

UNIVERSIDADE ESTADUAL DE CAMPINAS
IMECC - DEPARTAMENTO DE MATEMÁTICA

Dissertação de Mestrado

ESPAÇOS POSET E O PROBLEMA
DA DISTRIBUIÇÃO DE PESOS

Marcos Vinicius Pereira Spreafico

Orientador: Marcelo Firer

mvspreafico@gmail.com

Fevereiro de 2009

Espaços Poset e o problema da Distribuição de Pesos

Este exemplar corresponde à redação final da dissertação devidamente corrigida e defendida por Marcos Vinicius Pereira Spreafico e aprovada pela comissão julgadora.

Campinas, 26 de Fevereiro de 2009



Prof. Dr. Marcelo Firer
Orientador

Banca Examinadora:

- 1 Prof. Dr. Marcelo Firer
- 2 Prof. Dr. Emerson Luiz Do Monte Carmelo
- 3 Prof. Dr. Marcelo Muniz Silva Alves
- 4 Prof. Dr. José Plínio de Oliveira Santos

Dissertação apresentada ao Instituto de Matemática, Estatística e Computação Científica, UNICAMP, como requisito parcial para obtenção do Título de MESTRE em Matemática

**FICHA CATALOGRÁFICA ELABORADA PELA
BIBLIOTECA DO IMECC DA UNICAMP**

Bibliotecária: Maria Fabiana Bezerra Müller – CRB8 / 6162

Spreafico, Marcos Vinicius Pereira
Sp77e Espaços Poset e o problema da distribuição de pesos/Marcos Vinicius
Pereira Spreafico-- Campinas, [S.P. : s.n.], 2009.

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

1.Conjuntos ordenados. 2.Códigos de controle de erros (Teoria da
informação). 3. Métricas sobre ordens parciais. . I. Sobrenome, Nome
do Orientador. II. Universidade Estadual de Campinas. Instituto de
Matemática, Estatística e Computação Científica. III. Título.

(mfbm/imecc)

Título em inglês: Poset space and the weight distribution problem

Palavras-chave em inglês (Keywords): Ordered sets; Error-correcting codes (Information theory); Poset metric

Área de concentração: Matemática

Titulação: Mestrado em Matemática

Banca examinadora: Marcelo firer (orientador); Marcelo Muniz Silva Alves (UFPR); José Plínio Oliveira dos Santos (UNICAMP); Emerson Luiz do Monte Carmelo (UEM)

Data da defesa: 26/02/2009

Programa de Pós-Graduação: Matemática

Dissertação de Mestrado defendida em 26 de fevereiro de 2009 e aprovada

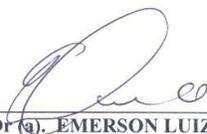
Pela Banca Examinadora composta pelos Profs. Drs.



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



Prof. (a). Dr (a). JOSÉ PLÍNIO DE OLIVEIRA SANTOS



Prof. (a). Dr (a). EMERSON LUIZ DO MONTE CARMELO



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

Agradecimentos

Primeiramente a Deus por tudo em minha vida. Aos meus pais, pelo carinho e apoio.

Ao meu orientador Prof. Dr. Marcelo Firer pelo apoio, paciência e orientação.

Ao CNPq pelo apoio financeiro.

Por fim, a todos meus colegas e professores do departamento de matemática do IMECC e meus professores de graduação do DMA - UEM que me incentivaram.

Sumário

Abstract	vi
Resumo	vii
Introdução	1
1 Conjuntos parcialmente ordenados	4
1.1 Conceitos básicos	4
1.2 Classes de ordens	7
1.3 Homomorfismo e isomorfismo de poset	10
2 Códigos lineares ponderados	13
2.1 Distância de Hamming e Isometrias	14
2.2 Códigos Poset	22
3 Distribuição de pesos	31
3.1 Distribuição de pesos de algumas classes de posets	31
3.2 Determinação da ordem via distribuição de pesos	37
3.3 Conjecturas (descartadas e mantidas)	49
3.3.1 Conjectura assumindo a hipótese de reconstrução	52

Abstract

In this work, we introduce the concept of poset codes (Brualdi - 1995) and in this context we study the weight distribution problem, presenting the necessary concepts of the partially ordered set and error correcting codes theory.

