}) = 0 \end{aligned}$$

Segue do Lema 3.1 que $a_i = 0$ para $i = 1, \ldots, d_j$. Com isso, temos que

$$\sum_{v \in \beta_{j-1}} a_v v + \sum_{\gamma \in \Gamma_j} b_\gamma \gamma + \sum_{\delta \in \Delta_{j-1}} c_\delta \delta = 0.$$

Mas $\beta_{j-1} \cup \Gamma_j \cup \Delta_{j-1}$ é base de $V_1 \oplus \ldots \oplus V_{t_{j-1}} \oplus \ldots \oplus V_{t_j-1}$. Logo $a_v, b_\gamma, c_\delta = 0$ para todo $v \in \beta_{j-1}, \gamma \in \Gamma_j$ e $\delta \in \Delta_{j-1}$. Segue que $\Gamma_j \cup \Delta_{j-1} \cup \beta_j$ é um subconjunto linearmente independente de $V_1 \oplus \ldots \oplus V_{t_j}$.

Seja $\widehat{\Delta}_j$ um conjunto tal que $\Gamma_j \cup \beta_j \cup \Delta_{j-1} \cup \widehat{\Delta}_j$ é base de $V_1 \oplus \ldots \oplus V_{t_j}$. Agora basta mostrar que $M(v) \subset H_{t_j}$ para $v \in \widehat{\Delta}_j$ o que é feito da mesma forma que no caso anterior. ■

Para $X \subset [n]$ denote por $E_X := \{v \in \mathbb{F}_q^n | \text{supp}(v) \subset X\}$. Cometeremos um abuso de notação escrevendo E_i ao invés de $E_{\{i\}}$. Em particular, $V_i = E_{H_i}$. Portanto, tem-se

$$\mathbb{F}_q^n = V_1 \oplus \ldots \oplus V_{t_s} \oplus E_{H_{t_s+1}} \oplus \ldots \oplus E_{H_h}.$$

Assim, lembrando que $\Lambda(\mathcal{C}) = \{t_1, \ldots, t_s\}$, é imediato que

$$\beta = \alpha_s \cup \left(\bigcup_{l=t_s+1}^{h} \widehat{\Gamma}_l \right) = \left(\bigcup_{l \in [h] \setminus \Lambda(\mathcal{C})} \widehat{\Gamma}_l \right) \cup \beta_s \cup \Delta_s$$

é uma base de $\mathbb{F}_q^n$.

Para o próximo lema é necessário introduzir mais uma notação. Para cada $i \in P$, seja $\langle i \rangle^* := \langle i \rangle \setminus \{i\}$.

No lema a seguir definimos uma transformação linear sobre a base de $\mathbb{F}_q^n$ construída no Lema 3.3 que associa os elementos de β_s aos elementos do conjunto obtido no Lema 3.1.

Lema 3.4. *Seja $T : \mathbb{F}_q^n \to \mathbb{F}_q^n$ a transformação linear definida na base β da seguinte maneira:*

$$T(v) = \begin{cases} v & \text{para } v \in \bigcup_{l \notin \Lambda(\mathcal{C})}^{h} \widehat{\Gamma}_l \\ p_{t_l}(v) & \text{para } v \in \widehat{\beta}_l \cup \widehat{\Delta}_l \end{cases}$$

Então, para todo $i \in \{1, \ldots, n\}$ e para todo $e \in E_i$, existem $0 \neq e' \in E_i$ e $u \in E_{\langle i \rangle^*}$ tais que $T(e) = e' + u$.

Demonstração: Seja $e \in E_i$. Se não existe $t_j \in \Lambda(\mathcal{C})$ tal que $i \in H_{t_j}$ então, basta tomar $e' = e$ e $u = 0$.

Se $e \in E_i$ e $i \in t_j$ para algum $t_j \in \Lambda(\mathcal{C})$, então $e \in V_1 \oplus \ldots \oplus V_{t_j}$, $\langle i \rangle^* = \bigcup_{l=1}^{t_j - 1} H_l$ e $E_{\langle i \rangle^*} = V_1 \oplus \ldots \oplus V_{t_j - 1}$. Segue do Lema 3.3 que $\alpha_j = \Gamma_j \cup \beta_j \cup \Delta_j$ é base de $V_1 \oplus \ldots \oplus V_{t_j}$. Consideremos a seguinte decomposição de e:

$$e = \gamma + \sum_{l=1}^{j} b_l + \sum_{l=1}^{j} \delta_l$$

onde $\gamma \in \langle \Gamma_j \rangle$, $b_l \in \langle \widehat{\beta}_l \rangle$ e $\delta_l \in \langle \widehat{\Delta}_l \rangle$. Assim, aplicando T nesta decomposição de e tem-se

$$\begin{aligned} T(e) &= T(\gamma) + \sum_{l=1}^{j} T(b_l) + \sum_{l=1}^{j} T(\delta_l) \\ &= \gamma + \sum_{l=1}^{j} p_{t_l}(b_l) + \sum_{l=1}^{j} p_{t_l}(\delta_l) \\ &= \gamma + \sum_{l=1}^{j-1} p_{t_l}(b_l) + \sum_{l=1}^{j-1} p_{t_l}(\delta_l) + (p_{t_j}(b_j) + p_{t_j}(\delta_j)) \\ &= \gamma + \sum_{l=1}^{j-1} p_{t_l}(b_l + \delta_l) + p_{t_j}(b_j + \delta_j). \end{aligned}$$

Segue que

$$T(e) = \gamma + \sum_{l=1}^{j-1} p_{t_l}(b_l + \delta_l) + p_{t_j}(b_j + \delta_j)$$

com

$$\gamma + \sum_{l=1}^{j-1} p_{t_l}(b_l + \delta_l) \in V_1 \oplus \ldots \oplus V_{t_j - 1}.$$

Note que

$$\begin{aligned} e = p_{t_j}(e) &= p_{t_j}(\gamma + \sum_{l=1}^{j} b_l + \sum_{l=1}^{j} \delta_l) \\ &= p_{t_j}(b_j + \delta_j), \end{aligned}$$

ou seja, $p_{t_j}(b_j + \delta_j) \in E_i$.

Assim, tomando $e' = p_{t_j}(b_j + \delta_j)$ e $u = \gamma + \sum_{l=1}^{j-1} p_{t_l}(b_l + \delta_l)$ temos que T satisfaz as condições do enunciado. ■

Note que a aplicação definida no lema acima preserva o peso dos vetores da base, mas isso não implica que ela é uma isometria.

Como já foi visto na seção 2.2.2 o grupo das isometrias lineares de $(\mathbb{F}_q^n, d_P)$, que é denotado por $GL_P(n)$, satisfaz:

$$GL_P(n) \cong \mathcal{U}(P) \rtimes Aut(P).$$

onde $\mathcal{U}(P) = \{(a_{ij} \in M_{n\times n}(\mathbb{F}_q)) : a_{ij} = 0 \text{ se } i \not\preceq j \text{ e } a_{ii} \neq 0\}$ e $Aut(P)$ é o grupo dos automorfismos de poset de P.

Note que a componente $\mathcal{U}(P)$ de $GL_P(n)$ nos permite mexer livremente nos níveis inferiores ao nível maximal do suporte dos elementos da base de $\mathbb{F}_q^n$, uma vez que $i \preceq j$ se, e somente se i está num nível inferior ao de j no poset hierárquico. Esse fato foi explorado na construção de T no Lema 3.4. Considere agora uma forma simplificada da Proposição 4.3 de [2].

Proposição 3.1. *Seja $T : \mathbb{F}_q^n \to \mathbb{F}_q^n$ um isomorfismo linear que satisfaz a seguinte condição: para cada vetor não nulo $v_i \in E_i$ existem um vetor não-nulo $v_i' \in E_i$ e um vetor $u_i \in E_{\langle i \rangle}^*$ tais que $T(v_i) = v_i' + u_i$. Então $T \in GL_P(n)$.*

Se for demonstrado que a aplicação T dada no Lema 3.4 é um isomorfismo podemos usar a Proposição 3.1 para mostrar que T é uma isometria linear e assim achar um código $\mathcal{C}'$ que seja equivalente a $\mathcal{C}$.

Teorema 3.2. *[Forma canônica-sistemática] Seja $\mathcal{C}$ um código $[n,k]_q$. Então $\mathcal{C}$ é equivalente a um código $\mathcal{C}'$ que possui uma matriz geradora $G' = (G'_{k,j})$ constituída de blocos $G'_{k,j}$ de dimensões $d_k \times n_j$ tais que $G'_{k,j}$ é a matriz nula para todo $j \neq t_k$ e para $j = t_k$ tem a seguinte forma: $G'_{k,t_k} = [\mathrm{Id}_{d_k} | A_{t_k}]$ onde Id_{d_k} é a matriz identidade de dimensões d_k e A_{t_k} é uma matriz de dimensões $d_k \times (n_{t_k} - d_k)$. Em outras palavras, G' tem a seguinte forma:*

$$G' = \begin{pmatrix} 0_{s,1} & \dots & & \dots & & \dots & 0_{s,t_s-1} & [\mathrm{Id}_{d_s}|A_{t_s}] & 0_{s,t_s+1} & \dots & 0_{s,h} \\ \vdots & & \vdots & & & \vdots & & \vdots & & \vdots & \\ 0_{2,1} & \dots & & \dots & 0_{2,t_2-1} & [\mathrm{Id}_{d_2}|A_{t_2}] & 0_{2,t_2+1} & \dots & & \dots & 0_{2,h} \\ 0_{1,1} & \dots & 0_{1,t_1-1} & [\mathrm{Id}_{d_1}|A_{t_1}] & 0_{1,t_1+1} & \dots & & \dots & & \dots & 0_{1,h} \end{pmatrix}$$

Chamaremos esta matriz G' de *forma canônica-sistemática para a matriz geradora de $\mathcal{C}$.*

Observação 3.1. *Mesmo que G' não seja uma matriz geradora de $\mathcal{C}$ ela é chamada de forma canônica-sistemática para a matriz geradora de $\mathcal{C}$ pois ela gera um código $\mathcal{C}'$ que é equivalente a $\mathcal{C}$, e portanto, $\mathcal{C}$ e $\mathcal{C}'$ possuem os mesmos invariantes da Teoria dos Códigos.*

Demonstração: Assumindo que $\mathcal{C}$ tem uma matriz geradora da forma que foi apresentada no Teorema 3.1, tome $T : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$ a transformação linear definida no Lema 3.4, isto é,

$$T(v) = \begin{cases} v & \text{para } v \in \bigcup_{l \notin \Lambda(\mathcal{C})}^{h} \widehat{\Gamma}_l \\ p_{t_l}(v) & \text{para } v \in \widehat{\beta}_l \cup \widehat{\Delta}_l \end{cases}$$

Mostraremos que T é uma isometria linear. Por definição, T é linear. Para mostrar que é um isomorfismo, é preciso mostrar que

$$\begin{aligned} T(\beta) &= \left(\bigcup_{l\notin\Lambda(\mathcal{C})}^{h} T(\widehat{\Gamma}_l)\right) \cup \left(\bigcup_{l=1}^{s} T(\beta_l)\right) \cup \left(\bigcup_{l=1}^{s} T(\widehat{\Delta}_l)\right) \\ &= \left(\bigcup_{l\notin\Lambda(C)}^{h} \widehat{\Gamma}_l\right) \cup \left(\bigcup_{l=1}^{s} p_{t_l}(\widehat{\beta}_{t_l})\right) \cup \left(\bigcup_{l=1}^{s} p_{t_l}(\widehat{\Delta}_{t_l})\right) \end{aligned}$$

é um conjunto linearmente independente.

Pelo Lema 3.2, basta mostrar que $p_{t_j}(\widehat{\beta}_j) \cup p_{t_j}(\widehat{\Delta}_j)$ é um conjunto linearmente independente para cada $j = 1, \ldots, s$.

Da definição de p_{t_j} e q_{t_j}, segue a seguinte igualdade:

$$\sum_{i=1}^{d_j} a_i v_{ji} + \sum_{\delta\in\widehat{\Delta}_j} b_\delta \delta = \sum_{i=1}^{d_j} a_i \left(p_{t_j}(v_{ji}) + q_{t_j}(v_{ji})\right) + \sum_{\delta\in\widehat{\Delta}_j} b_\delta \left(p_{t_j}(\delta) + q_{t_j}(\delta)\right).$$

Assumindo que $\sum_{i=1}^{d_j} a_i p_{t_j}(v_{ji}) + \sum_{\delta\in\widehat{\Delta}_j} b_\delta p_{t_j}(\delta) = 0$,

$$\sum_{i=1}^{d_j} a_i v_{ji} + \sum_{\delta\in\widehat{\Delta}_j} b_\delta \delta = \sum_{i=1}^{d_j} a_i q_{t_j}(v_{ji}) + \sum_{\delta\in\widehat{\Delta}_j} b_\delta q_{t_j}(\delta).$$

Devido ao fato de $v_{ji},\ \delta \in V_1 \oplus \cdots \oplus V_{t_j}$ para todo $i = 1, \ldots, d_j,\ \delta \in \widehat{\Delta}_j$ e da definição de q_{t_j}, segue que

$$\sum_{i=1}^{d_j} a_i q_{t_j}(v_{ji}) + \sum_{\delta\in\widehat{\Delta}_j} b_\delta q_{t_j}(\delta) \in V_1 \oplus \cdots \oplus V_{t_j-1} = \langle \beta_{j-1} \cup \Delta_{j-1} \cup \Gamma_j \rangle.$$

Uma vez que

(*i*) $\sum_{i=1}^{d_j} a_i v_{ji} + \sum_{\delta\in\widehat{\Delta}_j} b_\delta \delta \in \langle \widehat{\beta}_j \cup \widehat{\Delta}_j \rangle$;

(*ii*) $\sum_{i=1}^{d_j} a_i v_{ji} + \sum_{\delta\in\widehat{\Delta}_j} b_\delta \delta = \sum_{i=1}^{d_j} a_i q_{t_j}(v_{ji}) + \sum_{\delta\in\widehat{\Delta}_j} b_\delta q_{t_j}(\delta) \in \langle \beta_{j-1} \cup \Delta_{j-1} \cup \Gamma_j \rangle$;

(*iii*) $\langle \widehat{\beta}_j \cup \widehat{\Delta}_j \rangle \cap \langle \beta_{j-1} \cup \Delta_{j-1} \cup \Gamma_j \rangle = \emptyset$,

tem-se que

$$\sum_{i=1}^{d_j} a_i q_{t_j}(v_{ji}) + \sum_{\delta \in \widehat{\Delta}_j} b_\delta q_{t_j}(\delta) = \sum_{i=1}^{d_j} a_i v_{ji} + \sum_{\delta \in \widehat{\Delta}_j} b_\delta \delta = 0,$$

ou seja,

$$a_1 = \ldots = a_{d_j} = 0 \text{ e } b_\delta = 0, \forall \delta \in \widehat{\Delta}_j.$$

Daí que $p_{t_j}\left(\widehat{\beta}_j\right) \cup p_{t_j}\left(\widehat{\Delta}_j\right)$ é um conjunto linearmente independente. Logo T é um isomorfismo linear.

Assim, pelo Lema 3.4, T satisfaz a Proposição 3.1, e portanto, T é uma isometria linear. Com isso $\mathcal{C}$ e $\mathcal{C}' = T(\mathcal{C})$ são códigos equivalentes. A maneira como T foi construída garante que a matriz geradora de $\mathcal{C}'$ cujas linhas são os vetores da base ordenada $T(\beta_s)$, ordenados de baixo para cima, tem a seguinte forma:

$$B = \begin{pmatrix} 0_{s,1} & \ldots & & \ldots & & \ldots & B_{s,t_s} & 0_{s,t_s+1} & \ldots & 0_{s,h} \\ \vdots & & & \vdots & & & \vdots & & & \vdots \\ 0_{2,1} & \ldots & & \ldots & B_{2,t_2} & 0_{2,t_2+1} & \ldots & & \ldots & 0_{2,h} \\ 0_{1,1} & \ldots & B_{1,t_1} & 0_{1,t_1+1} & & \ldots & & \ldots & & 0_{1,h} \end{pmatrix}$$

onde $0_{i,j}$ é a matriz nula de dimensões $d_i \times n_j$, cada bloco B_{k,t_k} tem dimensões $d_k \times n_{t_k}$ e posto d_k.

Note que o sub-código gerado pelo conjunto de linhas

$$\begin{pmatrix} 0_{j,1} & \ldots & 0 & B_{j,t_j} & 0 & \ldots & 0 \end{pmatrix}$$

está inteiramente contido num sub-espaço de $\mathbb{F}_q^n$ gerado por coordenadas correspondentes a um único nível do poset hierárquico P. Assim, a métrica d_P restrita a esse sub-código coincide com a métrica de Hamming a menos de soma por uma constante, isto é, se x, y estão neste sub código, então $d_P(x,y) = K + d_H(x,y)$. Dessa maneira, permutações nas colunas desse sub-código são isometrias. Assim, cada bloco B_{k,t_k} pode ser substituído por $G'_{k,t_k} = [\mathrm{Id}_{d_k} | A_{t_k}]$, a forma sistemática deste sub-código. ■

É possível definir uma decomposição para $\mathcal{C}$ baseada na decomposição em blocos da matriz geradora de $\mathcal{C}$ apresentada no Teorema 3.2.

Note que se P for um poset anti-cadeia, isto é, se tivermos a métrica de Hamming e $\mathcal{C} \neq \emptyset$ temos que $h = s = 1$, ou seja G' possui apenas um bloco na forma $[Id_k|A]$ que é exatamente a forma sistemática para códigos com a métrica Hamming. Já no caso de P ser um poset cadeia temos que $|n_i| = 1$ para todo $i = 1, \ldots, h$. Então todos os blocos terão dimensão 1 e G' será a forma canônica apresentada em [3].

Corolário 3.1. *[Decomposição Canônica de um Código] Seja $\mathcal{C}$ um código $[n,k]_q$ poset hierárquico. Então $\mathcal{C}$ é equivalente a um código $\mathcal{C}'$ que pode ser decomposto da seguinte forma*

$$\mathcal{C}' = \mathcal{C}_1 \oplus \mathcal{C}_2 \oplus \ldots \oplus \mathcal{C}_h$$

onde h é a altura de P, $\operatorname{supp}(\mathcal{C}_i)$ está contido no i-ésimo nível H_i de P e $\sum_{i=1}^{h} \dim(\mathcal{C}_i) = k$.

Demonstração: Segue imediatamente do Teorema 3.2. ■

O código $\mathcal{C}'$ descrito no Corolário 3.1 é chamado de *decomposição canônica de* $\mathcal{C}$. $\mathcal{C}'$ é equivalente a $\mathcal{C}$ e, por esse motivo, ambos possuem os mesmos invariantes métricos, que é o que, de fato, estamos interessados.