The weight distribution is the cardinality of metric-spheres in finite dimensional vector space over a finite field endowed with a poset metric. The weight distribution problem asks for conditions to ensure that the weight distribution determines the metric. In this work we show that the weight distribution of some families of posets, namely the classes of anti-chain, chain, crown and hierarchical posets, determines the metric. We also show that the weight distribution determines some known invariants of posets. Finally, we present some conjectures relating the weight distribution problem and the reconstruction problem of graphs.

Resumo

Neste trabalho fazemos uma apresentação dos espaços poset, introduzidos por Brualdi (1995), apresentamos os conceitos necessários da teoria de conjuntos parcialmente ordenados e da teoria de códigos.

Trabalhamos com uma questão de caráter amplo e estrutural deste contexto, o problema da determinação da ordem através da distribuição de pesos. A distribuição de pesos é essencialmente o conjunto das cardinalidades das esferas métricas e a pergunta que se coloca é em que medida este invariante determina a métrica em questão. Demonstramos que para as classes de códigos, cadeia, anticadeia, coroa e hierárquico, classes importantes no contexto da teoria de códigos, o problema possui uma resposta positiva e justificamos algumas conjecturas que relacionam este problema ao da reconstrução de grafos.

Introdução

Os cenários usuais da teoria dos códigos corretores de erros são os espaços vetoriais de dimensão finita sobre corpos finitos, \mathbb{F}_q^n , geralmente dotados de uma métrica conhecida como métrica de Hamming, utilizada para se calcular os invariantes e construir algoritmos de correção de erros.

Em 1995 Brualdi, Graves e Lawrence ([1]) introduzem em \mathbb{F}_q^n uma nova família de métricas, ponderadas por conjuntos parcialmente ordenados. Estas métricas generalizam a métrica de Hamming e, essencialmente, consideram que as coordenadas das n -uplas possuem pesos distintos ao se calcular a distância entre os elementos de \mathbb{F}_q^n .

A partir de então, surgem vários novos códigos perfeitos, códigos que com a métrica de Hamming não eram perfeitos assumindo determinada métrica passam a ser perfeitos, ver exemplo 2.2.5.

Neste contexto nos deparamos com uma questão estrutural de caráter amplo, *o problema da determinação da métrica através da distribuição de pesos*. A distribuição de pesos de um espaço poset (espaço vetorial finito munido com uma métrica ponderada) é simplesmente o conjunto das cardinalidades das esferas métricas, um invariante mais fraco que a métrica. Neste trabalho buscamos condições sobre a ordem que permitem garantir que a dis-

tribuição de pesos determine, a menos de isomorfismo, a métrica (e a ordem) em questão.

Nos dois primeiros capítulos é feito um apanhado geral de definições, resultados e exemplos já conhecidos na literatura enquanto que o terceiro capítulo é composto de resultados originais, salvo menção em contrário.

No primeiro capítulo introduziremos os conceitos básicos sobre a teoria de conjuntos parcialmente ordenados (poset), algumas formas de representar um poset, apresentaremos as famílias de poset mais trabalhadas no contexto de códigos corretores de erros, a saber, anticadeia, cadeia, coroa e hierárquico, ilustrando cada nova definição com exemplos sempre que possível.

No segundo capítulo apresentaremos as definições básicas necessárias para o desenvolvimento deste trabalho no contexto de códigos corretores de erros. Inicialmente, falaremos sobre códigos lineares mostrando algumas propriedades que nos servirão para fazermos um paralelo com os códigos com a métrica ponderada por uma ordem parcial. Encerraremos este capítulo apresentando um problema que até o momento permanece em aberto e trabalha com questões estruturais, a saber, *o problema da extensão de isometrias*, um problema bastante complexo com o qual começamos a lidar e onde surgiu o problema central deste trabalho, o problema da distribuição de pesos.

No terceiro capítulo introduzimos, com todos os detalhes, o problema da determinação da ordem através da distribuição de pesos. Inicialmente, procuramos obter as distribuições de pesos dos espaços posets mais usuais da bibliografia. Logo em seguida, na seção 3.2 começamos por apresentar um contra-exemplo para o caso geral e a partir de então, procurando condições para que o problema tenha uma resposta positiva, restringimos o problema

sobre algumas classes de posets afim de termos condições suficientes para que a problema tenha uma resposta afirmativa.

Por fim, na última seção, abordamos e justificamos algumas conjecturas, que surgiram durante pesquisas feitas ao longo deste trabalho, para trabalhos futuros e apresentamos um resultado, interessante por si próprio, que surgiu originalmente para descartar uma conjectura prévia.