Exemplo 3.2. *Considere o código do Exemplo 3.1. Calculando $p_2(\widehat{\beta}_1), p_4(\widehat{\beta}_2), p_6(\widehat{\beta}_3)$ (a isometria dada no Teorema 3.2) e ordenando o resultado de baixo para cima, tem-se a seguinte matriz geradora de $\mathcal{C}'$:*

$$G' = \left(\begin{array}{c|c|c|c|c|c|c} 0\ 0 & 0\ 0\ 0 & 0\ 0 & 0\ 0\ 0\ 0 & 0\ 0 & 1 & 0\ 0 \\ \hline 0\ 0 & 0\ 0\ 0 & 0\ 0 & 1\ 1\ 0\ 1 & 0\ 0 & 0 & 0\ 0 \\ 0\ 0 & 0\ 0\ 0 & 0\ 0 & 1\ 1\ 1\ 1 & 0\ 0 & 0 & 0\ 0 \\ \hline 0\ 0 & 0\ 0\ 1 & 0\ 0 & 0\ 0\ 0\ 0 & 0\ 0 & 0 & 0\ 0 \\ 0\ 0 & 0\ 1\ 0 & 0\ 0 & 0\ 0\ 0\ 0 & 0\ 0 & 0 & 0\ 0 \end{array}\right)$$

Substituindo cada bloco pela forma sistemática do respectivo sub-código considerando a métrica de Hamming, temos

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

Esta é a forma canônica-sistemática para a matriz geradora de $\mathcal{C}$.

Observação 3.2. *A matriz geradora apresentada no Teorema 3.2 é chamada de forma canônica-sistemática pois ela é canônica nos níveis, no sentido que* $\dim(\mathcal{C}_i)$ *é unicamente determinado pela hierarquia de* $P-$*pesos generalizada de* $\mathcal{C}$ *como será visto na Seção 3.2, Exemplo 3.4 . Em particular, os níveis correspondentes aos blocos que são identicamente nulos em todas as linhas de* G'*, apresentada no Teorema 3.2 ou, equivalentemente, os níveis que correspondem aos códigos* $\mathcal{C}_i$ *na decomposição apresentada no Corolário 3.1 com* $\dim(\mathcal{C}_i) = 0$ *correspondem aos níveis que não estão em* $\Lambda(\mathcal{C})$*, isto é,* $\dim(\mathcal{C}_i) = 0$ *se, e somente se* $i \in [n] \setminus \Lambda(\mathcal{C})$*. A restrição da métrica poset* d_P *ao* i*-ésimo nível* H_i *é, essencialmente, equivalente à métrica de Hamming* d_H*, a menos da soma por uma constante, isto é, dados* $x \neq y \in \mathbb{F}_q^n$ *com* $supp(x)$, $supp(y) \subseteq H_i$*, então* $d_P(x, y) = d_H(x, y) + s_{i-1}$*. A forma de* G' *também é chamada de "sistemática" pois os blocos* $G'_{i,t_i} = [\mathrm{Id}_i | A_{t_i}]$ *são as formas sistemáticas para as matrizes geradoras de* $\mathcal{C}_i$ *vistos como códigos em espaços com a métrica de Hamming.*

3.2 Invariantes Métricos

Tendo em mãos a decomposição canônica para códigos hierárquicos, não é difícil determinar a expressão de alguns dos principais invariantes da Teoria de Códigos, tais como a distância mínima do código e o seu raio de empacotamento. A decomposição canônica também nos permite determinar quais códigos hierárquicos são MDS e P-perfeitos. Por fim, usando a decomposição canônica dos códigos hierárquicos é possível definir um algoritmo de decodificação por síndrome que tem ganho exponencial, em termos de complexidade de busca, se comparado ao algoritmo usual de decodificação por síndrome.

Nesta seção, P é um $(n; n_1, \ldots, n_h)$ poset hierárquico e $\mathcal{C}$ é um código $[n, k]_q$ com a sua decomposição canônica como estabelecida no Corolário 3.1, isto é, $\mathcal{C} = \mathcal{C}_1 \oplus \mathcal{C}_2 \oplus \ldots \oplus \mathcal{C}_h$ com $\mathrm{supp}(\mathcal{C}_i) \subseteq H_i$, h sendo a altura de P e $\sum_{i=1}^{h} dim(\mathcal{C}_i) = k$. Denote por k_i a dimensão de $\mathcal{C}_i$ e lembre que $k_i \neq 0$ se, e somente se, $i \in \Lambda(\mathcal{C})$. Note que se $i < t_1$ então,$k_i = 0$, e daí pode-se omitir as primeiras componentes nulas da decomposição canônica de $\mathcal{C}$, isto é, $\mathcal{C} = \mathcal{C}_{t_1} \oplus \mathcal{C}_{t_1+1} \oplus \ldots \oplus \mathcal{C}_h$.

Lembre também que a restrição de d_P a $\mathcal{C}_l$, que será denotada por d^l, é equivalente a métrica de Hamming somada uma constante que depende de l.

Distância Mínima e P-pesos generalizados.

A distância mínima dos códigos poset hierárquico é dada pela seguinte proposição.

Proposição 3.2. *Seja $\mathcal{C}$ um código hierárquico, sua distância mínima é dada por*

$$\delta_P = s_{t_1-1} + \delta_{t_1},$$

onde $t_1 = \min \Lambda(\mathcal{C}), s_{t_1-1} = \sum_{i=1}^{t_1-1} n_i$ e δ_{t_1} é a distância mínima de $\mathcal{C}_{t_1}$ considerado como um código num espaço com a métrica de Hamming.

Demonstração: Seja $c_{t_1} \in \mathcal{C}_{t_1}$ tal que $\omega_H(c_{t_1}) = \delta_{t_1}$, então, $\omega_P(c_{t_1}) = s_{t_1-1} + \delta_{t_1}$, ou seja, $\delta_P \leq s_{t_1-1} + \delta_{t_1}$.

Note que não existe $c \in \mathcal{C}$ com $\omega_P(c) < s_{t_1-1}+\delta_{t_1}$, uma vez que se $\omega_P(c) < s_{t_1-1}+\delta_{t_1}$ teríamos $\text{supp}(c) \subseteq H_{t_1}$, ou seja, teríamos $c \in \mathcal{C}_{t_1}$ com $\omega_H(c) < \delta_{t_1}$, o que contradiria a minimalidade de δ_{t_1}. ■

Exemplo 3.3. *Considere o código dado no Exemplo 3.1 com a matriz geradora G na forma canônica-sistemática, como dada no Exemplo 3.2:*

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

Assim, $t_1 = 2, s_1 = 2$ e $\mathcal{C}_2$ tem a seguinte matriz geradora:

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

Logo, $\delta_2 = 1$, uma vez que $w_H(010) = 1$. Assim, $\delta_P = 2 + 1 = 3$.

De maneira análoga a que foi feita na Proposição 3.2, é possível descrever os P-pesos generalizados de $\mathcal{C}$, de uma maneira mais simples utilizando a sua decomposição canônica. Antes, para evitar somatórios nas expressões a seguir, denote $r_i = d_1+d_2+\ldots+d_i$, para $i = 1, 2, \ldots, h$, onde $d_0 = 0$ e $d_i = \dim(\mathcal{C}_i)$.

Proposição 3.3. *Dado $1 \leq i \leq k$, seja j tal que $r_{j-1} < i \leq r_j$. Então, o i-ésimo P-peso generalizado $\delta_{P,i}$ de $\mathcal{C}$ é:*

$$\delta_{P,i} = s_{t_j-1} + \delta_{H,(i-r_{j-1})}(\mathcal{C}_{t_j}) \tag{3.3}$$

onde $\delta_{H,(i-r_{j-1})}(\mathcal{C}_{t_i})$ é o $(i - r_{j-1})$-ésimo peso generalizado de $\mathcal{C}_{t_i}$ no sentido da métrica de Hamming..

Demonstração: A demonstração dessa proposição segue de maneira análoga à demonstração da Proposição 3.2. Seja $\widehat{D}_{t_j} \subset \mathcal{C}_{t_j}$ tal que $|\text{supp}(\widehat{D}_{t_j})| = \delta_{H,(i-r_{j-1})}(\mathcal{C}_{t_j})$ e $dim(\widehat{D}_{t_j}) = i - r_{j-1}$. Então $|\langle \text{supp}(\widehat{D}_{t_j})\rangle| = s_{t_j-1} + \delta_{H,(i-r_{j-1})}(\mathcal{C}_{t_j})$. Considere o seguinte sub-código de $\mathcal{C}$:

$$\widehat{D} = \mathcal{C}_{t_1} \oplus \ldots \mathcal{C}_{t_j-1} \oplus \widehat{D}_{t_j}.$$

Segue que $\dim(\widehat{D}) = r_{j-1} + (i - r_{j-1}) = i$ e que $|\langle \text{supp}(\widehat{D})\rangle| = |\langle \text{supp}(\widehat{D}_{t_j})\rangle| = s_{t_j-1} + \delta_{H,(i-r_{j-1})}(\mathcal{C}_{t_j})$. Com isso, $\delta_{P,i} \leq s_{t_j-1} + \delta_{H,(i-r_{j-1})}(\mathcal{C}_{t_j})$.

Considerando agora D o sub-código de $\mathcal{C}$ que realiza o i-ésimo P-peso generalizado, isto é, $D \subset \mathcal{C}$ é tal que $|\langle \text{supp}(D)\rangle| = \delta_{P,i}$.

Note que $D \subseteq \mathcal{C}_{t_1} \oplus \ldots \oplus \mathcal{C}_{t_j}$ pois do contrário teríamos

$$|\langle \text{supp}(D)\rangle| > s_{t_j} > s_{t_j-1} + \delta_{H,(i-r_{j-1})}(\mathcal{C}_{t_j}) = |\langle \text{supp}(\widehat{D})\rangle|,$$

o que contradiz a minimalidade de $\delta_{P,i}$. Assim, pode-se considerar a decomposição

$$D = D_1 \oplus \ldots \oplus D_{t_j},$$

onde $D_l \subset \mathcal{C}_l$ para $l \in \{1, \ldots, t_j\}$. Temos novamente que

$$|\langle \text{supp}(D)\rangle| = |\langle \text{supp}(D_{t_j})\rangle| = |\text{supp}(D_{t_j})| + s_{t_j-1}.$$

Pela minimalidade de $\delta_{H,(i-r_{j-1})}(\mathcal{C}_{t_j})$, tem-se que

$$|\text{supp}(D_{t_j})| \geq \delta_{H,(i-r_{j-1})}(\mathcal{C}_{t_j})$$

ou seja

$$\delta_{P,i} = |\langle \text{supp}(D)\rangle| = s_{t_j-1} + |\text{supp}(D_{t_j})| \geq s_{t_j-1} + \delta_{H,(i-r_{j-1})}(\mathcal{C}_{t_j}) \geq \delta_{P,i}$$

Assim, $\delta_{P,i} = s_{t_j-1} + \delta_{H,(i-r_{j-1})}(\mathcal{C}_{t_j})$. ■

Vejamos agora como a decomposição canônica de um código é determinada pela sua hierarquia de P-pesos.

Exemplo 3.4. *Considere P um $(16; 2, 3, 2, 4, 2, 1, 2)$ poset hierárquico e $\mathcal{C}$ um $[16, 5]_2$ código munido da métrica poset P com a seguinte hierarquia de P-pesos:*

$$\{3, 5, 9, 11, 14\}.$$

Da hierarquia de P-pesos podemos concluir que $dim(\mathcal{C}_1) = 0$ pois, do contrário, teríamos que ter $\delta_{P,1} = 1$ ou 2.

Como $\delta_{P,1} = 3$ temos que a palavra de $\mathcal{C}$ com menor peso está em $\mathcal{C}_2$, logo $t_1 = 2$.

Temos que $\delta_{P,2} = 5$, assim, $\mathcal{C}$ tem um sub-código bi-dimensional contido em $\mathcal{C}_2$, pois, caso contrário $\delta_{P,2}$ teria que ser maior que $5 = n_1 + n_2 = s_2$.

$\delta_{P,3} = 9$, o que indica que $dim(\mathcal{C}_3) = 0$ pois se $dim(\mathcal{C}_3) \neq 0$ teríamos que ter que algum i tal que $\delta_{P,i} \in \{6, 7\}$. $\delta_{P,3} = 9$ também indica que $dim(\mathcal{C}_4) \neq 0$, pois se $dim(\mathcal{C}_4) = 0$ teríamos que ter $\delta_{P,3} \geq 12 > 11 = s_4$.

$\delta_{P,4} = 11$ nos diz que $\mathcal{C}$ tem um sub-código bi-dimensional contido em $\mathcal{C}_4$ usando um argumento análogo ao usado no caso $\delta_{P,2} = 5$.

$\delta_{P,5} = 14$ determina que:

- *$\mathcal{C}$ não tem mais que 2 elementos linearmente independentes em $\mathcal{C}_4$, pois dai teríamos que $\delta_{P,5} \leq 11$;*
- *$dim(\mathcal{C}_5) = 0$ pois se $dim(\mathcal{C}_5) \neq 0$, $\delta_{P,5} \in \{12, 13\}$;*
- *$dim(\mathcal{C}_6) \neq 0$, pois se $dim(\mathcal{C}_6) \geq 0$ teríamos $\delta_{P,5} > 14 = s_6$. Como as únicas possibilidades para $dim(\mathcal{C}_6)$ são 0 ou 1, temos que $dim(\mathcal{C}_6) = 1$.*

  $dim(\mathcal{C}_7) = 0$, pois $\mathcal{C}$ tem dimensão 5 e já temos um espaço de dimensão 5 contido em $\mathcal{C}_1 \oplus \mathcal{C}_2 \oplus \mathcal{C}_3 \oplus \mathcal{C}_4 \oplus \mathcal{C}_5 \oplus \mathcal{C}_6$.

Resumindo: $dim(\mathcal{C}_1) = dim(\mathcal{C}_3) = dim(\mathcal{C}_5) = dim(\mathcal{C}_5) = 0, dim(\mathcal{C}_2) = dim(\mathcal{C}_4) = 2$ e $dim(\mathcal{C}_6) = 1$.

Por isso a decomposição dada no Corolário 3.1 é chamada de *decomposição canônica* de $\mathcal{C}$.

Raio de Empacotamento

Na definição de raio de empacotamento fica bem claro que este conceito depende diretamente da métrica adotada. É fato conhecido que, se P é um poset anti-cadeia (originando a métrica de Hamming), o raio de empacotamento de $\mathcal{C}$ é dado por:

$$R_{d_H}(\mathcal{C}) = \left\lfloor \frac{\delta_H - 1}{2} \right\rfloor,$$

onde $\lfloor x \rfloor$ é a parte inteira de x e δ_H é a distância mínima de $\mathcal{C}$ segundo a métrica Hamming.

Se P for um poset cadeia o *Teorema* 5 de [3] estabelece que

$$R_{d_P}(\mathcal{C}) = \delta_P - 1,$$

onde δ_P é a distância minima de $\mathcal{C}$ segundo a métrica cadeia.

Foi visto no Exemplo 2.12 que o conjunto dos posets também é um poset onde o poset anti-cadeia é o elemento minimal, o poset cadeia é o maximal e portanto os posets hierárquicos estão entre estes dois posets. Com isso, se P é um poset hierárquico, pode-se esperar que

$$\left\lfloor \frac{\delta_P - 1}{2} \right\rfloor \leq R_{d_P}(\mathcal{C}) \leq \delta_P - 1.$$

A seguir, utilizando a decomposição canônica dos códigos hierárquicos, será apresentada uma proposição que determina o raio de empacotamento de um código em função da sua distância mínima δ_P e da distância mínima de $\mathcal{C}_{t_1}$ visto como um código com a métrica de Hamming δ_{t_1}. Para demonstra-la usa-se que a distância entre duas palavras $x, y \in \mathbb{F}_q^n$ depende apenas dos elementos maximais do suporte de $x - y$.

Proposição 3.4. *Sob as mesmas condições da Proposição 3.2,*

$$R := R_{d_P}(\mathcal{C}) = s_{t_1 - 1} + \left\lfloor \frac{\delta_{t_1} - 1}{2} \right\rfloor.$$

Demonstração: Pela linearidade de $\mathcal{C}$ e como as métricas poset são invariantes por translação, basta mostrar que $B_{d_P}(0, R) \cap B_{d_P}(c, R) = \emptyset$ para todo $c \in \mathcal{C}$ e que $B_{d_P}(0, R+1) \cap B_{d_P}(c, R+1) \neq \emptyset$ para algum $c \in \mathcal{C}$.

Considere a decomposição canônica de $\mathcal{C}$. Seja $c \in \mathcal{C}$ e suponha que exista $x \in \mathbb{F}_q^n$ tal que $x \in B_{d_P}(0,R) \cap B_{d_P}(c,R)$. Note que $M(x) \subset H_{t_1}$. De fato, se $M(x) \subset H_j$ com $j < t_1$, teríamos

$$\begin{aligned} d_P(x,c) &= \omega_{d_P}(c) \\ &\geq \delta_P \\ &= s_{t_1-1} + \delta_{t_1} \\ &> s_{t_1-1} + \left\lfloor \frac{\delta_{t_1}-1}{2} \right\rfloor. \end{aligned}$$

Por outro lado, se $j > t_1$ teríamos

$$d_P(x,0) = \omega_{d_P}(x) \geq s_{j-1} + 1 \geq s_{t_1} > s_{t_1-1} + \left\lfloor \frac{\delta_{t_1}-1}{2} \right\rfloor,$$

Logo $j = t_1$. Note que isso também mostra que, sob as mesmas condições, se $x \in B_{d_P}(0,R) \cap B_{d_P}(c,R)$ com $c \in \mathcal{C}$, então $M(c) \subseteq H_{t_1}$. Como $M(x) \subseteq H_{t_1}$, se $M(c) \subseteq H_l$ com $l > t_1$, teríamos $d_P(x,c) = \omega_{d_P}(c) > s_{l-1} + 1 > R$. Então $M(c), M(x) \subseteq H_j$. Segue que

$$d_P(x,c) = \omega_{d_P}(x-c) = s_{t_1-1} + |M(x-c)|$$

e como $\omega_{d_P}(x-c) = d_P(x,c) \leq s_{t_1-1} + \left\lfloor \frac{\delta_{t_1}-1}{2} \right\rfloor = R$, tem-se que

$$s_{t_1-1} + |M(x-c)| \leq s_{t_1-1} + \left\lfloor \frac{\delta_{t_1}-1}{2} \right\rfloor$$

e daí que

$$|M(x-c)| \leq \left\lfloor \frac{\delta_{t_1}-1}{2} \right\rfloor < \frac{\delta_{t_1}}{2}.$$

Mas, como $|M(c)| \geq \delta_{t_1}$,

$$|M(x) \cap M(c)| \geq \frac{\delta_{t_1}}{2} > \left\lfloor \frac{\delta_{t_1}-1}{2} \right\rfloor,$$

ou seja,

$$\omega_{d_P}(x) = s_{t_1-1} + |M(x)| > s_{t_1-1} + \left\lfloor \frac{\delta_{t_1}-1}{2} \right\rfloor = R,$$

contradizendo o fato de $x \in B_{d_P}(0,R)$.

Agora é necessário mostrar que $B_{d_P}(0, R+1) \cap B_{d_P}(c, R+1) \neq \emptyset$ para algum $c \in \mathcal{C}$. Seja $c \in \mathcal{C}$ tal que c realize a distância mínima de $\mathcal{C}$, ou seja $\omega_{d_P}(c) = \delta_P = s_{t_1-1} + \delta_{t_1}$. Assim, $\text{supp}(c) \subseteq H_{t_1}$, ou seja,

$$c = \sum_{i=1}^{n_{t_1}} c_i e_{s_{t_1-1}+i},$$

onde $\{e_1, e_2, ..., e_n\}$ é a base canônica de $\mathbb{F}_q^n$.

Note que $|\text{supp}(c)| = \delta_{t_1}$. Seja $A \subset \text{supp}(c)$ tal que $|A| = \left\lfloor \frac{\delta_{t_1}-1}{2} \right\rfloor + 1$. Tome $x \in \mathbb{F}_q^n$ definido da seguinte maneira:

$$x = \sum_{i \in A} c_i e_{s_{j-1}+i}.$$

Com isso

$$d_P(x, 0) = s_{t_1-1} + \left\lfloor \frac{\delta_{t_1} - 1}{2} \right\rfloor + 1 = R + 1$$

e

$$d_P(x, c) = s_{t_1-1} + |\text{supp}(c) \backslash A|.$$

Mas $|\text{supp}(c)\backslash A|$ é $\left\lfloor \frac{\delta_{t_1}-1}{2} \right\rfloor$ ou $\left\lfloor \frac{\delta_{t_1}-1}{2} \right\rfloor - 1$, dependendo da paridade de δ_{t_1}. Em ambos os casos, $x \in B_{d_P}(0, R+1) \cap B_{d_P}(c, R+1)$. ■

Exemplo 3.5. *Considere o código dado no Exemplo 3.1 com a matriz geradora na forma canônica-sistemática como dada no Exemplo 3.2. Temos que $t_1 = 2, s_1 = 2$ e $\delta_2 = 1$, logo, o raio de empacotamento de $\mathcal{C}$ é $2 + \left\lfloor \frac{1-1}{2} \right\rfloor = 2$*

Limitante de Singleton e códigos hierárquicos MDS

Teorema 3.3 (Códigos MDS)**.** *Seja $\mathcal{C} = \mathcal{C}_{t_1} \oplus \ldots \oplus \mathcal{C}_h$ um código hierárquico na sua decomposição canônica. Então $\mathcal{C}$ é um código MDS se, e somente se, $\mathcal{C} = \mathcal{C}_{t_1} \oplus V_{t_1+1} \oplus \ldots \oplus V_h$ e $\mathcal{C}_{t_1}$ é um código MDS em (V_{t_1}, d_H).*

Demonstração: Se $\mathcal{C}$ é um código MDS então o limitante de Singleton é atingido, isto é,

$$\delta_P = n - k + 1. \tag{3.4}$$

Lembre que $n = \sum_{i=1}^{h} n_i$ e $k = \sum_{i=1}^{h} k_i$, onde $n_i = |H_i| = \dim(V_i)$, $k_i = dim(\mathcal{C}_i)$ e $\mathcal{C}_i \subseteq V_i$. Pela Proposição 3.2 temos que $\delta_P = s_{t_1-1} + \delta_{t_1}$, onde δ_{t_1} é a distância mínima de $\mathcal{C}_{t_1}$ visto como um sub-código de V_{t_1} munido da métrica de Hamming. Desta maneira, a equação (3.4) fica da seguinte forma:

$$\sum_{i=1}^{t_1-1} n_i + \delta_{t_1} = \sum_{i=1}^{h} n_i - \sum_{i=1}^{h} k_i + 1. \tag{3.5}$$

Lembrando que $k_i = 0$ se $i \notin \Lambda(\mathcal{C})$ a equação (3.5) assume a seguinte expressão:

$$\delta_{t_1} = \sum_{i \in \Lambda(\mathcal{C})} (n_i - k_i) + \sum_{\substack{i=t_1+1 \\ i \notin \Lambda(\mathcal{C})}}^{h} n_i + 1. \tag{3.6}$$

A cota de Singleton para $\mathcal{C}_i$, visto como um sub-código de V_{t_1} munido da métrica de Hamming, estabelece que $\delta_{t_1} \leq n_{t_1} - k_{t_1} + 1$. Com isso,

$$\sum_{i \in \Lambda(\mathcal{C}) \setminus \{t_1\}} (n_i - k_i) + \sum_{\substack{i=t_1+1 \\ i \notin \Lambda(\mathcal{C})}}^{h} n_i \leq 0.$$

Mas $\mathcal{C}_i \subseteq V_i$, o que implica que $0 \leq k_i \leq n_i$ para todo i. Logo,

$$\sum_{i \in \Lambda(\mathcal{C}) \setminus \{t_1\}} (n_i - k_i) + \sum_{\substack{i=t_1+1 \\ i \notin \Lambda(\mathcal{C})}}^{h} n_i = 0. \tag{3.7}$$

Note que se existisse $i > t_1$ tal que $i \notin \Lambda(\mathcal{C})$, teríamos $\sum_{\substack{i=t_1+1 \\ i \notin \Lambda(\mathcal{C})}}^{h} n_i > 0$. O que não pode acontecer, pois isso contradiria a equação (3.7). Assim, se $i > t_1, i \in \Lambda(\mathcal{C})$. Desta forma, a equação (3.7) se resume a

$$\sum_{i=t_1+1}^{h} (n_i - k_i) = 0, \tag{3.8}$$

o que implica que $n_i = k_i$ para todo $i \geq t_1 + 1$, ou seja, $\mathcal{C} = \mathcal{C}_{t_1} \oplus V_{t_1+1} \oplus \ldots \oplus V_h$. Com isso, a equação (3.6) fica

$$\delta_{t_1} = n_{t_1} - k_{t_1} + 1.$$

Isto é, $\mathcal{C}_{t_1}$ é um código MDS em V_{t_1} munido da métrica de Hamming.

Se $\mathcal{C} = \mathcal{C}_{t_1} \oplus V_{t_1+1} \oplus \ldots \oplus V_h$ com $\mathcal{C}_{t_1}$ sendo um código MDS em V_{t_1} munido da métrica de Hamming, então é imediato que $\mathcal{C}$ atinge o limitante de Singleton. ■

Códigos Hierárquicos perfeitos

A decomposição canônica de um código e a descrição de seu raio de empacotamento em termos de δ_{t_1} permitem a classificação dos códigos hierárquicos perfeitos.

O Lema a seguir é trivial, porém, muito útil. Ele segue do fato de, na métrica hierárquica, apenas os elementos do suporte que estão no nível mais alto, determinam o peso da palavra.

Lema 3.5. *Seja $R = R_{d_P}(\mathcal{C})$ o raio de empacotamento de $\mathcal{C}$ segundo a métrica hierárquica e $x \in \mathbb{F}_q^n$ tal que $x \in B_{d_P}(c, R)$ para algum $c \in \mathcal{C}$. Se $M(c) \subset H_i$ e $M(x) \subset H_j$ então $i = j$.*

Demonstração:

Se $x \in B_{d_P}(c, R)$, temos que $d_P(x, c) \leq R$.

Se $j < i$, temos que $d_P(x, c) = \omega_{d_P}(c) \geq s_{t_1-1} + \delta_{t_1} > R$.

Se $j > i$, temos que $d_P(x, c) = \omega_{d_P}(x) > \omega_{d_P}(c) \geq s_{t_1-1} + \delta_{t_1} > R$.

Assim, temos que $j = i$.

■

Deste resultado segue que dado um código perfeito $\mathcal{C}$, temos que $i \in \Lambda(\mathcal{C})$ para todo $i \geq t_1$. De fato, como $\mathcal{C}$ é perfeito, dado $x \in \mathbb{F}_q^n$, existe $c \in \mathcal{C}$ tal que $x \in B_{d_P}(c, R)$. Segue do Lema 3.5 que $M(c) \subset H_i$, o que implica que $i \in \Lambda(\mathcal{C})$. Com isso temos que $\mathcal{C} = \mathcal{C}_{t_1} \oplus \ldots \oplus \mathcal{C}_h$ com $\dim(\mathcal{C}_i) > 0$ para todo $i \geq t_1$.

Teorema 3.4 (Códigos hierárquicos perfeitos)**.** *Um código hierárquico $\mathcal{C}$ é perfeito se, e somente se, $\mathcal{C} = \mathcal{C}_{t_1} \oplus V_{t_1+1} \oplus \ldots \oplus V_h$ e $\mathcal{C}_{t_1}$ é um código perfeito em V_{t_1} com a métrica de Hamming.*

Demonstração: Comecemos assumindo que $\mathcal{C}$ é um código hierárquico perfeito.

Suponha que $\mathcal{C}_l \neq V_l$ para algum $l \geq t_1 + 1$. Assim, tome $x_l \in V_l \backslash \mathcal{C}_l$. Como $\mathcal{C}$ é perfeito, existe $c \in \mathcal{C}$ tal que $x \in B_{d_P}(c, R)$. Pelo Lema 3.5, segue que $M(c) \subset H_l$, assim, $c = c_{t_1} + \cdots + c_l$

com $c_i \in \mathcal{C}_i$. Como $x_l \notin \mathcal{C}_l,\ x_l \neq c_l$. Dessa forma, $d_P(c, x_l) = d_H(c_l, x_l) + s_{l-1} > s_{t_1} > R$, um absurdo.

Agora, temos que mostrar que $\mathcal{C}_{t_1}$ é perfeito em V_{t_1} considerando a métrica de Hamming. É importante lembrar que como estamos lidando com um código num espaço com a métrica de Hamming, o seu raio de empacotamento é dado por $\tilde{R} = \left\lfloor \frac{\delta_{t_1}-1}{2} \right\rfloor$.

Seja $x \in V_{t_1}$. Como $\mathcal{C}$ é perfeito, existe $c \in \mathcal{C}$ tal que $x \in B_P(c, R)$. Pelo Lema 3.5, $M(c) \subset H_{t_1}$, ou seja, $c \in \mathcal{C}_{t_1}$. Mas, se $x \in B_P(c, R)$, então

$$d_P(c, x) = |\langle \text{supp}(c - x) \rangle| = s_{t_1-1} + |\text{supp}(c - x)| \leq R,$$

pois $\text{supp}(c - x) \subseteq H_{t_1}$. Como $R = s_{t_1-1} + \left\lfloor \frac{\delta_{t_1}-1}{2} \right\rfloor$, segue que

$$d_H(x, c) = |\text{supp}(c - x)| = d_H(c, x) \leq \left\lfloor \frac{\delta_{t_1} - 1}{2} \right\rfloor = \tilde{R},$$

ou seja, para todo $x \in V_{t_1}$, existe $c \in \mathcal{C}_{t_1}$ tal que $x \in B_H(c, \tilde{R})$. Logo $\mathcal{C}_{t_1}$ é perfeito em V_{t_1} com a métrica de Hamming.

Assuma agora que $\mathcal{C}_{t_1} \subseteq V_{t_1}$ é um código perfeito (considerando a métrica de Hamming) em V_{t_1}. Seja $x = x_1 + \ldots + x_{t_1} + \ldots + x_h \in \mathbb{F}_q^n$, com $x_i \in V_i$. Como $\mathcal{C}_{t_1}$ é um código perfeito em V_{t_1}, existe $c_{t_1} \in \mathcal{C}_{t_1}$ tal que $d_H(c_{t_1}, x_{t_1}) \leq \left\lfloor \frac{\delta_{t_1}-1}{2} \right\rfloor$. Tome $c = c_{t_1} + x_{t_1+1} + \ldots + x_h \in \mathcal{C}$. Assim,

$$\begin{aligned} d_P(x, c) &= \omega_{d_P}(x - c) \\ &= \omega_{d_P}(x_1 + \ldots + x_{t_1} - c_{t_1}) \\ &= |\langle \text{supp}(x_1 + \ldots + x_{t_1} - c_{t_1}) \rangle| \\ &= |\langle \text{supp}(x_{t_1} - c_{t_1}) \rangle| \\ &= s_{t_1-1} + d_H(c_{t_1}, x_{t_1}) \\ &\leq s_{t_1-1} + \left\lfloor \frac{\delta_{t_1} - 1}{2} \right\rfloor = R, \end{aligned}$$

ou seja, $x \in B_P(c, R)$ e daí que $\mathcal{C}$ é perfeito. ■

3.2.1 Decodificação por Síndrome

Considerando a decomposição de $\mathbb{F}_q^n$ induzida pelos níveis de P, como na equação (3.2), temos

$$\mathbb{F}_q^n = V_1 \oplus V_2 \oplus \ldots \oplus V_h,$$

onde $V_i \simeq \mathbb{F}_q^{n_i}$ e $\text{supp}(V_i) = H_i$, isto é, o suporte de V_i está no $i-$ésimo nível do poset P. Com isso, todo elemento $x \in \mathbb{F}_q^n$ pode ser escrito, de forma única, como $x = x_1 + \ldots + x_h$ com $x_i \in V_i$.

Note que, como na decomposição de $\mathbb{F}_q^n$, na decomposição canônica de $\mathcal{C} = \mathcal{C}_1 \oplus \ldots \oplus \mathcal{C}_h$, todo elemento $x \in \mathcal{C}$ também pode ser escrito de maneira única como $x = x_1 + \ldots + x_h$ com $x_i \in \mathcal{C}_i \subseteq V_i$.

Isto, e o fato de $x_i = 0$ se $i \notin \Lambda(\mathcal{C})$ nos permitem melhorar consideravelmente, em temos de complexidade, o algoritmo de decodificação por síndrome. De fato, seja y a palavra recebida a ser decodificada:

Algoritmo 3.1. (Decodificação por síndrome em códigos na sua decomposição canônica)

(*i*) *Considere a decomposição* $y = y_1 + y_2 + \ldots + y_h$, *com* $\text{supp}(y_i) \subset H_i$, *com* H_i *sendo o* i*-ésimo nível do poset* P*;*

(*ii*) *Se* $i \in \Lambda(\mathcal{C})$, *determine* $a(y_i)$ *decodificando* y_i *em cada* $\mathcal{C}_i$ *usando o algoritmo de decodificação usual por síndrome, conforme apresentado na seção 2.1.4;*

(*iii*) *Se* $i \notin \Lambda(\mathcal{C})$, $a(y_i) = 0$;

(*iv*) *Faça* $a(y) = a(y_1) + a(y_1) + \ldots + a(y_h)$.

Assim, definindo

$$y_\Lambda = \sum_{i \in \Lambda} y_i \quad \text{e} \quad y_{\Lambda^\perp} = \sum_{i \in [h] \backslash \Lambda(\mathcal{C})} y_i,$$

quando recebermos y, desconsideramos a componente $y_{\Lambda^\perp}$ e efetuamos a decodificação por síndrome em cada componente y_i relativa a $\mathcal{C}_i$, para $i \in \Lambda(\mathcal{C})$.

A complexidade da decodificação por síndrome é determinada, essencialmente, pela busca de elementos líderes das classes laterais do código. Se $\mathcal{C}$ for um código $[n,k]_q$, esse número é q^{n-k}.

Considerando a decomposição de $\mathbb{F}_q^n$, induzida pelos níveis do poset P, e $\mathcal{C}$ na sua decomposição canônica, para cada $i \in [h] \backslash \Lambda(\mathcal{C})$ a decodificação apenas ignora as n_i entradas

correspondentes ao nível H_i do poset; para cada $i \in \Lambda(\mathcal{C})$ fazemos a decodificação por síndrome de um código $[n_i, d_i]_q$, tendo assim que buscar entre $q^{n_i-d_i}$ líderes das classes laterais de $\mathcal{C}$. Desconsiderando os demais custos computacionais envolvidos neste algoritmo e, considerando apenas a busca entre os elementos líderes das classes laterais de $\mathcal{C}$, para um código na sua decomposição canônica temos

$$\sum_{i\in\Lambda} q^{n_i-k_i}$$

operações de busca.

Considerando o poset hierárquico minimal (o anti-cadeia), que induz a métrica de Hamming em $\mathbb{F}_q^n$, temos que $h = 1$ assim, $\Lambda(\mathcal{C}) = \{1\}, n_1 = n$ e $d_1 = k$. Dessa forma, a complexidade do algoritmo de decodificação por síndrome, correspondente à busca por líderes das classes laterais de $\mathcal{C}$ é q^{n-k}.

Por outro lado, quando temos o poset maximal (o poset cadeia), $h = n$, $|\Lambda(\mathcal{C})| = k$, $|[h]\backslash\Lambda(\mathcal{C})| = n - k$ e $d_i = n_i = 1$, para todo $i \in \Lambda(\mathcal{C})$. Neste caso temos a menor complexidade de busca possível $(n - k)$, como visto em [3]. No caso intermediário, temos um algoritmo com ganho exponencial, quando comparado com a decodificação por síndrome usual de códigos em espaços com métrica de Hamming, e perda exponencial, quando comparado com códigos em espaços com a métrica cadeia. Dessa forma, temos o seguinte quadro comparativo:

$$\underbrace{n-k}_{\substack{\text{Complexidade da}\\ \text{decodificação em}\\ \text{poset cadeia}}} \leq \underbrace{\textstyle\sum_{i\in\Lambda} q^{n_i-k_i}}_{\substack{\text{Complexidade da}\\ \text{decodificação em}\\ \text{poset hierárquico}}} \leq \underbrace{q^{n-k}}_{\substack{\text{Complexidade da}\\ \text{decodificação em}\\ \text{poset anti-cadeia}}}$$

Figura 3.1: Comparação entre as complexidades de decodificação (considerando apenas os líderes de classes laterais) entre os posets cadeia, hierárquico e anti-cadeia.