Capítulo 1

Conjuntos parcialmente ordenados

1.1 Conceitos básicos

Seja P um conjunto não vazio. Uma relação de ordem parcial \preceq é uma relação reflexiva, anti-simétrica e transitiva, ou seja, dados a, b e c em P , $a \preceq a$, se $a \preceq b$ e $b \preceq a$ então $a = b$ e se $a \preceq b$ e $b \preceq c$ então $a \preceq c$. O par (P, \preceq) será chamado *conjunto parcialmente ordenado (poset)* e denotado simplesmente por P . Quando estivermos utilizando mais de uma relação de ordem usaremos a notação \preceq_P , afim de distinguir as relações em questão, para indicar que a relação está definida no poset P .

Dois pontos $a, b \in P$ são ditos *comparáveis* se $a \preceq b$ ou $b \preceq a$, caso contrário são ditos *não comparáveis*. Diremos que b *cobre* a se $a \preceq b$ e não existe $c \neq a$ e $c \neq b$ em P tal que $a \preceq c$ e $c \preceq b$. Por exemplo, considerando a ordem natural sobre $\{1, 2, 3\}$, temos que 3 cobre 2, 2 cobre 1 mas 3 não

cobre 1.

Um poset P é chamado *cadeia* ou *linear* se qualquer dois elementos de P são comparáveis. Por outro lado, se quaisquer dois pontos distintos de P são não comparáveis então o poset é chamado de *anticadeia*. Um exemplo de cadeia é o conjunto dos números naturais munido com a relação de "menor do que" ($\mathbb{N}, <$). Se X tem cardinalidade finita n , então uma cadeia (X, \prec_X) é denotada simplesmente por C_n .

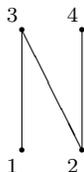
Alguns exemplos:

- Considere $\wp(X)$ a família de todos subconjuntos de um dado conjunto X , e defina $A \preceq B$ se A está contido em B , onde $A, B \in \wp(X)$. Então $(\wp(X), \preceq)$ é um poset.
- Dado $X \subset \mathbb{N}$ e $a \preceq b$ se a divide b , onde $a, b \in X$. Então (X, \preceq) é um poset.

Afim de facilitar a compreensão dos posets introduziremos alguns conceitos que nos serão úteis mais adiante.

Definimos o *diagrama de Hasse* de um poset P da seguinte maneira: os elementos de P serão representados por pontos, e se x cobre y o ponto x será situado acima do ponto y com uma aresta ligando os dois pontos.

Exemplos 1.1.1. Se N é o poset definido por $N := (\{1, 2, 3, 4\}, 1 \preceq 3, 2 \preceq 3 \text{ e } 2 \preceq 4)$ o diagrama de Hasse de N será:



Dados (P, \preceq) um poset e $S \subset P$ um subconjunto de P . Diremos que (S, \preceq) é um *subposet* de P se considerarmos em S a ordem induzida da restrição da ordem de P . Assim, dizemos que $S \subset P$ é uma cadeia de P se o subposet (S, \preceq_P) for uma cadeia.

Dizemos que $I \subseteq P$, não vazio, é um *ideal* de P se, dado $y \in I$ e $x \preceq y$ em P , então $x \in I$. Dado um conjunto $A \subset P$, denotaremos o menor ideal de P (com respeito a ordem \subseteq) contendo A por $\langle A \rangle$. Um ideal $I \subset P$ é dito *principal* se existe $j \in I$ tal que $I = \langle j \rangle$.

Dado poset (P, \preceq) e $j \in P$, o *posto* $p(j, P)$ de um elemento $j \in P$ (denotado simplesmente por $p(j)$ quando não houver ambiguidades), é o comprimento da maior cadeia de P que tem x como elemento máximo, ou seja,

$$p(x) = \text{máx}\{|C|; C \subset \langle x \rangle \text{ e } C \text{ é cadeia}\}.$$

A *altura* $h(P)$ do poset P é o posto maximal de seus elementos.

O i -ésimo nível de P , denotado por N_i^P , é o subconjunto de P contendo todos elementos de posto i em P , isto é, $N_i^P := \{j \in P; p(j, P) = i\}$. A *estrutura-nível* de P é a sequência, em ordem crescente de nível, das cardinalidades de cada nível:

$$N(P) := (|N_1^P|, |N_2^P|, \dots, |N_{h(P)}^P|).$$

No exemplo acima 1.1.1, é fácil ver que, $h(P) = 2$ e P possui apenas 2 níveis tais que, $N_1(P) = \{1, 2\}$, $N_2(P) = \{3, 4\}$, logo, a estrutura-nível de P é $N(P) = (2, 2)$.

Um nível N_i^P qualquer pode ser particionado em subconjuntos disjuntos a partir da análise da cardinalidade dos ideais principais gerados por um

elemento de N_i^P . Dessa forma, definimos $N_{i,j}^P$ o subconjunto de N_i^P formado pelos elementos que geram um ideal de cardinalidade j , isto é, $N_{i,j}^P := \{k \in N_i^P : |\langle k \rangle| = j\}$. É claro que, $N_{i,j}^P = \emptyset$ se $j < i$. Podemos assim expressar P como a união disjunta $P = \bigcup_{j=i}^n \bigcup_{i=1}^n N_{i,j}^P$.

Além do diagrama de Hasse, outra maneira de representarmos um poset é através de sua matriz de adjacência. Dado um poset P sobre $[n]$, sua *matriz de adjacência* é a matriz quadrada de $n \times n$, $M(P) = (a_{ij})_{n \times n}$, definida por

$$a_{ij} = \begin{cases} 1 & \text{se } i \preceq j \text{ e } i \neq j \\ 0 & \text{caso contrário.} \end{cases}$$

Voltando agora no exemplo 1.1.1, a matriz de adjacência do poset N é:

$$M(N) = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

1.2 Classes de ordens

Recordamos e apresentamos a seguir algumas famílias de posets que acompanharão todo o desenvolvimento deste trabalho. Estas famílias são aquelas mais estudadas no contexto de códigos corretores de erros que será discutida no próximo capítulo.

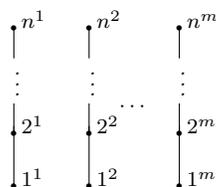
Exemplos 1.2.1 (Anticadeia). *A anticadeia, já apresentada anteriormente será denotada por H e seu diagrama de Hasse é:*

$$\begin{array}{cccc} \bullet & \bullet & \cdots & \bullet \\ 1 & 2 & & n \end{array}$$

Exemplos 1.2.2 (Cadeia). *O poset cadeia como já definido anteriormente será denotado por \mathcal{C} e sua representação em diagrama de Hasse é:*



Exemplos 1.2.3 (Rosenbloom-Tsfasman). *A união finita e disjunta de cadeias de mesmo comprimento que chamaremos de ordem de Rosenbloom-Tsfasman e denotaremos por \mathcal{RT} .*



Exemplos 1.2.4 (Coroa). *Seja \mathcal{CR} o poset sobre $[2m]$, definido da seguinte maneira $1 \prec_{\mathcal{CR}} m+1$, $1 \prec_{\mathcal{CR}} 2m$, $i \prec_{\mathcal{CR}} m+i$ e $i \prec_{\mathcal{CR}} m+i-1$, para todo $i = 2, 3, \dots, m$. Este poset é chamado coroa e seu diagrama de Hasse é mostrado abaixo,*

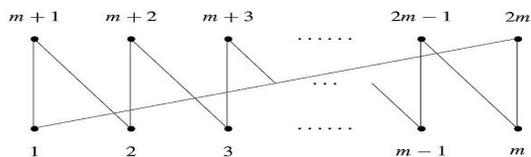


Figura 1.1: diagrama de Hasse do poset coroa

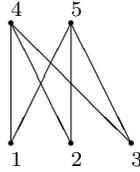
Antes de apresentarmos o próximo exemplo, precisamos introduzir o conceito de soma ordinária entre posets.

Dados dois posets P e Q , a *soma ordinária* de P e Q é o poset $P \oplus Q$ tal que

$$x \preceq_{P \oplus Q} y \Leftrightarrow \begin{cases} x \preceq_P y & \text{se } x, y \in P \\ x \preceq_Q y & \text{se } x, y \in Q \\ x \in P \text{ e } y \in Q \end{cases}$$

ou seja, além das relações advindas de P e de Q , todos elementos de Q são maiores que todos elementos de P na soma $P \oplus Q$.

Por exemplo, se $H^1 = \{1, 2, 3\}$ é uma anticadeia de cardinalidade 3 e $H^2 = \{4, 5\}$ é uma anticadeia de cardinalidade 2 então o diagrama de Hasse de $H^1 \oplus H^2$ é



Note que a soma ordinária não é comutativa, isto é, $P \oplus Q \neq Q \oplus P$, em geral.