Dado uma palavra recebida y, para aplicarmos o algoritmo de decodificação por síndrome em um código $\mathcal{C}$, não necessariamente na sua decomposição canônica, devemos proceder da seguinte maneira:

Algoritmo 3.2. (Algoritmo de decodificação para códigos que não estão na sua decomposição canônica)

(*i*) *Considere a isometria linear* $T : \mathbb{F}_q^n \to \mathbb{F}_q^n$ *tal que* $\mathcal{C}' = T(\mathcal{C})$ *é decomposição canônica de* $\mathcal{C}$*. A existência de tal isometria linear é garantida pelo Teorema 3.2;*

(*ii*) *Aplique o Algoritmo de decodificação por síndrome em* $T(y)$ *relativamente ao código* $\mathcal{C}'$*, obtendo uma palavra-código* $a(T(y)) \in \mathcal{C}'$*;*

(*iii*) *Decodifique* y *como* $T^{-1}(a(T(y))) \in \mathcal{C}$*.*

Para realizarmos o algoritmo de decodificação por síndrome precisamos conhecer a matriz de paridade. Uma forma canônica-sistemática para a matriz de paridade H' pode ser obtida da matriz geradora na forma canônica-sistemática G'. A matriz H' é uma uma matriz $(n-k) \times n$ com todas as entradas nulas, exceto aquelas correspondentes aos blocos que serão multiplicados pelos blocos não nulos de G' (estabelecida no Teorema 3.2). Para cada bloco $G'_{k,t_k} = [\mathrm{Id}_{t_k} | A_{t_k}]$ de G' temos em H' o bloco $H'_{k,t_k} = [-A_{t_k}^T | \mathrm{Id}_{n_{t_k}-t_k}]$. Porém, note que com o Algoritmo 3.2 não precisamos construir a matriz de paridade H', precisamos apenas das matrizes de paridade de cada componente.

Capítulo 4

Propriedade de Extensão de Ideais e Classificação das Órbitas das Isometrias

As identidades de MacWilliams [15], no contexto de métrica de Hamming, estabelecem uma relação entre os polinômios enumeradores de um código e do seu dual. Esta relação, que no contexto clássico é determinada pelos pesos de Hamming das palavras código, mascara uma situação mais rica, onde na realidade a relação estabelecida entre um código e seu dual depende na realidade não dos pesos das palavras, mas das órbitas das palavras-código pelo grupo de isometrias lineares. De uma maneira mais genérica, é possível dizer que uma identidade do tipo MacWilliams é estabelecida para códigos poset ao se considerar uma relação de equivalência entre os ideais do referido poset, conforme mostrado recentemente em [7]. Estas identidades do tipo MacWilliams estimulam estudar relações entre ideais de poset, o que fazemos neste capítulo.

Na seção 4.1, usando os resultados de [20], que relacionam os automorfismos do poset com as isometrias do espaço munido das respectivas métricas posets, é estudado quando é possível em um poset P estender um isomorfismo entre ideais de P para um automorfismo de P e mostrado que os posets hierárquicos e NRT possuem tal propriedade. Ainda nesta seção, é apresentada uma definição alternativa para poset árvore uni-raiz, regular por nível que facilitará

a demonstração de que esta classe de posets também possui a propriedade de extensão.

Em [4] Barg e Purkayastha definem uma função que classifica as órbitas das isometrias de espaços munidos da métrica NRT. Na seção 4.2 estendemos este conceito para posets de maneira geral, criando a definição de *formato de uma palavra* (shape). Dessa maneira, o formato de uma palavra atua na classificação das órbitas dos elementos de $(\mathbb{F}_q, d_P)$ segundo as isometrias deste espaço (o que, devido à Proposição 4.1 é equivalente a determinar quando existe um automorfismo de P entre os ideais gerados pelos suportes dos elementos). É mostrado que para os posets hierárquicos, o peso cumpre este papel. Para posets NRT usa-se a função apresentada em [4]. Também é mostrado que o *string* de árvores, conforme definido em [1], satisfaz as condições de formato para posets árvores uni-raiz, regulares por nível.

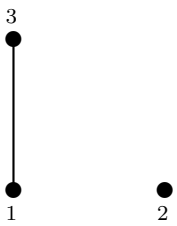
Além do dual é possível obter novos posets a partir de outros posets [26]. Na seção 4.3 será estudado quando o poset, que surge a partir da operação de dois posets que possuem a propriedade de extensão, herda esta propriedade de seus geradores e, no caso de herdar, encontramos expressões para seu formato, em termos dos formatos de seus geradores.

4.1 Propriedade de Extensão

Seja P um poset sobre um conjunto finito. Dois ideais $I, J \in \mathcal{I}(P)$ são *isomorfos*, denotado por $I \sim J$, se existe uma isomorfismo de ordem $g : I \to J$ tal que $g(I) = J$.

Note que dado um poset $P = (X, \preceq)$, um ideal $I \in \mathcal{I}(P)$ e um automorfismo $\sigma \in Aut(P)$, tem-se que $\sigma(I) \sim I$ pois $\sigma|_I$ é um isomorfismo de ordem. No entanto, a recíproca, não necessariamente é verdadeira, isto é, dados dois ideais isomorfos $I, J \in \mathcal{I}(P)$, nem sempre existe um automorfismo $\sigma \in Aut(P)$ tal que $\sigma(I) = J$.

Exemplo 4.1. *Considere* $([3], \preceq)$ *onde a relação de ordem é dada da por* $1 \preceq 3$. *Assim,* $\{1\}$ *e* $\{2\}$ *são ideais isomorfos, mas, como* $Aut(P) = \{id\}$, *não existe automorfismo* T *tal que* $T(\{1\}) = \{2\}$.



Definição 4.1. *Sejam P um poset e $I \in \mathcal{I}(P)$. O conjunto dos elementos de $\mathcal{I}(P)$ que são isomorfos a I será denotado por $\tilde{I}$. Isto é,*

$$\tilde{I} = \{J \in \mathcal{I}(P); I \sim J\}.$$

Note que isso define uma relação de equivalência em $\mathcal{I}(P)$ de modo que $\tilde{I} = \tilde{J}$ se, e somente se, $I \sim J$.

De forma análoga, tem-se uma relação de equivalência no conjunto dos filtros de P da seguinte maneira: dado $I \in \mathcal{F}(P)$, as classes de equivalência são definidas como

$$\tilde{I}^{\perp} = \{J \in \mathcal{F}(P); I \sim J\}.$$

Neste caso, $I, J \in \mathcal{F}(P)$ são equivalentes se, e somente se, $\tilde{I}^{\perp} = \tilde{J}^{\perp}$

Definição 4.2. *Um poset $P = (X, \preceq)$ tem a propriedade de extensão de ideais (propriedade-IE), se para todo $I, J \in \mathcal{I}(P)$ tal que $I \sim J$ existe $\sigma \in Aut(P)$ tal que $\sigma(I) = J$. Analogamente, $P = (X, \preceq)$ tem a propriedade de extensão de filtros (propriedade-FE) se para todo $I, J \in \mathcal{F}(P)$ tais que $I \sim J$ existe $\sigma \in Aut(P)$ tal que $\sigma(I) = J$.*

Note que o poset apresentado no Exemplo 4.1 não possui a propriedade-IE.

Em [24] Schmerl estabelece uma propriedade de extensão diferente e muito mais forte sobre posets enumeráveis, finitos ou infinitos. Segundo [24], um poset $P = (X, \preceq)$ é *homogêneo* se para todo $Y \subset X$ com Y finito (não necessariamente um ideal) e $f : Y \hookrightarrow X$ um mergulho[1] de Y em X tem-se que existe um automorfismo $F \in Aut(P)$ tal que $F|_Y = f$. Ainda em [24] encontra-se uma classificação completa dos posets homogêneos dividindo-os em 4 famílias. Como a propriedade de homogeneidade não é sobre ideais, a única família de posets homogêneos finitos é a dos anti-cadeias.

Neste capítulo, quando não for passsível de dúvida, cometeremos o abuso de denotar, para $x \in \mathbb{F}_q^n$, $\langle \text{supp}(x) \rangle$ por $\langle x \rangle$.

Definição 4.3. *$(\mathbb{F}_q^n, d_P)$ tem as órbitas determinadas pelos ideais (propriedade $\tilde{I}$) se, para todo $x, y \in \mathbb{F}_q^n$, existe $T \in GL_P(n)$ tal que $T(x) = y$ se, e somente se, $\langle x \rangle \sim \langle y \rangle$.*

[1]Neste caso, um mergulho é uma aplicação injetiva tal que $i \preceq_Y j$ se, e somente se, $f(i) \preceq_X f(j)$.

Analogamente, $(\mathbb{F}_q^n, d_P)$ *tem as órbitas determinadas pelos filtros (propriedade* $\tilde{I}^{\perp}$*) se, para todo* $x, y \in \mathbb{F}_q^n$*, existe* $T \in GL_P(n)$ *tal que* $T(x) = y$ *se, e somente se,* $\langle x \rangle_{P^{\perp}} \sim \langle y \rangle_{P^{\perp}}$*, onde* $\langle x \rangle_{P^{\perp}}$ *é o ideal gerado por* x *em* $P^{\perp}$*, o poset dual de* P*.*

Lema 4.1. *Se* $\phi \in Aut(P)$*, então a aplicação* $T_\phi : \mathbb{F}_q^n \to \mathbb{F}_q^n$ *definida por*

$$T_\phi(x_1, \ldots, x_n) = (x_{\phi(1)}, \ldots, x_{\phi(n)})$$

é um elemento de $GL_P(n)$*.*

Demonstração: Seja $\phi \in Aut(P)$. Como ϕ é uma bijeção, segue que T_ϕ leva base canônica na base canônica, o que implica que T_ϕ é um isomorfismo linear.

Para mostrar que T_ϕ é uma isometria, tome $(x_1, \ldots, x_n) \in \mathbb{F}_q^n$. Dessa forma, tem-se que $T_\phi(x_1, \ldots, x_n) = (x_{\phi(1)}, \ldots, x_{\phi(n)})$. Como $\mathrm{supp}((x_1, \ldots, x_n)), \mathrm{supp}((x_{\phi(1)}, \ldots, x_{\phi(n)})) \subset [n]$ e pela definição de T_ϕ, segue que

$$\mathrm{supp}((x_1, \ldots, x_n)) \sim \mathrm{supp}((x_{\phi(1)}, \ldots, x_{\phi(n)})).$$

Então $|\langle \mathrm{supp}((x_1 \ldots, x_n)) \rangle| = |\langle (x_{\phi(1)}, \ldots, x_{\phi(n)}) \rangle|$, o que implica que

$$\omega_P((x_1, \ldots, x_n)) = \omega_P((x_{\phi(1)}, \ldots, x_{\phi(n)})) = \omega_P(T_\phi(x_1, \ldots, x_n)).$$

Segue que T_ϕ é uma isometria. ■

O resultado a seguir estabelece uma relação entre as isometrias lineares de espaços poset e os automorfismos de posets, cuja demonstração pode ser encontrada em [20].

Teorema 4.1. *[20] Seja* $P = ([n], \preceq)$ *um poset,* $\{e_1, e_2, \ldots, e_n\}$ *a base canônica de* $\mathbb{F}_q^n$ *e* $T \in GL_P(n)$ *uma isometria linear. Então o mapa* $\phi_T : [n] \to [n]$ *dado por*

$$\phi_T(i) = \max\{\mathrm{supp}(T(e_i))\}$$

é um automorfismo de P*.*

A aplicação ϕ_T, como definida acima é bem definida, uma vez que em [20] é mostrado que se $T \in \mathrm{GL}_P(n)$, então $\langle \mathrm{supp}(T(e_i)) \rangle$ é um ideal primo, isto é, possui um único elemento maximal.

Observe que o Lema 4.1 e o Teorema 4.1, além de estabelecer uma relação entre os automorfismo de posets e as isometrias lineares dos espaços posets, dá uma expressão explícita para esses automorfismos em termos das isometrias lineares.

Definição 4.4. *Dado $x \in \mathbb{F}_q^n$, a forma limpa de x, denotada por $\hat{x}$ é o vetor que satisfaz:*

- $\text{supp}(\hat{x}) = M(x)$;
- *Se $i \in \text{supp}(\hat{x})$, então $\hat{x}_i = 1$.*

Ou seja, $\hat{x}$ é o vetor obtido atribuindo 1 *às entradas cujas coordenadas sejam maximais em* $\text{supp}(x)$ *e zerando as demais.*

Lema 4.2. *Se um poset P tem a propriedade-IE, então $(\mathbb{F}_q^n, d_P)$ tem a propriedade $\tilde{I}$. Se um poset P tem a propriedade-FE, então $(\mathbb{F}_q^n, d_P)$ tem a propriedade $\tilde{I}^{\perp}$.*

Demonstração: Seja P com a propriedade-IE e $\{e_i; i = 1, \cdots, n\}$ a base canônica de $\mathbb{F}_q^n$. Pelo Teorema 4.1, dado $T \in GL_P(n)$, a aplicação $\phi_T : [n] \to [n]$ dada por $\phi_T(i) = M(\langle T(e_i)\rangle)$, é um automorfismo de poset, onde $M(.)$ é o conjunto dos elementos maximais do suporte do elemento no argumento. Assim, se $T \in GL_P(n)$ é tal que $T(x) = y$, mostremos que $\phi_T(\langle x\rangle) = \langle y\rangle$.

Tem-se que $x = \sum_{l \in \text{supp}(x)} x_l e_l$, assim, $y = T(x) = \sum_{l \in \text{supp}(x)} x_l T(e_l)$.

Pela definição de ϕ_T e do fato que $\langle \text{supp}(T(e_l))\rangle$ é um ideal primo, segue que $\langle \text{supp}(T(e_l))\rangle = \langle \text{supp}(e_{\phi_T(l)})\rangle$. Assim $y = T(x) = \sum_{l \in \text{supp}(x)} x_l \alpha_l e_{\phi_T(l)}$, ou seja $\text{supp}(y) = \phi_T(\text{supp}(x))$, e portanto, $\langle y\rangle = \langle \phi_T(x)\rangle = \phi_T(\langle x\rangle)$.

Então ϕ_T é um automorfismo de poset que satisfaz $\phi_T(\langle x\rangle) = \langle y\rangle$, assim, $\langle x\rangle \sim \langle y\rangle$.

Suponha agora que $\langle x\rangle \sim \langle y\rangle$. Como P tem a propriedade-IE, existe $\phi \in Aut(P)$ tal que $\phi(\langle x\rangle) = \langle y\rangle$. Seja $T_\phi : \mathbb{F}_q^n \to \mathbb{F}_q^n$ definida por $T_\phi(x_1, \cdots, x_n) = (x_{\phi(1)}, \cdots, x_{\phi(n)})$. Segue do Lema 4.1 que $T_\phi \in GL_P(n)$.

Considere a matriz $A_x = (a_{ij}) \in GL_P(n)$ tal que

$$\begin{aligned} a_{ii} &= x_i^{-1} \text{ se } i \in M(x); \\ a_{ii} &= 1 \text{ se } i \notin M(x); \\ a_{ij} &= 0 \text{ se } i \neq j. \end{aligned}$$

Dessa forma, $A_x x = (x'_1, \cdots, x'_n)$ é tal que $x'_i = 1$ se $i \in M(x)$ e $x'_i = x_i$ caso contrário.

Agora, considere a matriz $B_x = (b_{ij}) \in GL_P(n)$ definida da seguinte maneira:

$$\begin{aligned} b_{ij} &= 1 \text{ se } i = j; \\ b_{ij} &= -x_i^{-1} \text{ se } x_i \neq 0 \text{ e } j = \max\{k \in M(x); i \prec k\}; \\ b_{ij} &= 0 \text{ caso contrário.} \end{aligned}$$

Aqui, max é relativo à ordem usual $\leq$ dos números inteiros.

Considere $T_x := B_x A_x$. Por construção, $B_x A_x x = \hat{x}$. Segue daí que $T = T_y^{-1} \circ T_\phi \circ T_x$ é uma isometria linear que satisfaz $T(x) = y$. Isso encerra a demonstração de que $(\mathbb{F}_q^n, d_P)$ possui a propriedade $\tilde{I}$.

Para demonstrar a propriedade $\tilde{I}^\perp$, basta considerar o poset dual $P^\perp$. ■

Segue agora a recíproca do lema acima.

Lema 4.3. *Se $(\mathbb{F}_q^n, d_P)$ tem a propriedade $\tilde{I}$, então P tem a propriedade-IE. Se $(\mathbb{F}_q^n, d_P)$ tem a propriedade $\tilde{I}^\perp$, então P tem a propriedade-FE.*

Demonstração: Sejam $I, J \in \mathcal{I}(\mathcal{P})$ tais que $I \sim J$. Considere $\tilde{x}, \tilde{y}$ vetores que estão na sua forma limpa e que $\langle \text{supp}(\tilde{x}) \rangle = I, \langle \text{supp}(\tilde{y}) \rangle = J$. Então tem-se que $\langle \text{supp}(\tilde{x}) \rangle \sim \langle \text{supp}(\tilde{y}) \rangle$. Como $(\mathbb{F}_q^n, d_P)$ possui a propriedade $\tilde{I}$, tem-se que existe uma isometria linear $T \in GL_P(n)$ tal que $T(\tilde{x}) = \tilde{y}$.

Tome $\phi_T : [n] \longrightarrow [n]$ dada por $\phi_T(i) = \max\{\text{supp}(T(e_i))\}$, conforme definido no Teorema 4.1. Para mostrar que $\phi_T(I) = J$, basta mostrar que $\phi_T(\text{supp}(\tilde{x})) = \text{supp}(\tilde{y})$.

Seja $i \in \text{supp}(\tilde{x})$, então $\text{supp}(T(e_i)) \subseteq \text{supp}(\tilde{y})$. Segue que

$$\phi_T(i) = \max\{\text{supp}(T(e_i))\} \in \text{supp}(\tilde{y}).$$

Considerando $\tilde{x} = \sum_{l \in supp(\tilde{x})} \tilde{x}_l e_l$, tem-se que $\tilde{y} = T(\tilde{x}) = \sum_{l \in supp(\tilde{x})} \tilde{x}_l T(e_l)$. Então, para todo $i \in \text{supp}(\tilde{y})$, existe $l \in \text{supp}(\tilde{x})$ tal que $i \in \text{supp}(T(e_l))$. Mas $\text{supp}(T(e_l)) \subseteq \text{supp}(\tilde{y})$ e $i \in \text{supp}(\tilde{y})$, o que implica que i é maximal em $\text{supp}(T(e_l))$, uma vez que, pela definição de forma limpa, é maximal em $\text{supp}(\tilde{y})$. Desta forma, $\phi_T(l) = \max\{\text{supp}(T(e_l))\} = i$.

Para demonstrar a propriedade-FE, basta considerar o poset dual $P^\perp$. ■

Proposição 4.1. *Um poset P tem a propriedade-IE se, e somente se $(\mathbb{F}_q^n, d_P)$ tem a propriedade $\tilde{I}$. P tem a propriedade-FE se, e somente se $(\mathbb{F}_q^n, d_P)$ tem a propriedade $\tilde{I}^\perp$.*

Demonstração: Segue imediatamente dos Lemas 4.2 e 4.3. ■

Agora, apresentaremos alguns posets que possuem a propriedade-IE

Exemplo 4.2. *Espaços munidos de uma métrica hierárquica possuem a propriedade $\tilde{I}$. De fato, sabe-se que se P é um $(n; n_1, \ldots, n_h)$ poset hierárquico, então*

$$GL_P(n) \cong \mathcal{U}(P) \rtimes Aut(P),$$

onde $Aut(P) = S_{n_1} \otimes S_{n_2} \otimes \ldots \otimes S_{n_h}$ com S_{n_i} sendo o grupo das permutações sobre os elementos de H_{n_i} e $A \in \mathcal{U}(P)$ se, e somente se,

$$A = \left(\begin{array}{c|c|c|c} id_{n_1} & * & * & * \\ \hline 0 & id_{n_2} & * & * \\ \hline \vdots & 0 & \ddots & * \\ \hline 0 & \cdots & 0 & id_{n_h} \end{array}\right),$$

e $*$ podendo assumir qualquer valor.