Exemplos 1.2.5 (Hierárquico). *Seja \mathcal{H} o poset sobre $[n]$ definido da seguinte maneira, dados n, n_1, n_2, \dots, n_t inteiros positivos tais que $n_1 + n_2 + \dots + n_t = n$, então definimos*

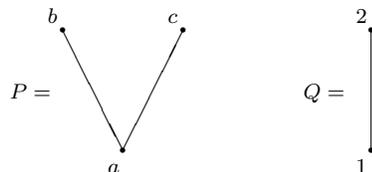
$$\mathcal{H} = H^1 \oplus H^2 \oplus \dots \oplus H^t$$

a soma ordinária de t anticadeias H^j onde $|H^j| = n_j$ para $j = 1, 2, \dots, t$. Esse poset é chamado Hierárquico.

Note que as classes de posets apresentadas acima não são classes disjuntas. As classes de posets hierárquico e a classe Rosenbloom-Tsfasman se intersectam nas classes anticadeia e cadeia que por sua vez também se intersectam quando $n = 1$, observe ainda que quando $n = 4$ o poset hierárquico coincide com o coroa.

1.3 Homomorfismo e isomorfismo de poset

Dados P e Q dois posets, dizemos que uma aplicação $f : (P, \preceq_P) \rightarrow (Q, \preceq_Q)$ é um *homomorfismo de ordem* se dados $x, y \in P$, se $x \preceq_P y$ então $f(x) \preceq_Q f(y)$. Por exemplo, se $P = \{a, b, c\}$ e $Q = \{1, 2\}$ com diagramas de Hasse



então a função definida por $f(a) = 1, f(b) = 2$ e $f(c) = 2$ é um homomorfismo de ordem entre P e Q .

A próxima proposição segue naturalmente das definições.

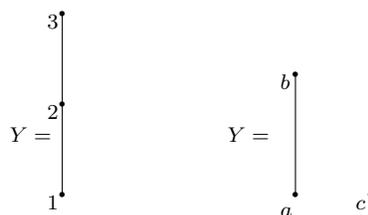
Proposição 1.3.1. *Dado $S \subseteq P$, seja \preceq_S uma ordem em S . Temos que (S, \preceq_S) é um subposet do poset (P, \preceq_P) se, e somente se, a aplicação inclusão $i : S \rightarrow P$ é um homomorfismo de ordem.*

Proposição 1.3.2. *A imagem $f(\mathcal{C}_n)$ de uma cadeia \mathcal{C}_n por um homomorfismo de ordem f é também uma cadeia.*

Demonstração: Dada $f : \mathcal{C}_n \rightarrow P$ um homomorfismo de ordem. Dados $a, b \in f(\mathcal{C}_n)$, existem $x, y \in \mathcal{C}_n$ tais que $f(x) = a$ e $f(y) = b$. Como \mathcal{C}_n é cadeia temos que $x \preceq_{\mathcal{C}_n} y$ ou $y \preceq_{\mathcal{C}_n} x$ e como f preserva ordem, para o primeiro caso teremos $a \preceq_{f(\mathcal{C}_n)} b$ enquanto que no segundo caso $b \preceq_{f(\mathcal{C}_n)} a$, ou seja, os elementos $a, b \in f(\mathcal{C}_n)$ são comparáveis e portanto $f(\mathcal{C}_n)$ é uma cadeia. \square

Como consequência direta da definição, qualquer função que possui uma anticadeia como domínio é um homomorfismo de ordem.

Considere agora $X = \{a, b, c\}$ e $Y = \{1, 2, 3\}$ dois posets com diagramas de Hasse



então $g : X \rightarrow Y$ tal que $g(a) = 1, g(b) = 3$ e $g(c) = 2$ é um homomorfismo de ordem entre X e Y . Desde que essa função é uma bijeção, a inversa g^{-1} de g existe mas a aplicação g^{-1} não preserva ordem, pois $1 \prec_Y 2$ e $g^{-1}(1) = a \not\prec_X c = g^{-1}(2)$. A partir desse exemplo, chegamos na idéia para a definição de o que é um isomorfismo entre dois posets.

Sejam (X, \prec_X) e (Y, \prec_Y) dois posets e $f : (X, \prec_X) \rightarrow (Y, \prec_Y)$ um homomorfismo de ordem. Caso a inversa de f exista e também seja um homomorfismo então dizemos que f é um *isomorfismo* entre (X, \prec_X) e (Y, \prec_Y) . Neste caso, ainda dizemos que (X, \prec_X) e (Y, \prec_Y) são isomorfos e denotamos por $X \approx Y$.

Algumas propriedades elementares:

1. A aplicação identidade é um isomorfismo de poset;
2. Se $f : X \rightarrow Y$ e $g : Y \rightarrow Z$ são isomorfismos, então a aplicação $g \circ f$ é um isomorfismo entre X e Z ;
3. Se f é um isomorfismo então, f^{-1} também é um isomorfismo de poset.

Segue das propriedades acima que isomorfismo entre posets define uma relação de equivalência no conjunto dos posets.

A seguir fornecemos uma caracterização de isomorfismos que segue diretamente da definição.

Considere $f : (X, \prec_X) \rightarrow (Y, \prec_Y)$ uma aplicação bijetora entre os posets X e Y . Então f é um isomorfismo se, e somente se, para quaisquer $x, y \in X$,

$$x \prec_X y \quad \text{se e somente se} \quad f(x) \prec_Y f(y).$$

Capítulo 2

Códigos lineares ponderados

A história dos Códigos Corretores de Erros começa em 1948 com a publicação do trabalho de Claude E. Shannon, ([12]). Inicialmente uns dos maiores interessados nesta teoria foram os matemáticos que a desenvolveram consideravelmente nas décadas de 50 e de 60. A partir da década de 70, com as pesquisas espaciais e a grande popularização dos computadores, essa teoria começou a interessar também aos engenheiros. Para maiores detalhes sobre Shannon e a história dos códigos corretores de erros veja IEEE Information Theory Society em <http://www.itsoc.org/shannon.html>

Neste capítulo apresentaremos uma introdução à teoria dos códigos corretores de erros ponderados por ordens parciais. Iniciaremos com conceitos básicos de códigos, somente os necessários para nossos objetivos, e depois faremos um paralelo com códigos posets, afim de podermos examinar quais estruturas são mantidas quando passamos de um espaço com a métrica de Hamming a um espaço com a métrica poset. Exploraremos os exemplos mais clássicos de códigos posets, a saber, anticadeia (ou Hamming), cadeia

(ou linear), coroa, hierárquico e RosenbloomTsfasman.

2.1 Distância de Hamming e Isometrias

Seja A um conjunto de cardinalidade finita q , e considere A^n o conjunto das n -uplas com entradas em A . A métrica mais usada neste contexto é aquela estabelecida pela distância de Hamming $d_H(x, y)$, definida como o número de coordenadas distintas de x e y , ou seja, se $x = (x_1, x_2, \dots, x_n), y = (y_1, y_2, \dots, y_n) \in A^n$ então

$$d_H(x, y) = |\{i : x_i \neq y_i, 1 \leq i \leq n\}|$$

A distância de Hamming define de fato uma métrica:

Proposição 2.1.1. *Dados $x, y, z \in A^n$, então:*

1. **Positividade:** $d_H(x, y) \geq 0$ com a igualdade valendo se, e só se, $x = y$,
2. **Simetria:** $d_H(x, y) = d_H(y, x)$,
3. **Desigualdade triangular:** $d_H(x, z) \leq d_H(x, y) + d_H(y, z)$.

Demonstração:

A primeira e a segunda propriedade são óbvias. Trataremos então de demonstrar apenas a terceira. Com efeito, se $x_i = z_i$ as i -ésimas coordenadas não contribuem para $d_H(x, z)$ e se $x_i \neq z_i$ a contribuição das i -ésimas coordenadas para $d_H(x, z)$ é um.

No caso em que a contribuição é zero, certamente a contribuição das i -ésimas coordenadas a $d_H(x, z)$ é menor ou igual à das i -ésimas coordenadas de $d_H(x, y) + d_H(y, z)$.

No outro caso em que a contribuição é 1, temos que $x_i \neq z_i$ e assim não podemos ter $x_i = y_i$ e $y_i = z_i$. Consequentemente, a contribuição das i -ésimas coordenadas a $d_H(x, y) + d_H(y, z)$ é maior ou igual a 1, que é a contribuição das i -ésimas coordenadas de $d_H(x, z)$. \square

Como em todo espaço métrico, podemos definir em (A^n, d_H) bolas e esferas. Dados $x \in A^n$ e $r \in \mathbb{N}$, definimos a *bola* e a *esfera de Hamming de centro em x e raio r* como sendo respectivamente os conjuntos

$$\begin{aligned} B(x, r) &= \{y \in A^n : d_H(x, y) \leq r\} \\ S(x, r) &= \{y \in A^n : d_H(x, y) = r\}. \end{aligned}$$