Sejam $x, y \in \mathbb{F}_q^n$ tais que $\omega_{d_P}(x) = \omega_{d_P}(y)$. Considere $x = x_1 + \ldots + x_h$ e $y = y_1 + \ldots + y_h$, onde $\mathrm{supp}(x_i), \mathrm{supp}(y_i) \subseteq H_i$, isto é, estamos considerando a decomposição de $\mathbb{F}_q^n$ induzida pelos níveis de P.

Como P é um poset hierárquico, temos que $M(x) \subseteq H_{l_x}, M(y) \subseteq H_{l_y}$ para $l_x, l_y \in \{1, \ldots, h\}$. Segue que $l_x = l_y = l$ uma vez que se $l_x < l_y$, necessariamente teríamos $\omega_{d_P}(x) < \omega_{d_P}(y)$. Desta forma, temos que $\omega_{d_P}(x) = s_{l-1} + |\mathrm{supp}(x_l)| = s_{l-1} + |\mathrm{supp}(y_l)| = \omega_{d_P}(y)$. Logo $|\mathrm{supp}(x_l)| = |\mathrm{supp}(y_l)|$.

Sejam $T_x, T_y \in \mathcal{U}(\mathcal{P})$ tais que $T_x(x) = \tilde{x}$ e $T_y(y) = \tilde{y}$ onde $\tilde{x}$ e $\tilde{y}$ são as formas limpas de x e y, respectivamente. Considere também $S \in S_{n_l}$ uma permutação dos elementos de H_l tal que $S(\tilde{x}) = \tilde{y}$. Desta forma ${T_y}^{-1} \circ S \circ T_x \in GL_P(n)$ é tal que ${T_y}^{-1} \circ S \circ T_x(x) = y$.

Com isso, mostramos que se P é um poset hierárquico, $(\mathbb{F}_q^n, d_P)$ possui a propriedade $\tilde{I}$. Portanto, pela Proposição 4.1, posets hierárquicos possuem a propriedade-IE. Como posets anti-cadeia e cadeia são casos particulares de posets hierárquicos, segue que essas famílias de poset também gozam da propriedade de extensão de ideais.

Os posets árvore uni-raiz, regulares por nível foram apresentados no Exemplo 4. Esse exemplo será retomado agora, porém de uma outra maneira, a fim de facilitar a demonstração de que esta classe também possui a propriedade-IE.

Definição 4.5. *Uma árvore uni-raiz, regular por nível é um poset definido da seguinte maneira: Seja* $n = 1 + q_1 + q_1q_2 + \cdots + q_1q_2 \ldots q_r$ *e considere o conjunto:*

$$\mathcal{H} = \{\emptyset\} \cup \{\epsilon_1; \epsilon_1 \in \mathbb{Z}_{q_1}\} \cup \{\epsilon_1\epsilon_2; \epsilon_j \in \mathbb{Z}_{q_j}\} \cup \cdots \cup \{\epsilon_1\epsilon_2 ... \epsilon_h; \epsilon_j \in \mathbb{Z}_{q_j}\}.$$

Sejam $a = a_1 \ldots a_p$ *e* $b = b_1 \ldots b_q \in \mathcal{H}$ *a relação de ordem parcial em* $\mathcal{H}$ *é dada por.*

$$a \preceq b \text{ se, e somente se, } p \leq q \text{ e } a_i = b_i, i = 1, \ldots, p \ .$$

Neste caso, $P = (\mathcal{H}, \preceq)$ *é uma* $(n; q_1, q_2, \ldots, q_{h-1})$ *árvore uni-raiz, regular por nível.*

Note primeiramente que P possui um único elemento minimal (a palavra vazia), por isso P é chamado de árvore uni-raiz. Note também que, dado $a = a_1 \ldots a_{i-1} \in \mathcal{H}$, $l(a) = i$, *isto é, a está no i-ésimo nível de P. Note que todo elemento do i-ésimo nível possui exatamente* q_{i+1} *filhos. Por esta razão P é dito regular por nível* (*a regularidade está no número de filhos dos elementos de cada nível*).

Proposição 4.2. *Árvores uni-raiz, regulares por nível possuem a propriedade-IE.*

Demonstração: Sejam $P = (\mathcal{H}, \preceq)$ uma árvore regular por nível de altura h. Dados $a = a_1 \ldots a_p, b = b_1 \ldots b_q \in \mathcal{H}$ com $a \preceq b$ tem-se $b = a|b_{p+1} \cdots b_q$, onde $x|y$ é a concatenação de palavras.

Seja $I, J \in \mathcal{I}(P)$ dois ideais isomorfos, e seja ϕ um isomorfismo tal que $\phi(I) = J$. Agora, será construída $\phi^* \in Aut(P)$ tal que a restrição $\phi^*|_I = \phi$, ou seja, para todo $a \in I$, $\phi^*(a) = \phi(a)$. Dado $a \in \mathcal{H} \backslash I$, considere a cadeia da raiz até a. Esta cadeia é única e intersecta I porque P possui um único elemento minimal. Seja a^I o último vértice desta cadeia que pertence à I (o "encontro" de a e I). Daí, $a^I = b^0 \preceq b^1 \preceq \cdots \preceq b^{l(a)-l(a^I)} = a$ para alguns vértices $b^1, \ldots, b^{l(a)-l(a^I)-1}$.

Note que cada vértice $b^l, l \geq 1$ é obtido pela concatenação de a^I com a sequência formada por l letras $b_1, \ldots, b_l$, onde $b_j \in \{0, 1, \ldots, q_{l(a^I)+j} - 1\}, j = 1, \ldots, l$.

Dado $a \in I$, defina o conjunto de descendentes de a não pertencentes a I:

$$\Lambda_{a,I} = \{0 \leq j \leq q_{l(a)} - 1 : \ a|j \notin I\}.$$

(eventualmente, este conjunto pode ser vazio).

Uma vez que I e J são isomorfos e P é regular por nível, segue que

$$|\Lambda_{a,I}| = |\Lambda_{\phi(a),J}|, \quad a \in I,$$

Assim, para cada $a \in I$ existe uma bijeção $\gamma_a : \{0, 1, \ldots, q_{l(a)} - 1\} \to \{0, 1, \ldots, q_{l(\phi(a))} - 1\}$ tal que $\gamma_a(\Lambda_{a,I}) = \Lambda_{\phi(a),J}$ e $\phi(a)|\gamma_a(j) = \phi(a|j)$ para $j \in \{0, 1, \ldots, q_{l(a)} - 1\} \backslash \Lambda_{a,I}$. Em outras palavras, γ_a induz a mesma aplicação que ϕ quando restrita aos filhos de a que estão em I.

Agora, defina o isomorfismo ϕ^* da seguinte maneira. Dado $a = a^I|b_{l(a^I)+1}, \cdots, b_{l(a)} \in \mathcal{H}$ defina $\phi^*(a)$ como

$$\phi^*(a) = \phi(a)|\gamma_a(b_{l(a^I)+1}), b_{l(a^I)+2}, \ldots b_{l(a)}.$$

Como γ_a é uma bijeção e P é regular por nível, ϕ^* é bem definida. Por construção ϕ^* é uma bijeção que preserva a ordem. Portanto, ϕ^* é um isomorfismo de ordem, que também satisfaz $\phi^*|_I = \phi$. ■

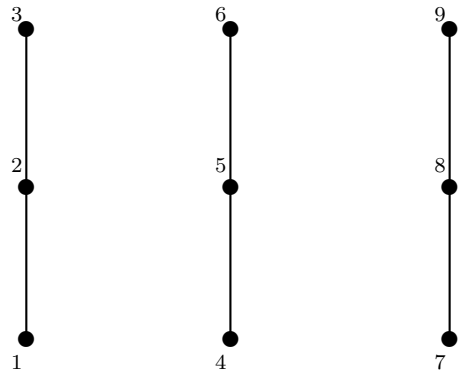
4.2 Formato de um vetor

Como foi visto no Exemplo 4.2 nos espaços munidos de métricas anti-cadeia, cadeia e hierárquicas, dois vetores têm o mesmo peso se, e somente se, eles estão na mesma órbita das isometrias. Neste contexto, o peso é um invariante numérico do vetor que caracteriza a órbita a qual ele pertence. Toda função que tiver esta propriedade será chamada de *formato* (shape) do vetor.

Definição 4.6. *Seja $(\mathbb{F}_q^n, P)$ um espaço poset. Uma aplicação $s : \mathbb{F}_q^n \to \mathbb{Z}^m$ é dita uma aplicação* formato *ou* shape *se ela é constante em cada órbita dos elementos de $GL_P(n)$. Se s é uma aplicação formato, $s(x)$ é chamado de formato de x.*

Posets NRT também satisfazem a propriedade-IE, mas a cardinalidade dos ideais não é o suficiente para determinar as órbitas dos isomorfismos, de fato, considere o seguinte exemplo.

Exemplo 4.3. *Seja $P = ([9], \preceq)$ um poset NRT definido como a união de 3 cadeias disjuntas de comprimento 3. Tome também $\{3\}$ e $\{1, 4, 7\}$. Assim $\langle 3\rangle = \{1, 2, 3\}, \langle 1, 4, 7\rangle = \{1, 4, 7\}$, ou seja, $|\langle 3\rangle| = |\langle 1, 4, 7\rangle|$, mas claramente $\langle 7\rangle$ e $\langle 1, 2, 3\rangle$ não são isomorfos.*



O formato de vetores são conhecidos apenas para um pequeno número de posets. Seguem mais alguns exemplos de formatos.

Exemplo 4.4. *Formato em posets hierárquicos.*

Seja $x \in (\mathbb{F}_q^n, d_P)$ com P um poset hierárquico. Tome $s(x) = \omega_{d_P}(x)$. Foi visto no Exemplo 4.2 que se $x, y \in \mathbb{F}_q^n$ são tais que $\omega_{d_P}(x) = \omega_{d_P}(y)$, então existe $T \in GL_P(n)$ tal que $T(x) = y$, logo ω_{d_P} é um formato.

Lembrando que posets hierárquicos são uma generalização dos posets cadeia e anti cadeia, segue que o peso também é um formato para essas duas famílias.

Exemplo 4.5. *Formato para posets NRT.*([4])

Seja $n = m.r$ e P uma união disjunta de r cadeias de comprimento m e $x \in (\mathbb{F}_q^n, d_P)$. Desta forma, x é a concatenação de r blocos de comprimento m cada, onde o suporte do $i-$ésimo bloco está contido na i-ésima componente de P. Assim, tem-se a seguinte expressão para x:

$$x = (x_{11}, \ldots, x_{1m}; x_{21}, \ldots, x_{2m}; \ldots, x_{r1}, \ldots, x_{rm}).$$

Desta maneira, o formato de x é definido como

$$\text{shape}(x) = e = (e_0, e_1, \ldots, e_m),$$

onde $e_0 = r - \sum_{i=1}^{m} e_i$ e para $i = 1, \ldots, m, e_i$ é a quantidade de blocos de x tais que a última componente não-nula é a i-ésima, contando a partir do começo do bloco. Em outras palavras, se $x = (x_1, \ldots, x_r)$, onde x_i é o $i =$ésimo bloco de x, então $e_i = |\{x_j; |\langle x_j \rangle| = i\}|$. Ou seja, e_i conta quantas componentes de x têm peso i. Então, a partir desta definição de formato é imediato

ver que se $\text{shape}(x) = e = (e_0, e_1, \ldots, e_m)$*, tem-se que* $\omega_P(x) = \sum_{i=1}^{m} ie_i$*, mas a recíproca não é verdadeira, isto é, existem palavras com o mesmo peso e formatos diferentes.*

Para mostrar que, de fato, esta função é um formato para posets NRT tome a decomposição de $\mathbb{F}_q^n$ *induzida pelas cadeias de* P*, isto é,*

$$\mathbb{F}_q^n = \underbrace{\mathbb{F}_q^m \oplus \ldots \oplus \mathbb{F}_q^m}_{r \text{ vezes}}.$$

Esta decomposição de $\mathbb{F}_q^n$ *induz naturalmente uma decomposição dos elementos, isto é, se* $x \in \mathbb{F}_q^n$*, então* x *pode ser escrito de forma única como* $x = x_1 + \ldots + x_r$*, com* $x_i \in \mathbb{F}_q^m$ *e, com isso* $\langle \text{supp}(x) \rangle = \langle \text{supp}(x_1) \rangle \cup \ldots \cup \langle \text{supp}(x_r) \rangle$*. Desta forma,* $\langle \text{supp}(x) \rangle \sim \langle \text{supp}(y) \rangle$ *se, e somente se* $\langle \text{supp}(x_i) \rangle \sim \langle \text{supp}(y_{\sigma(i)}) \rangle$ *onde* σ *é uma permutação em* $\{1, \ldots, r\}$*. Como a métrica NRT restrita a cada componente* $\mathbb{F}_q^m$ *é exatamente a métrica cadeia,* $\langle \text{supp}(x_i) \rangle \sim \langle \text{supp}(y_{\sigma(i)}) \rangle$ *se, e somente se, as duas palavras tem a mesma altura. Então, se* $\text{shape}(x) = \text{shape}(y)$ *estes elementos têm a mesma quantidade de componentes com a mesma altura, daí segue que* $\langle \text{supp}(x) \rangle \sim \langle \text{supp}(y) \rangle$*.*

A estrutura do grupo de isometrias sugere que os formatos são determinados pelos ideais, e não pelos vetores. Este é o caso de todos os exemplos conhecidos. Em particular, se P possui a propriedade-IE, então o formato depende apenas das classes de ideais isomorfos no sentido que $\text{shape}(x) = \text{shape}(y)$ se, e somente se, $\langle x \rangle \sim \langle y \rangle$. Usualmente, é difícil se determinar o formato, e acreditamos que não é possível determinar uma expressão genérica para o formato. Ainda mais, nos casos conhecidos o formato não determina apenas as órbitas das isometrias, mas também outras importantes invariantes, tais como, o peso do vetor e o raio de empacotamento dos espaços uni-dimensionais gerados por ele.

4.2.1 Formato para Posets Árvore uni-raiz, Regulares por Nível

Na Proposição 4.1 foi mostrado que se P é um poset, então o formato dos vetores em $(\mathbb{F}_q^n, d_P)$ é determinado por ideais, isto é, x e y estão na mesma órbita de $GL_P(n)$ se, e somente se, $\langle x \rangle \sim \langle y \rangle$. Assim, as órbitas são caracterizadas pelas classes de equivalência de ideais $\tilde{I}$.

Note que se P é uma árvore uni-raiz, regular por nível, os ideais de P são sub-árvores (não necessariamente regulares por nível), e seus isomorfismos podem ser obtidos pela restrição dos

automorfismos de P. De fato, na Proposição 4.2 foi mostrado que árvores regulares por nível têm a propriedade-IE.

O problema de isomorfismo de árvores é um assunto clássico na ciência da computação. Encontramos na literatura ([22],[1]) indicações de como caracterizar as órbitas por isomorfismo de subárvores, sem, no entanto, encontrar demonstrações de que de fato essas caracterizações são válidas. Nesta seção será demonstrado que uma dessas maneiras de representar uma árvore (ou sub-árvore) através de uma sequência numérica (conforme feito em [22]) caracteriza as órbitas dos elementos de $\mathbb{F}_q^n$ por isometrias, o que pela Proposição 4.1 significa que árvores que forem representadas pela mesma sequência são isomorfas.

Segundo [6], as *as sub árvores imediatas de* $\mathcal{H}$ são as subárvores de $\mathcal{H}$ que têm como raízes os filhos da raiz de $\mathcal{H}$. Para melhor compreensão desta definição, considere o seguinte exemplo:

Exemplo 4.6. *Seja* $\mathcal{H}$ *uma* $(27; 2, 3, 1, 2)$ *árvore regular por nível. A raiz de* $\mathcal{H}$ *(representado pelo número* 1*) tem exatamente dois filhos* ($q_1 = 2$)*. Assim* $\mathcal{H}$ *tem duas sub-árvores imediatas* $\mathcal{H}_1$ *e* $\mathcal{H}_2$ *cujas raízes são os filhos de* 1 *que são representados por* 2 *e* 3*. Assim,* $\mathcal{H}_1$ *e* $\mathcal{H}_2$ *são as* $(12; 3, 1, 2)$ *árvores regulares por nível* $\mathcal{H}_1$ *e* $\mathcal{H}_2$ *que têm como raízes* 2 *e* 3*, respectivamente, isto é,* $\mathcal{H}_1$ *é constituída pelos vértices* $2, 4, 5, 6, 10, 11, 12, 16, 17, 18, 19, 20, 21$ *e* $\mathcal{H}_2$ *é constituída por* $3, 7, 8, 9, 13, 14, 15, 22, 23, 24, 25, 26, 27$.

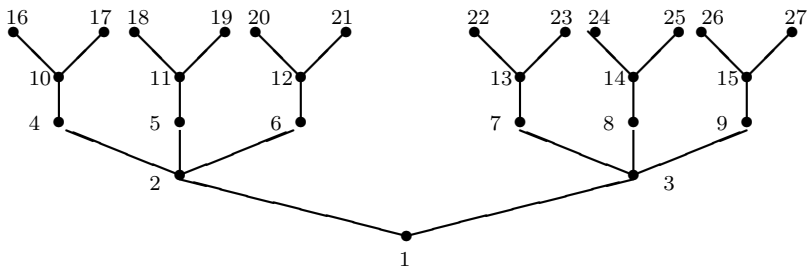


Figura 4.1: Diagrama de Hasse de uma $(27; 2, 3, 1, 2)$ árvore regular por nível.

Candidatos a formato em árvores uni-raiz, regulares por nível

Antes de finalmente chegarmos a um formato em posets árvore uni-raiz, regular por nível, testamos uma série de candidatos. Com fim de registro, apresentaremos esses candidatos a

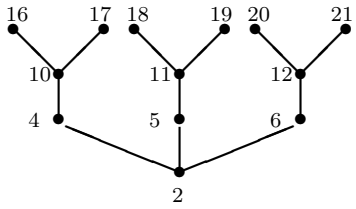


Figura 4.2: Diagrama de Hasse de $\mathcal{H}_1$

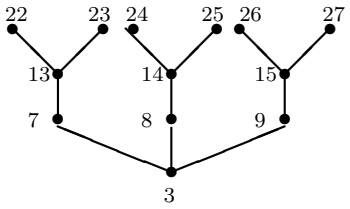


Figura 4.3: Diagrama de Hasse de $\mathcal{H}_2$

seguir, discutindo porque eles pareciam bons candidatos e porque eles não são funções formato, lembrando que já foi mostrado (Exemplo 4.3) que o peso, nem sempre é um formato. Nos exemplos a seguir, nos referiremos ao formato de uma palavra como o formato do ideal gerado pelo seu suporte.