Proposição 2.1.2. *Dados $x \in A^n$ e $r \in \mathbb{N}$ a cardinalidade da bola de Hamming de centro em x e raio r é dada por:*

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

Demonstração: Note primeiramente que $|S(x, r)| = |S(0, r)|$ qualquer que seja $x \in \mathbb{F}_q^n$, isto é, a cardinalidade de esferas de Hamming independe da escolha do centro. Com efeito, se $y \in S(0, r)$ então $y + x \in S(x, r)$ pois $d_H(0, y) = d_H(x, y + x)$. Logo, $|S(x, r)| \leq |S(0, r)|$ e como $d_H(0, y) = d_H(x - x, y - x) = d_H(x, y)$ segue que, se $y \in S(x, r)$ então $y - x \in S(0, r)$ e assim $|S(0, r)| \leq |S(x, r)|$, donde obtemos a igualdade. Mostraremos agora que $|S(0, r)| = \binom{n}{r} (q-1)^r$, e com isso obtemos que qualquer esfera de raio r tem

essa cardinalidade. Tome $y = (y_1, \dots, y_n) \in S(0, r)$ assim, y tem exatamente r coordenadas não nulas e como essas r coordenadas podem ocorrer em n posições então existem $\binom{n}{r}$ possibilidades para as coordenadas não nulas. E como cada coordenada $y_i \in \mathbb{F}_q^n$ não nula pode assumir $(q - 1)$ valores em \mathbb{F}_q então existem $\binom{n}{r}(q - 1)^r$ elementos em \mathbb{F}_q^n que dista r da origem.

A proposição segue do fato que a bola é a união disjunta de esferas, isto é, $B(x, r) = \bigcup_{t=0}^r S(x, t)$, onde $S(x, i) \cap S(x, j) = \emptyset$ para $i \neq j$. \square

Note que a cardinalidade de esferas e bolas de Hamming independe da escolha do centro, depende apenas do raio escolhido.

Chamamos de *código* a qualquer subconjunto de $C \subset A^n$.

Definição 2.1.3. *Seja C um código em A^n , definimos a distância mínima $d(C)$ de C por:*

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

Proposição 2.1.4. *Considere C um código com distância mínima d e $r = \lfloor \frac{d-1}{2} \rfloor$. Lembramos que $\lfloor t \rfloor$ é o maior inteiro menor ou igual a t . Então,*

$$B(x, r) \cap B(y, r) = \emptyset$$

para quaisquer $x \neq y \in C$.

Demonstração: Suponhamos que exista w em A^n tal que $w \in B(x, r) \cap B(y, r)$. Dessa forma, $d_H(x, w) \leq r$ e $d_H(w, y) \leq r$ e da desigualdade triangular segue que $d_H(x, y) \leq d_H(x, w) + d_H(w, y) \leq d - 1$, o que é um absurdo já que a distância mínima de C é d e $x, y \in C$. Portanto a interseção das bolas acima é vazia. \square

Definição 2.1.5. *Seja $C \subset A^n$ um código com distância mínima d e $r = \lfloor \frac{d-1}{2} \rfloor$. Se*

$$\bigcup_{x \in C} B(x, r) = A^n$$

então dizemos que C é um código perfeito.

Sempre que se define uma classe de objetos matemáticos, como por exemplo o dos códigos de comprimento n sobre um conjunto com q elementos, costuma-se definir também a noção de equivalência entre elementos deste conjunto. A noção de equivalência de códigos repousa sobre o conceito de isometrias, que passamos a tratar abaixo.

Definição 2.1.6. *Seja A um conjunto finito e n um número natural. Diremos que uma função $f : A^n \rightarrow A^n$ é uma **isometria** de A^n (de Hamming) se ela preserva a métrica de Hamming, ou seja, se*

$$d(f(x), f(y)) = d_H(x, y) \quad \forall x, y \in A^n$$

As isometrias de Hamming possuem propriedades notáveis, que já foram totalmente classificadas, entretanto, pela simplicidade dos argumentos utilizados vamos descrever tais propriedades com intuito de mais adiante podermos compará-las com as isometrias de um código poset.