Tentativa 1

Inspirado no formato em posets NRT, definimos $s(I) =: (e_0, e_1, \ldots, e_h)$, onde e_i é a quantidade de elementos de I no i-ésimo nível, ou seja

$$e_i = |\{x \in I; l(x) = i\}|,$$

onde l é a função altura.

Tentativa 4.1. *Duas sub-árvores são isomorfas se, e somente se, elas têm a mesma altura e a mesma quantidade de elementos em cada nível.*

Porém, esta conjectura se mostrou falsa. Segue um contra exemplo.

Exemplo 4.7. *Seja P um $(13; 4, 2)$ poset árvore uni-raiz, regular por nível representado pela figura 4.4:*

Em P considere $I = \langle 3, 4, 5, 6, 7\rangle$ e $J = \langle 3, 4, 6, 13\rangle$ representados nas figuras 4.5 e 4.6, respectivamente. $s(I) = (1, 4, 2) = s(J)$, mas claramente não são sub-arvores isomorfas, umas vez que em I existem dois elementos maiores que dois, enquanto em J não existe nenhum elemento no segundo nível que seja menor que dois elementos de J. .

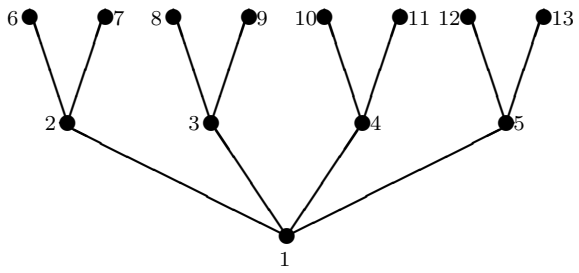


Figura 4.4: Diagrama de Hasse de um $(13; 4, 2)$ poset árvore regular por nível.

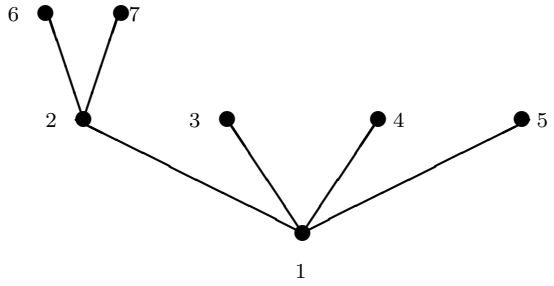


Figura 4.5: Diagrama de Hasse de $I = \langle 3, 4, 5, 6, 7\rangle$

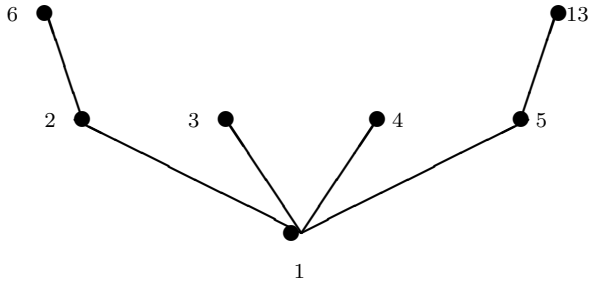


Figura 4.6: Diagrama de Hasse de $J = \langle 3, 4, 6, 13\rangle$

Tentativa 2

Por que o exemplo anterior não funcionou? Talvez porque não levamos em consideração o *espectro de graus* de P.

Definição 4.7. *O espectro de graus de uma árvore é a sequência de inteiros não negativos* $\{d_j\}_{j\in\mathbb{Z}^+}$, *onde* d_j *é o número de vértices que têm* j *filhos.*

Assim, façamos uma nova tentativa.

Tentativa 4.2. *Duas sub-árvores são isomorfas se, e somente se, elas têm o mesmo espectro de graus.*

Esta tentativa também falhou. Vejamos porque.

Exemplo 4.8. *Considere* P *um* $(11; 2, 2, 1)$ *poset árvore uni-raiz, regular por nível conforme representado na figura 4.7 e tome* $I, J \in \mathcal{I}(\mathcal{C})$ *dados por* $I = \langle 4, 5, 10\rangle$ *e* $J = \langle 5, 6, 8\rangle$*, representados nas figuras 4.8 e 4.9. Note que ambos possuem* $(3, 2, 2)$ *como espectro de graus, porém*

não são isomorfos, uma vez que em J existe um elemento no segundo nível que é menor que 3 *elementos de J e isso não acontece em I*

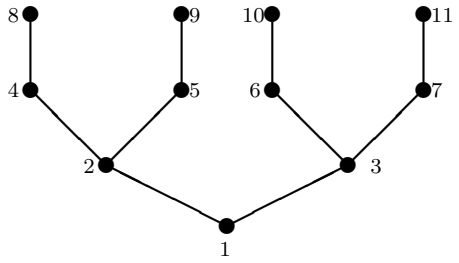


Figura 4.7: Diagrama de Hasse de um $(11; 2, 2, 1)$ poset árvore regular por nível.

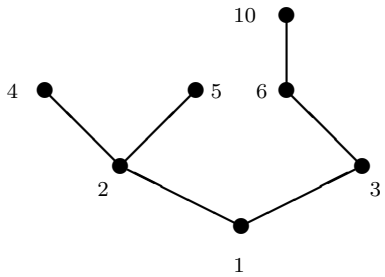


Figura 4.8: Diagrama de Hasse de $I = \langle 4, 5, 10\rangle$

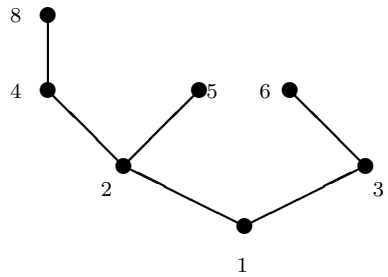


Figura 4.9: Diagrama de Hasse de $J = \langle 5, 6, 8\rangle$

Tentativa 3

A conjectura anterior parecia boa, porém, ela não se preocupava em como se davam as ramificações. Para tentar resolver esse problema, considere a seguinte tentativa:

Tentativa 4.3. *Duas sub-árvores são isomorfas se, e somente se, elas têm o mesmo espectro de graus em cada nível.*

Essa conjectura, engloba os principais aspectos das duas anteriores: uma vez que ter espectros de graus iguais em cada nível necessariamente implica que teremos as mesmas quantidades de elementos em cada nível e obviamente, ter espectros de graus iguais em cada nível também implica que temos o mesmo espectro de graus.

Infelizmente, essa tentativa também é falha.

Exemplo 4.9. *Seja P um $(31; 2, 2, 2, 2)$ poset árvore regular por nível como representado na figura 4.10. Em P considere os ideais $I = \langle 4, 5, 14, 31\rangle$ e $J = \langle 5, 7, 9, 16\rangle$, representados nas figuras 4.11 e 4.12, respectivamente. Em ambos os ideais temos os seguintes espectros de graus em cada nível:*

Nível	*Espectro de graus*
Primeiro	$(0, 0, 1)$
Segundo	$(0, 1, 1)$
Terceiro	$(2, 0, 1)$
Quarto	$(1, 1, 0)$
Quinto	$(1, 0, 0)$

Entretanto, eles não podem ser isomorfos, uma vez que em I o elemento 2 está no segundo nível e tem apenas dois elementos de I que são maiores que ele, enquanto em J existem 1 ou 5 elementos maiores que os elementos do segundo nível.

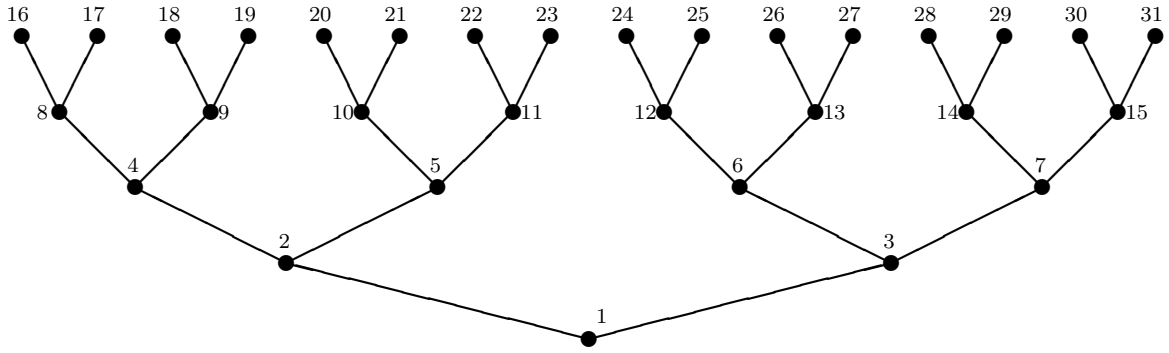


Figura 4.10: Diagrama de Hasse de um $(31; 2, 2, 2, 2)$ poset árvore regular por nível.

Formato em árvore uni-raiz, regular por nível

Acabamos de ver uma série de candidatos a formato em árvores uni-raiz, regulares por nível, mas nenhum deles serviu. Apresentaremos agora uma função que, finalmente, cumpre as condições para ser uma função formato em posets árvore uni-raiz, regular por nível.

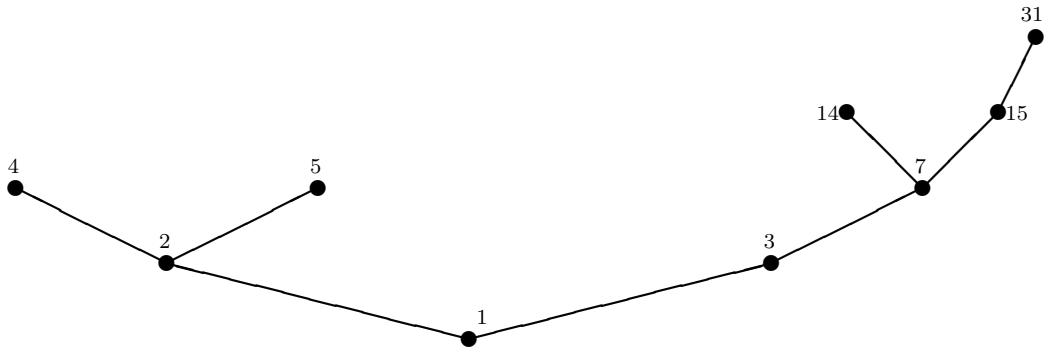


Figura 4.11: Diagrama de Hasse de $I = \langle 4, 5, 14, 31 \rangle$.

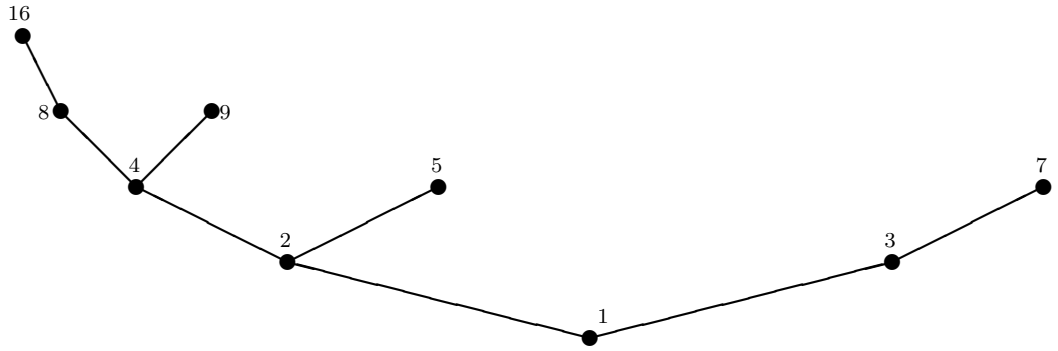


Figura 4.12: Diagrama de Hasse de $J = \langle 5, 7, 9, 16 \rangle$.

Definição 4.8. *[1] Dada uma árvore uni-raiz $\mathcal{H}$. Definimos o string $St(\mathcal{H})$ de $\mathcal{H}$ recursivamente, por*

- 10*, se* $|\mathcal{H}| = 1$*;*
- $1St(\mathcal{H}_{\sigma(1)})St(\mathcal{H}_{\sigma(2)})...St(\mathcal{H}_{\sigma(p)})0$ *se* $|\mathcal{H}| \geq 1$*, onde* $\mathcal{H}_i$ *é uma sub-árvore imediata de* $\mathcal{H}$*,* $St(\mathcal{H}_i)$ *é o string de* $\mathcal{H}_i$ *e* σ *é uma permutação em* $[p]$ *tal que* $St(\mathcal{H}_{\sigma(r)}) \geq St(\mathcal{H}_{\sigma(r+1)})$*.*

Strings são palavras binárias que também podem ser vistas como números inteiros (por isso podemos incluir a condição $St(\mathcal{H}_{\sigma(r)}) \geq St(\mathcal{H}_{\sigma(r+1)})$ na Definição 4.8). Note que o string é definido para uma árvore uni-raiz qualquer, isto é, sua definição não se restringe às árvores uni-raiz, regulares por nível, no entanto, será mostrado que o string funciona como um formato para posets árvore uni-raiz, regular por nível.

A figura 4.13 ilustra o cálculo do string de uma árvore uni-raiz.

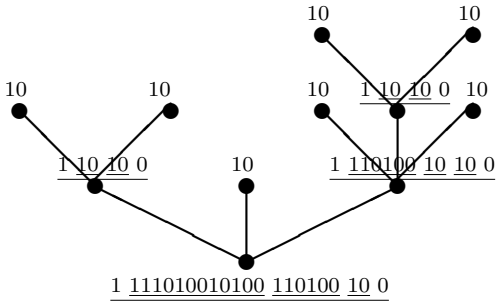


Figura 4.13: Cálculo do string de uma árvore

Observação 4.1. *Note que o string determina a cardinalidade de $\mathcal{H}$ pois para cada nó da árvore são introduzidos dois dígitos ao string, um* 0 *e um* 1*. Assim, $|\mathcal{H}|$ é igual a metade do comprimento do string ou igual a quantidade de 0's ou igual a quantidade de 1's que aparecem no string.*

Observação 4.2. *A partir do string de $\mathcal{H}$ é possível recuperar o string de suas sub-árvores imediatas. Para tal, deve-se proceder da seguinte maneira: seja $St(\mathcal{H}) = \delta_1\delta_2\cdots\delta_{2|\mathcal{H}|-1}\delta_{2|\mathcal{H}|}$ o string de uma árvore, onde $\delta_i \in \{0.1\}$*

(*i*) $\delta_1 = 1$ *e* $\delta_{2|\mathcal{H}|} = 0$;

(*ii*) *A partir de* δ_2*, conte a quantidade de* $0's$ *e* $1's$*. Quando elas forem iguais, pare;*

(*iii*) *Seja* $t_1 \in \{3, \cdots, 2|\mathcal{H}| - 1\}$ *o último* δ_i *que entrou na contagem do item anterior;*

(*iv*) $St(S_1) = \delta_2 \cdots \delta_{t_1}$;

(*v*) *Para obter o string da próxima sub árvore imediata, volte para o item* (*ii*) *a partir de* δ_{t_1+1};

(*vi*) *Pare quando* $\delta_{t_p} = \delta_{2|\mathcal{H}|-1}$*, para algum* p*.*

Para melhor compreensão deste processo, considere o seguinte exemplo:

Exemplo 4.10. *Seja* $\mathcal{H}$ *tal que* $St(\mathcal{H}) = 11101001100100$

(*i*) $\delta_1 = 1$ *e* $\delta_{14} = 0$;

(*ii*) *A partir de* δ_2*, a primeira vez que temos a mesma quantidade de* $0's$ *e* $1's$ *é em* δ_7;

(*iii*) $St(\mathcal{H}_1) = 110100 = \delta_2 \dots \delta_7$;

(*iv*) *A partir de* δ_8*, a primeira vez que temos a mesma quantidade de* $0's$ *e* $1's$ *é em* δ_{11};

(*v*) $St(\mathcal{H}_2) = 1100 = \delta_8 \dots \delta_{11}$;

(*vi*) *A partir de* δ_{12}*, a primeira vez que temos a mesma quantidade de* $0's$ *e* $1's$ *é em* $\delta_{13} = \delta_{2|\mathcal{H}|-1}$*, ultima subárvore;*

(*vii*) $St(\mathcal{H}_3) = 1\delta_{12}\delta_{13}0$.

Agora será apresentada uma definição de isomorfismo de árvores uni-raiz que é compatível com a a ordem induzida por elas. Mais adiante (Proposição 4.4) será mostrado que o conceito de isomorfismo de árvores uni-raiz e de isomorfismo de posets são equivalentes para posets árvore uni-raiz.

Definição 4.9. [6] *Seja* $T : \mathcal{H}_1 \to \mathcal{H}_2$ *uma bijeção. Temos que* T *é um isomorfismo de árvores uni-raiz se:*

- $|\mathcal{H}_1| = |\mathcal{H}_2| = 1$

Ou

- $\mathcal{H}_1$ *e* $\mathcal{H}_2$ *têm o mesmo número de sub árvores imediatas e sendo* $S_1, \cdots, S_p$ *as sub árvores imediatas de* $\mathcal{H}_1$ *e* $S_1', \cdots, S_p'$ *as sub árvores imediatas de* $\mathcal{H}_2$*, tem-se que:*

  (*i*) $T(S_i) = S'_{\sigma(i)}$*, onde* $\sigma : \{1, \cdots, p\} \longrightarrow \{1, \cdots, p\}$ *é uma permutação;*

  (*ii*) $T|_{S_i}$ *é isomorfismo de árvores uni-raiz para* $i = 1, \cdots, p$

Agora mostraremos que duas árvores uni-raiz $\mathcal{H}_1$ e $\mathcal{H}_2$ possuem o mesmo string se, e somente se, elas são isomorfas. Note que isso ainda não é equivalente a mostrarmos que o string é um formato. Para tal, seria necessário que $\mathcal{H}_1$ e $\mathcal{H}_2$ fossem sub-árvores de uma árvore maior $\mathcal{H}$ e que esse isomorfismo entre $\mathcal{H}_1$ e $\mathcal{H}_2$ fosse uma restrição de um automorfismo de $\mathcal{H}$.

Proposição 4.3. *Sejam $\mathcal{H}_1$ e $\mathcal{H}_2$ duas árvores uni-raiz. $St(\mathcal{H}_1) = St(\mathcal{H}_2)$ se, e somente se, existe $T : \mathcal{H}_1 \to \mathcal{H}_2$ um isomorfismo de árvores uni-raiz.*

Demonstração: Supondo que existe um isomorfismo de árvores uni-raiz T, tal que $T(\mathcal{H}_1) = \mathcal{H}_2$. Assim, $|\mathcal{H}_1| = |\mathcal{H}_2|$ uma vez que T é uma bijeção.

Essa demonstração será feita por indução em $|\mathcal{H}_1|$.

Se $|\mathcal{H}_1| = |\mathcal{H}_2| = 1$, então $St(\mathcal{H}_1) = St(\mathcal{H}_2) = 10$.

Se $|\mathcal{H}_1| > 1$, sejam $S_1, \cdots, S_p$ as sub árvores imediatas de $\mathcal{H}_1$ e $S_1^{'}, \cdots, S_q^{'}$ as de $\mathcal{H}_2$. Por definição de isomorfismo de árvores uni-raiz, $p = q$ e $T(S_i) = S_{\sigma(i)}^{'}$, onde σ é uma permutação em $[p]$. Assim, por hipótese de indução, $St(S_i) = St(S_{\sigma(i)}^{'})$ e dessa forma $St(\mathcal{H}_1) = St(\mathcal{H}_2)$.

Suponha agora que $St(\mathcal{H}_1) = St(\mathcal{H}_2)$. Assim, pela observação 4.1 $|H_1| = |\mathcal{H}_2|$. Faremos novamente por indução em $|\mathcal{H}_1|$. Como de costume, se $|\mathcal{H}_1| = |\mathcal{H}_2| = 1$ não há nada a ser feito.

Se $|\mathcal{H}_1| > 1$, seja $St(\mathcal{H}_1) = St(\mathcal{H}_2) = 1St(S_{\sigma(1)}) \cdots St(S_{\sigma(p)})0 = 1St(S'_{\gamma(1)}) \cdots St(S'_{\gamma(p)})0$, obtido da maneira apresentada na observação 4.2, ou seja $S_1, \ldots, S_p$ e $S'_1, \ldots, S'_p$ são sub árvores imediatas de $\mathcal{H}_1$ e $\mathcal{H}_2$ respectivamente e σ, γ são permutações em $[p]$ tais que $St(S_{\gamma(r)}) \geq St(S_{\gamma(r+1)})$ e $St(S'_{\sigma(r)}) \geq St(S'_{\sigma(r+1)})$. Assim, $St(S_{\sigma(i)}) = St(S'_{\gamma(i)})$ para $i = 1, \cdots, p$. Como $|St(S_{\sigma(i)})| = |St(S'_{\gamma(i)})| < |\mathcal{H}_1|$, por hipótese de indução, $S_{\sigma(i)}$ e $S'_{\gamma(i)}$ são sub-árvores isomorfas para todo $i = 1, \cdots, p$. Assim, $\mathcal{H}_1$ e $\mathcal{H}_2$ são árvores isomorfas ■

Definição 4.10. *Seja $\mathcal{H}$ um poset árvore uni-raiz, regular por nível e $v \in \mathcal{H}$. Denote por $v\mathcal{H}$ a maior sub-árvore de $\mathcal{H}$ que tem v como raiz, isto é, $v\mathcal{H} = \{y \in \mathcal{H}; v \preceq y\} = \langle v \rangle_{\mathcal{H}^\perp}$.*

Lema 4.4. *$T : \mathcal{H}_1 \to \mathcal{H}_2$ um isomorfismo de ordem e $v \in \mathcal{H}_1$. Então $T(v\mathcal{H}_1) = T(v)\mathcal{H}_2$*

Demonstração: Se $y \in T(v\mathcal{H}_1)$, então, existe $z \in v\mathcal{H}_1$ tal que $T(z) = y$. Seja $v = x_0 \preceq x_1 \cdots \preceq x_r = z$ a (única) cadeia que liga v a z com x_{i+1} sendo filho de x_i, para todo $i = 1, \cdots, r-1$. Como T é um isomorfismo de ordem, $T(v) = T(x_0) \preceq T(x_1) \cdots \preceq T(x_r) = T(z)$ é a (única) cadeia que liga $T(v)$ a $T(z) = y$ com $T(x_{i+1})$ sendo filho de $T(x_i)$, para todo $i = 1, \cdots, r-1$. Assim, $T(v) \preceq y$, o que implica que $y \in T(v)\mathcal{H}_2$.

Seja $y \in T(v)\mathcal{H}_2$ e sejam $T(v) = y_0 \preceq y_1 \preceq \cdots \preceq y_r = y$ a (única) cadeia que liga $T(v)$ a y com y_{i+1} sendo filho de y_i, para todo $i = 1, \cdots, r-1$ o conjunto de arestas que unem $T(v)$ a y. T é uma bijeção, então, para cada $i = 1, \cdots, r$ existe $x_i \in \mathcal{H}_1$ tal que $T(x_i) = y_i$ e existe

$x \in \mathcal{H}_1$ tal que $T(x) = y$, ou seja $T(v) \preceq T(x_1) \preceq \cdots \preceq T(x_r) = T(x)$, então, por T ser um isomorfismo de ordem, $v \preceq x_1 \preceq \cdots \preceq x_r = x$. Assim $v \preceq x$, ou seja, $x \in v\mathcal{H}_1$, que implica que $T(x) = y \in T(v\mathcal{H}_1)$. ■

O lema a seguir mostra que o resultado obtido no lema anterior é verdadeiro no caso de isomorfismo de árvores uni-raiz.

Lema 4.5. *Seja $T : \mathcal{H}_1 \to \mathcal{H}_2$ um isomorfismo de árvores uni-raiz e $v \in \mathcal{H}_1$. Então $T(v\mathcal{H}_1) = T(v)\mathcal{H}_2$*

Demonstração: Seja $T : \mathcal{H}_1 \to \mathcal{H}_2$ um isomorfismo de árvores uni-raiz e $v \in \mathcal{H}_1$. Pela definição de isomorfismo de árvores uni-raiz Tv é o elemento de $\mathcal{H}_2$ tal que se w é filho de v, então existe u filho de Tv tal que $T(w\mathcal{H}_1) = u\mathcal{H}_2$, pois $w\mathcal{H}_1$ é uma sub-árvore imediata de $v\mathcal{H}_1$ e $u\mathcal{H}_2$ é uma sub-árvore imediata de $T(v)\mathcal{H}_2$, isso implica que $T(v\mathcal{H}_1) \subseteq T(v)\mathcal{H}_2$.

Note também, que não existe u filho de Tv tal que não exista w filho de v com $T(w\mathcal{H}_1) = u\mathcal{H}_2$, uma vez que $T|_{v\mathcal{H}_1}$ é isomorfismo de árvores uni-raiz, portanto, as sub-árvores imediatas de $T(v)\mathcal{H}_2$ são imagens por T de sub-árvores de $v\mathcal{H}_1$. Assim, temos que:

$$T(v\mathcal{H}_1) = T(v)\mathcal{H}_2.$$

■

Os lemas 4.4 e 4.5 mostram uma característica compartilhada por isomorfismos de árvores uni-raiz e os isomorfismos de ordem, isso sugere que existe alguma relação entre esses dois tipos distintos de isomorfismo. A Proposição a seguir mostra que de fato, esses isomorfismos são equivalentes.

Proposição 4.4. *Seja $T : \mathcal{H}_1 \to \mathcal{H}_2$ uma bijeção entre $\mathcal{H}_1$ e $\mathcal{H}_2$. T é isomorfismo de ordem se, e somente se, é isomorfismo de árvores uni-raiz.*

Demonstração: Suponha que T é um isomorfismo de árvores uni-raiz. Sejam $x, y \in \mathcal{H}_1$ tal que $x \preceq y$. Começaremos assumindo que y é filho de x. Pelo lema 4.5 temos que $T(x\mathcal{H}_1) = T(x)\mathcal{H}_2$. Como y é filho de x segue que $y\mathcal{H}_1$ é uma sub-árvore imediata de $x\mathcal{H}_1$, assim, existe $\mathcal{H}_3$ uma sub-árvore imediata de $T(x\mathcal{H}_1) = T(x)\mathcal{H}_2$ tal que $T(y\mathcal{H}_1) = \mathcal{H}_3$. Mas se $\mathcal{H}_3$ é sub-árvore imediata de $T(x)\mathcal{H}_2$, temos que $\mathcal{H}_3 = z\mathcal{H}_2$, onde z é filho de $T(x)$. Mas novamente, pelo lema 4.5, temos que $\mathcal{H}_3 = z\mathcal{H}_2 = T(y\mathcal{H}_1) = T(y)\mathcal{H}_2$. Como T é uma bijeção, $z = T(y)$, o que implica que $T(y)$ é um filho de $T(x)$.

Caso y não seja um filho de x, considere a (única) cadeia $x = x_0 \preceq x_1 \preceq x_2 \cdots \preceq x_r = y$ tal que x_{i+1} é filho de x_i. Assim, pelo caso anterior, temos que $T(x_{i+1})$ é filho de $T(x_i)$. Assim temos $T(x) = T(x_0) \preceq T(x_1) \preceq T(x_2) \cdots \preceq T(x_r) = T(y)$.

Isso mostra que todo isomorfismo de árvores uni-raiz também é um isomorfismo de ordem.

Suponha agora que T é um isomorfismo de ordem. Se $|\mathcal{H}_1| = |\mathcal{H}_2| = 1$, não há nada a fazer.

Suponha agora que $|\mathcal{H}_1| = |\mathcal{H}_2| > 1$. Sejam $S_1 \cdots, S_p$ as sub árvores imediatas de $\mathcal{H}_1$, $S'_1 \cdots, S'_q$ as sub árvore imediatas de $\mathcal{H}_2$, α a raiz de H_1, α_i a raiz de S_i para $i = 1 \cdots, p$, β a raiz de $\mathcal{H}_2$ e β_i a raiz de S'_i para $i = 1 \cdots, q$, ou seja, α_i é filho de α para $i = 1, \cdots, p$ e β_i é filho de β para $i = 1, \cdots q$. Note que $T(\alpha) = \beta$ e como T é um isomorfismo de ordem, temos também que T é uma bijeção entre os filhos de α e β. Assim, temos que $p = q$ e $T(\alpha_i) = \beta_{\sigma(i)}$, onde σ é uma permutação em $\{1, \cdots, p\}$.

Precisamos agora mostrar que $T|S_i$ é um isomorfismo de árvores uni-raiz para $i = 1, \cdots, p$. De fato, suponha que exista i tal que $T|S_i$ não seja um isomorfismo de árvores uni-raiz.

T é isomorfismo de ordem, em particular é injetor, portanto $|S_i| = |T(S_i)|$. Se $T|S_i$ não é um isomorfismo de árvores uni-raiz um dos seguintes fatos ocorre:

a) A quantidade de sub árvores imediatas de S_i e de $T(S_i)$ são diferentes;

b) Existe U_j sub árvore imediata de S_i tal que $T(U_j)$ não é uma sub árvore imediata de $T(S_i)$;

c) Existe U_j sub árvore imediata de S_i tal que $T|U_j$ não é isomorfismo de árvores.

Temos que a quantidade de sub-árvores imediatas é igual ao número de filhos e como T é um isomorfismo de ordem, (a) não acontece. Pelo Lema 4.4, (b) não pode acontecer e se tivéssemos (c) daríamos um "loop" nas afirmações acima, e cada vez que uma sub árvore passar por esse "loop", a cardinalidade da sub-árvore tal que a restrição de T não é um isomorfismo de árvores uni-raiz diminui. E mais, em algum momento, esta sub-árvore terá cardinalidade 1 (quando possuir apenas a raiz). Seja S_i essa sub árvore tal que $|S_i| = 1$. Quando isso acontecer, teremos, $|T(S_i)| = 1$.

Segue que $T|S_i$ é um isomorfismo de árvores uni-raiz. ■

Corolário 4.1. *Sejam $\mathcal{H}_1$ e $\mathcal{H}_2$ árvores uni-raiz. $\mathcal{H}_1 \sim \mathcal{H}_2$ se, e somente se $St(\mathcal{H}_1) = St(\mathcal{H}_2)$.*

Demonstração: Da Proposição 4.3, $St(\mathcal{H}_1) = St(\mathcal{H}_2)$ se, e somente se existe $T : \mathcal{H}_1 \to \mathcal{H}_2$ um isomorfismos de árvores uni-raiz tal que $T(\mathcal{H}_1) = \mathcal{H}_2$. Da Proposição 4.4, T é um isomorfismo de ordem, portanto $\mathcal{H}_1 \sim \mathcal{H}_2$. ■

Corolário 4.2. *Seja $\mathcal{H}$ um poset árvore uni-raiz, regular por nível e $\mathcal{H}_1, \mathcal{H}_2 \in \mathcal{I}(\mathcal{H})$.*

$$\mathcal{H}_1 \sim \mathcal{H}_2 \text{ se, e somente se } St(\mathcal{H}_I) = St(\mathcal{H}_J)$$

Demonstração: Segue imediatamente do Corolário 4.1. ■

Assim, encerramos esta seção apresentando um formato para posets árvore uni-raiz, regular por nível .

Corolário 4.3. *Seja $P = ([n], \preceq)$ um poset árvore uni-raiz, regular por nível. Dados $x, y \in \mathbb{F}_q^n$, existe $T \in GL_P(n)$ tal que $T(x) = y$ se, e somente se, $St(\langle \text{supp}(x) \rangle) = St(\langle \text{supp}(y) \rangle)$.*

Demonstração: Seja $P = ([n], \preceq)$ um poset árvore uni-raiz, regular por nível. Segue da Proposição 4.2 que P tem a propriedade-IE. Da Proposição 4.1, isso é equivalente a $(\mathbb{F}_q^n, d_P)$ ter a propriedade $\tilde{I}$. Do Corolário 4.2, segue que $St(\langle \text{supp}(x) \rangle) = St(\langle \text{supp}(x) \rangle)$ se, e somente se $\langle \text{supp}(x) \rangle \sim \langle \text{supp}(y) \rangle$.

Como $(\mathbb{F}_q^n, d_P)$ tem a propriedade $\tilde{I}$, segue que $\langle \text{supp}(x) \rangle \sim \langle \text{supp}(y) \rangle$ se, e somente se, existe $T \in GL_P(n)$ tal que $T(x) = y$. ■

4.3 Operações em posets

Existem inúmeras maneiras de se obter novos posets a partir de outros posets. Além do poset dual, também existe a soma e o produto direto e a soma e o produto ordinal [26]. Já são conhecidas algumas famílias de posets que gozam da propriedade de extensão (hierárquicos, NRT e árvore uni-raiz, regular por nível). Nesta seção será estudado quando o poset que surge a partir de uma operação entre dois posets que possuem a propriedade-IE, herda esta propriedade de seus geradores e, no caso de tal poset herdar a propriedade-IE, se é possível estabelecer uma função formato para este novo poset em termos das funções formato dos posets geradores.

Sejam $P = ([n], \preceq_P)$ e $Q([m], \preceq_Q)$ posets com a propriedade-IE e suponha que shape_P e shape_Q sejam funções formato de P e Q respectivamente.

Soma Ordinal

O poset $P \oplus Q$ é definido em $[m+n]$ da seguinte maneira. Dados $i, j \in [m+n]$,

$$i \preceq_\oplus j \iff \begin{cases} i, j \leq n \text{ e } i \preceq_P j \text{ ou;} \\ i, j > n \text{ e } (i-n) \preceq_Q (j-n) \text{ ou;} \\ i \leq n \leq j. \end{cases}$$

Ou seja, o diagrama de Hasse de $P \oplus Q$ é o diagrama de Q desenhado sobre o diagrama de P e ligando todos os elementos minimais de Q a todos os elementos maximais de P.

Exemplo 4.11. *Suponha que $P = ([3], \preceq_P)$ seja um $(3; 1, 2)$ poset hierárquico e $Q = ([4], \preceq_Q)$ um NRT de duas cadeias de altura 2. Assim, temos os seguintes diagramas de Hasse:*

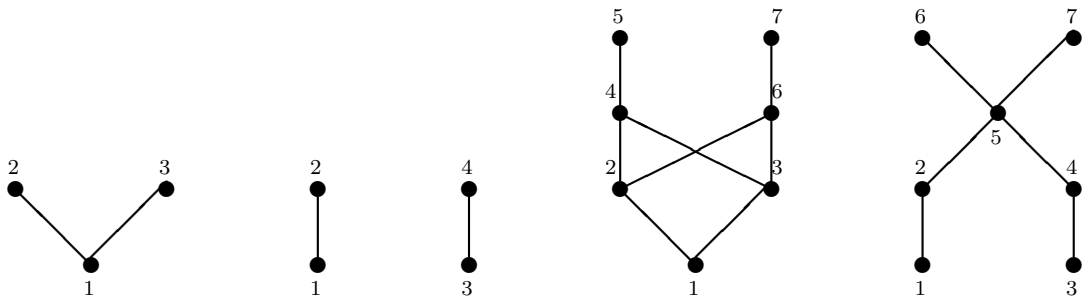


Figura 4.14: Diagramas de Hasse de $P = ([3], \preceq_P), Q = ([4], \preceq_Q), P \oplus Q = ([7], \preceq_{P\oplus Q})$ e $Q \oplus P = ([7], \preceq_{Q\oplus P})$, respectivamente.

Observe que o poset hierárquico é a soma ordinal de vários posets anti-cadeia (um para cada nível). Note também que é possível construir posets auto-duais a partir de posets quaisquer. Para tal, basta tomar $P \oplus P^\perp$ para qualquer poset P.

Lema 4.6. *Se P e Q satisfazem a propriedade-IE, então $P \oplus Q$ também satisfaz.*

Demonstração: Dado $Y \subset [m+n]$, considere os seguintes conjuntos:

$$\begin{aligned} Y_n &= \{i \in [m+n] : i \in Y \text{ e } i \leq n\}; \\ Y^m &= \{i \in [m+n] : i > n\}; \\ Y_m &= Y^m - n := \{i - n : i \in Y^m\}. \end{aligned}$$

Agora, seja $I \in \mathcal{I}(P \oplus Q)$. É imediato que $I_m \in \mathcal{I}(Q), I_n \in \mathcal{I}(P)$, e se $I_m \neq \emptyset$, então $I_n = [n]$. Inversamente, dado $I \in \mathcal{I}(Q), I \neq \emptyset$, segue que $[n] \cup \{i + n \mid i \in I\}$ é um ideal em $P \oplus Q$, e se $I \in \mathcal{I}(P)$, então (visto como um subconjunto de $[m+n]$) também é um elemento de $\mathcal{I}(P \oplus Q)$.

Assuma agora que $I, J \in \mathcal{I}(P \oplus Q)$ e suponha que existe um isomorfismo de posets $\phi : I \to J$. Naturalmente, temos que $\phi(I_n) = J_n$ e $\phi(I^m) = J^m$.

Primeiramente, suponha que $I_m \neq \emptyset$ (logo $J_m \neq \emptyset$), então $I_n = J_n = [n]$. Note que I_m e J_m, vistos como subconjuntos de $[m]$ são ideais em Q e a aplicação $\overline{\phi} : I_m \to J_m$ definida por $\overline{\phi}(i) = \phi(i+n) - n$ é um isomorfismo de posets entre I_m e J_m. Como Q tem a propriedade-IE existe $\xi \in Aut(Q)$ tal que $\xi(I_m) = J_m$. Definamos a aplicação $\tilde{\phi} : [m+n] \to [m+n]$ da seguinte maneira:

$$\tilde{\phi}(i) = \begin{cases} \xi(i-n) + n & \text{para } i > n \\ i & \text{para } i \leq n. \end{cases}$$

Assim, $\tilde{\phi} \in Aut(P \oplus Q)$ e $\tilde{\phi}(I) = J$.

Agora, suponha que $I_m = J_m = \emptyset$. Desta forma $I = I_n$ e $J = J_n$ são ideais isomorfos em $[n] \subset [m+n]$. Pela propriedade-IE de P, existe $\xi \in Aut(P)$ tal que $\xi(I_n) = J_n$. Defina a aplicação $\tilde{\phi} : [m+n] \to [m+n]$ da seguinte maneira:

$$\tilde{\phi}(i) = \begin{cases} i & \text{for } i > n \\ \xi(i) & \text{for } i \leq n. \end{cases}$$

Segue que $\tilde{\phi} \in Aut(P \oplus Q)$ e $\tilde{\phi}(I) = J$. ■

Para simplificar a notação, o formato em $P \oplus Q$ será denotado por $\text{shape}_{\oplus}$.

Proposição 4.5. *Seja $I \in \mathcal{I}(P \oplus Q)$. Então a seguinte aplicação*

$$\text{shape}_{\oplus}(I) = \begin{cases} (0, \text{shape}_P(I_n)) & \text{se } I_m = \emptyset \\ (1, \text{shape}_Q(I_m)) & \text{se } I_m \neq \emptyset \end{cases}$$

é uma função formato em $P \oplus Q$.

Demonstração: Sejam $I, J \in \mathcal{I}(P \oplus Q)$ ideais, e suponha que $\text{shape}_{\oplus}(I) = \text{shape}_{\oplus}(J)$. Suponhamos inicialmente que $I_m \neq \emptyset$, ou equivalentemente, que

$$\text{shape}_{\oplus}(I) = (1, \text{shape}_Q(I_m)) = \text{shape}_{\oplus}(J) = (1, \text{shape}_Q(J_m)),$$

ou seja, $\text{shape}_Q(I_m) = \text{shape}_Q(J_m)$. Segue que existe ϕ um isomorfismo de posets tal que $\phi(I_m) = J_m$. Uma vez que $I_m \neq \emptyset$, temos que $I_n = J_n = [n]$; assim, $I = [n] \cup I^m$ e $J = [n] \cup J^m$. Defina $\tilde{\phi} : [n+m] \to [n+m]$ da seguinte maneira:

$$\tilde{\phi}(i) = \begin{cases} i & \text{se } i \leq n \\ \phi(i-n) + n & \text{se } i > n. \end{cases}$$

Temos que $\tilde{\phi}$ é um isomorfismo de posets e que $\tilde{\phi}(I) = J$, isto é, $I \sim J$.

Agora, suponha que $I_m = \emptyset$. Desta forma, temos

$$(0, \text{shape}_P(I_n)) = (0, \text{shape}_P(J_n)) \Rightarrow \text{shape}_P(I) = \text{shape}_P(J_n).$$

Assim, pela definição de formato, temos que existe $\phi : [n] \to [n]$ um automorfismo de P tal que $\phi(I_n) = J_n$, Defina $\tilde{\phi} : I \to J$ da seguinte maneira:

$$\tilde{\phi}(i) = \begin{cases} \phi(i) & \text{se } i \leq n \\ i & \text{se } i > n. \end{cases}$$

Com isso, temos que $\tilde{\phi}$ é um automorfismo do poset $P \oplus Q$ tal que $\tilde{\phi}(I) = J$.

Reciprocamente, vamos assumir que $I \sim J$. Assim, temos que $I_n \sim J_n$ e $I^m \sim J^m$. Suponha que $I_m = \emptyset$. Como $I_n \sim J_n$ e P possui a propriedade-IE temos que $\text{shape}_P(I_n) = \text{shape}_P(J_n)$, e daí que

$$\text{shape}_{\oplus}(I) = (0, \text{shape}_P(I_n)) = (0, \text{shape}_P(J_n)) = \text{shape}_{\oplus}(J).$$

Supondo que $I_m \neq \emptyset$, então

$$I = [n] \cup I^m, \ J = [n] \cup J^m$$

e que o isomorfismo $\phi : I \to J$ leva I^m em J^m. Segue que a aplicação $\tilde{\phi} : I_m \to J_m$ definida por $\tilde{\phi}(i) = \phi(i+n) - n$ é um isomorfismo de posets em Q. Temos que Q possui a propriedade$-IE$, assim, temos que $\text{shape}_Q(I_m) = \text{shape}_Q(I_m)$, logo

$$\text{shape}_{\oplus}(I) = (1, \text{shape}_Q(I_m)) = (1, \text{shape}_Q(J_m)) = \text{shape}_{\oplus}(J).$$

■

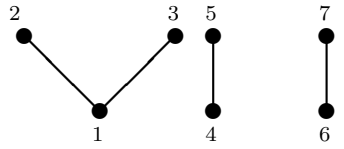
Soma Direta

Dados P e Q, a soma direta entre eles resulta num poset $P + Q$ cujo diagrama de Hasse é simplesmente os diagramas de P e Q um ao lado do outro. Para ser mais exato, dados $i, j \in [n + m]$ temos

$$i \preceq_+ j \iff \begin{cases} i, j \leq n \text{ e } i \preceq_P j \text{ ou} \\ i, j > n \text{ e } (i - n) \preceq_Q (j - n) \end{cases},$$

isto é, dois elementos só serão comparáveis se estiverem no mesmo poset gerador. Para ilustrar esta relação de ordem considere o seguinte exemplo:

Exemplo 4.12. *Considere os mesmos posets apresentados no Exemplo 4.11.* $(P+Q, \preceq_+)$ *tem a seguinte relação de ordem:* $1 \preceq_+ 2; 1 \preceq_+ 3; 4 \preceq_+ 5$ *e* $6 \preceq_+ 7$.



$P + Q = ([7], \preceq_{P+Q})$

Este poset não necessariamente herda a propriedade-IE de P e Q. Para comprovar tal fato, considere P e Q posets que não sejam isomorfos. Tome $i \in [n]$ um elemento minimal em P e $j \in [m]$ um minimal em Q. Os conjuntos $\{i\}$ e $\{j + n\}$ claramente são ideais isomorfos em $P + Q$, mas não existe automorfismo de posets em $P + Q$ que leve um no outro.

No entanto, note que se P e Q forem posets cadeia de mesma altura, possuindo portanto a propriedade-IE, o poset $P + Q$ é um poset NRT de duas cadeias. Logo, neste caso, $P + Q$ herda a propriedade.

Produto Ordinal

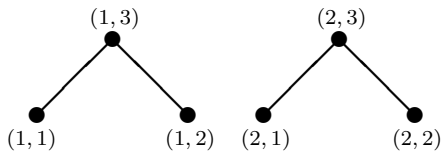
Dados dois posets $P = ([n], \preceq_P)$ e $Q = ([m], \preceq_Q)$, o poset $P \otimes Q = ([n] \times [m], \preceq_\otimes)$ é definido pela seguinte relação de ordem.

$$(i, j) \preceq_\otimes (i', j') \iff i = i' \text{ e } j \preceq_Q j'.$$

Note que na construção da relação de ordem $\preceq_{\otimes}$ a relação $\preceq_P$ não influencia em absolutamente nada. Assim $P \otimes Q$ é constituído de n cópias de Q onde os elementos só podem ser comparáveis se estiverem na mesma cópia de Q. Com isso, o diagrama de Hasse de $P \otimes Q$ será n cópias do diagrama de Hasse de Q desconexas postas uma ao lado da outra.

No produto ordinal existem casos em que a propriedade-IE é herdada de P e Q e casos em que ela não é herdada. De fato, Seja $P = ([n], \preceq_P)$ um poset qualquer sobre r e Q um poset cadeia sobre m. Como vimos anteriormente, $P \otimes Q$ será uma união de cópias desconexas de Q formando assim um poset NRT sobre $r = m.n$ e, como vimos no Exemplo 4.3, códigos NRT possuem a propriedade de extensão. Agora, para ilustrar um caso em que ela não é herdada, considere o seguinte exemplo:

Exemplo 4.13. *Seja P um poset qualquer sobre $\{1, 2\}$ e Q um $(3; 2, 1)-$poset hierárquico. Então, os conjuntos $I = \{(1, 1), (1, 2)\}$ e $J = \{(1, 1), (2, 1)\}$ são ideais isomorfos. Note também que não existe $\phi \in Aut(P \otimes Q)$ que leve I em J. De fato, $(1, 1)$ e $(1, 2) \preceq_{\otimes} (1, 3)$. No entanto, não existe $(x, y) \in P \otimes Q$ tal que $(1, 1)$ e $(2, 1) \preceq_{\otimes} (x, y)$ uma vez que $(1, 1) \preceq_{\otimes} (x, y)$ implica que $x = 1$.*



$P \otimes Q = ([2] \times [3], \preceq_{\otimes})$

Produto Direto

Dados dois posets $P = ([n], \preceq_P)$ e $Q = ([m], \preceq_Q)$, o poset $P \times Q = ([n] \times [m], \preceq_{\times})$ é definido pela seguinte relação de ordem:

$$(i, j) \preceq_{\times} (i', j') \iff i \preceq_P i' \text{ e } j \preceq_Q j'.$$

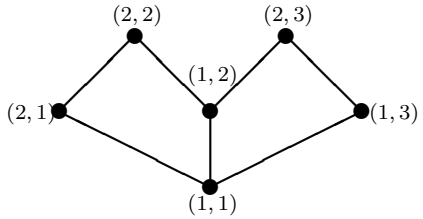
$P \times Q$ não necessariamente herda a propriedade-IE, como pode ser visto no seguinte exemplo:

Exemplo 4.14. *Sejam $P = ([2], \preceq_P)$ e $Q = ([3], \preceq_Q)$ tais que P é um poset cadeia e Q é um*

$(3; 1, 2)$ *poset hierárquico. Desta forma,* $\preceq_\times$ *é definido da seguinte forma:*

$$(1,1) \preceq_\times (2,1);\ (1,1) \preceq_\times (1,2); (1,1) \preceq_\times (1,3)$$
$$(2,1) \preceq_\times (2,2); (1,2) \preceq_\times (2,2); (1,2) \preceq_\times (2,3); (1,3) \preceq_\times (2,3).$$

Assim, os conjuntos $I = \{(1,1),(1,2)\}$ *e* $J = \{(1,1),(2,1)\}$ *são ideais em* $P \times Q$*, e são isomorfos, mas não existe* $\phi \in Aut(P \times Q)$ *tal que* $\phi(I) = J$*. De fato, basta observar que* $(1,2)$ *é menor que dois elementos de* $P \times Q$ $((2,2)$ *e* $(2,3))$ *enquanto* $(2,1)$ *só é menor que um, a saber,* $(2,2)$*.*



$P \times Q = ([2] \times [3], \preceq_\times)$

Capítulo 5

Considerações Finais

Neste capítulo apresentamos algumas possibilidades de continuação de estudos, a partir do que foi feito neste trabalho.

Para os códigos em espaços com a métrica de Hamming, existe a forma sistemática. Em [3] é apresentado uma forma canônica para os códigos em espaços com a métrica cadeia. No capítulo 3 deste trabalho generalizamos as duas representações apresentando uma maneira de representar os códigos poset hierárquico. Essa representação nos permitiu calcular facilmente alguns importantes parâmetros desta família de códigos. Com isso, nos parece que estudar formas de se representar outras famílias de códigos poset pode render bons frutos.

Considerando os códigos sobre anéis, a falta de invertibilidade dos elementos do espaço não nos permite realizar todas as operações que realizamos quando trabalhamos com códigos em espaços vetoriais definidos sobre corpos finitos. Por isso a transição de códigos sobre corpos finitos para códigos sobre anéis não é tão simples. Em [16] e [19] encontramos uma representações para códigos lineares sobre anéis, ambos os trabalhos consideram a métrica cadeia. Uma buscar por representações para mais famílias de códigos lineares sobre anéis pode apresentar resultados muito interessantes.

No capítulo 4 definimos a propriedade de extensão de ideais (propriedade-IE), que diz que um poset tem essa propriedade se, e somente se, todo isomorfismo entre seus ideais pode ser estendido para uma automorfismo do poset. Também definimos a propriedade $\tilde{I}$ que diz que as órbitas das isometrias lineares de $(\mathbb{F}_q^n, d_P)$ são determinadas por classes de equivalência, sob

isomorfismo de ideais, no conjunto dos ideais de P, em outras palavras, temos que existe uma isometria linear $T \in GL_P(n)$ tal que $T(x) = y$ se, e somente se, $\langle \text{supp}(x) \rangle \sim \langle \text{supp}(y) \rangle$. Em seguida, mostramos que essas propriedades são equivalentes e encontramos algumas famílias de poset que possuem estas propriedades, a saber, os hierárquicos, os NRT e os árvore com regular por nível. Seria interessante aumentar a lista de famílias que possuem essa propriedade.

Ainda no capítulo 4 definimos o *formato*, uma função que caracteriza as órbitas, sob as isometrias do espaço poset, porém, só conseguimos determinar essa função para algumas classes particulares de espaços poset. Determinamos a função formato para espaços hierárquicos, NRT e árvore com raiz, regular por nível. Uma busca por funções formato para outras famílias de espaços poset não deve ser negligenciada.

No final do capítulo 4 vimos que quando construímos posets a partir de operações sobre outros poset, alguns destes novos posets herdam a propriedade-IE de seus geradores, quando estes a possuem. Conseguimos mostrar que quando realizamos a soma ordinal sobre dois posets que possuem a propriedade-IE, esta propriedade herdada. No entanto, vimos que sob determinadas condições, os posets que surgem da soma direta e do produto ordinal herdam a propriedade-IE. Deve-se tentar determinar a existência de condições necessárias e suficientes para que esta propriedade seja herdada nessas operações.

A busca por mais operações que preservem esta propriedade pode levar a uma forma de decomposição, similar à decomposição de um número inteiro como produto de potências de números primos, dos posets em elementos primais que possuam a propriedade-IE.

Referências Bibliográficas

[1] A. Aho, J. Hopcroft, and J.Ullman. *The design and analysis of computer algorithms*. Addison-Wesley Publishing Co., Reading, MA, 1974.

[2] M. Alves, L. Panek, and M. Firer. Error-block codes and poset metrics. *Adv. Math.Commun*, 2:95–111, 2008.

[3] M. Alves, L. Panek, and M. Firer. Classification of Niederreiter-Rosenbloom-Tsfasman block codes. *IEEE Trans. on Inform. Theory*, 56(10):5207–5216, 2010.

[4] A. Barg and P. Purkayastha. Bounds on ordered codes and orthogonal arrays. *Moscow Math. J.*, 2:211–243, 2009.

[5] R. Brualdi, J. Graves, and K.M. Lawrence. Codes with a poset metric. *Discrete Mathematics*, 147:57–72, 1995.

[6] S. R. Buss. Alogtime algorithms for tree isomorphism, comparison, and canonization. In *Computational Logic and Proof Theory*, volume 1289 of *Lecture Notes in Computer Science*, pages 18–33. Springer Berlin Heidelberg, 1997.

[7] S. Choi, J. Hyun, D. Oh, and H. Kim. *Mac-Williams type equivalence relations. arXiv:1205:1090*, 2013.

[8] H. Domingues and G. Iezzi. *Álgebra Moderna*. Atual Editora, São Paulo, 1982.

[9] M. Firer, L. Panek, and L. Rifo. Coding in the presence of semantic value of information: Unequal error protection using poset decoders. *CoRR*, abs/1108.3832, 2011.

[10] G. H. Hardy. *"Ramanujan's Work on Partitions"and "Asymptotic Theory of Partitions.* AMS, New York: Chelsea, 1999.

[11] A. Hefez and M. Villela. *Códigos Corretores de Erros*. Série de Computação e Matemática. IMPA, Rio de Janeiro, 2002.

[12] W. C. Huffman and V. Pless. *Fundamentals of Error Correcting Codes*. Cambridge University Press, Cambridge, U.K., 2003.

[13] S. Jain. Bursts in m-metric array codes. *Linear Algebra and its Applications*, 418(1):130 – 141, 2006.

[14] H. JongYoon and K. Hyun Kwang. Maximum distance separable poset codes. *Designs, Codes and Cryptography*, 48(3):247–261, 2008.

[15] F. J. MacWilliams. A theorem on the distribution of weights in a systematic code. *The Bell System Technical Journal*, 42:79–94, 1963.

[16] O. Mehmet and S. Irfan. Linear codes over $\mathbb{F}_q[u]/(u^s)$ with respect to the rosenbloom-tsfasman metric. *Designs, Codes and Cryptography*, 38(1):17–29, 2006.

[17] H. Niederreiter. A combinatorial problem for vector spaces over finite fields. *Discrete Mathematics*, 96:221–228, 1991.

[18] H. Niederreiter. Orthogonal array and other combinatorial aspects in the theory of uniform point distributions in unit cubes. *Discrete Mathematics*, 106/107:361?367, 1992.

[19] M. Ozen and I. Siap. Codes over Galois rings with respect to the RosenbloomâTsfasman metric. *Journal of The Franklin Institute-engineering and Applied Mathematics*, 344:790–799, 2007.

[20] L. Panek, M. Firer, H. K. Kim, and J. Y. Hyun. Groups of linear isometries on poset structures. *Discrete Mathematics*, 308:4116–4123, 2008.

[21] W. Park and A. Barg. The ordered hamming metric and ordered symmetric channels. In *(ISIT), 2011 IEEE International Symposium on Information Theory Proceedings*, pages 2283–2287, July 2011.

[22] R. Read and C. Berge. The coding of various kinds of unlabeled trees. *Graph Theory and Computing*, 1:153–182, 1972.

[23] R. Roth. *Introduction to Coding Theory*. Cambridge University Press, 2006.

[24] H. Schmerl. Countable homogeneous partially ordered sets. *Algebra Universalis*, 9:315–328, 1979.

[25] R. Singleton. Maximum distance q-nary codes. *Information Theory, IEEE Transactions*, 10:116 – 118, 1964.

[26] R. P. Stanley. *Enumerative combinatorics*. Cambridge University Press, Cambridg, 2012.

[27] M. Rosembloom; M. A. Tsfasman. Codes for m-metric. *Problems of Information Transmission*, 33(1):45–52, 1997.

[28] V.K. Wei. Generalized Hamming weights for linear codes. *IEEE Trans. on Inform. Theory*, 37:1412–1418, 1991.

Índice Remissivo