Proposição 2.1.7. *Toda isometria $f : A^n \rightarrow A^n$ é uma bijeção de A^n .*

Demonstração: Uma isometria de espaços métricos é sempre injetora. Como A^n é finito, esta deve ser bijetora. \square

Assim como para qualquer espaço métrico, temos que o conjunto das isometrias é um grupo com a operação usual de composição, ou seja:

Proposição 2.1.8. *Sejam $f, g : A^n \rightarrow A^n$ isometrias. Então valem as seguintes propriedades:*

1. *A função identidade de A^n é uma isometria;*
2. *f^{-1} é uma isometria de A^n ;*
3. *A composta $g \circ f$ é uma isometria de A^n .*

Definição 2.1.9. *Dizemos que dois códigos $C \subset A^n$ e $C' \subset A^n$ são equivalentes se existe uma isometria $f : A^n \rightarrow A^n$ tal que $f(C) = C'$.*

Segue então da proposição anterior que a relação de equivalência entre códigos é uma relação de equivalência, ou seja, reflexiva, simétrica e transitiva. De fato, sendo a função identidade uma isometria de A^n segue que todo código é equivalente a si mesmo. Se C é equivalente a C' então existe uma isometria para A^n tal que $f(C) = C'$ e então do segundo item da proposição f^{-1} é uma isometria de A^n tal que $f^{-1}(C') = C$ e assim C' é equivalente a C . Finalmente, se C é equivalente a C' e C' é equivalente a C'' então existem f e g isometrias de A^n tais que $f(C) = C'$ e $g(C') = C''$ assim pelo terceiro item da proposição anterior $(g \circ f)$ é uma isometria de A^n e é tal que $(g \circ f)(C) = C''$ tornando assim C equivalente a C'' . Como queríamos demonstrar.

Os exemplos a seguir nos fornecem duas maneiras de se obter um código equivalente a partir de outro.

- Se $f : A \rightarrow A$ é uma bijeção, e i é um número inteiro tal que $1 \leq i \leq n$, a aplicação $T_{f^i} : A^n \rightarrow A^n$ tal que $(x_1, \dots, x_i, \dots, x_n) \mapsto (x_1, \dots, f(x_i), \dots, x_n)$ é uma isometria.

- Se π é uma permutação de $\{1, 2, \dots, n\}$, a aplicação permutação de coordenadas

$$T_\pi : A^n \rightarrow A^n(x_1, \dots, x_n) \mapsto (x_{\pi(1)}, \dots, x_{\pi(n)})$$

é uma isometria.

Teorema 2.1.10. *Seja $F : A^n \rightarrow A^n$ uma isometria de A^n então existem uma permutação π de $\{1, 2, \dots, n\}$ e bijeções f_i de A , $i = 1, \dots, n$, tais que*

$$F = T_\pi \circ T_{f_1^{-1}} \circ \dots \circ T_{f_n^{-1}}.$$

Não demonstraremos esse teorema aqui, pois isso foge dos nossos objetivos. Mas tal demonstração não é difícil e pode ser encontrada em [10].

Decorre do teorema acima que dois códigos de comprimento n com entradas em um conjunto A são equivalentes se um puder ser obtido do outro mediante uma sequência de operações do tipo:

- (i) Substituição dos símbolos numa dada posição fixa em todas as palavras do código por meio de uma bijeção de A .
- (ii) Permutação das posições dos símbolos em todas as palavras do código mediante uma permutação fixa de $\{1, 2, \dots, n\}$.

Usualmente, nos textos sobre códigos, a definição de códigos equivalentes é apresentada dessa forma.

É possível (e necessário, se quisermos algum resultado que transcenda as questões de contagem) enriquecer C através de diversas estruturas, a mais simples e mais importante de todas é a de espaço vetorial. Seja \mathbb{F}_q um corpo de cardinalidade q e considere o espaço vetorial \mathbb{F}_q^n das n -uplas com entradas no corpo \mathbb{F}_q . Dizemos que $C \subset \mathbb{F}_q^n$ é um *código linear* de comprimento n sobre \mathbb{F}_q se C for um subespaço vetorial de \mathbb{F}_q^n .

Definição 2.1.11. Dado $x \in \mathbb{F}_q^n$ definimos o **peso** de x por:

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

É facilmente observado que o peso de um elemento x é dado por $\omega(x) = d_H(x, 0)$, e por tal motivo chamamos a função peso de *peso de Hamming*. Dado um código linear C , definimos o peso de C como o menor dos pesos dos elementos não nulos de C , isto é, $\omega(C) = \min\{\omega(x) : x \in C \setminus \{0\}\}$.

Proposição 2.1.12. Seja C um código linear de comprimento n e d a distância mínima de C . Valem as propriedades:

1. $\forall x, y \in C, d(x, y) = \omega(x - y)$.
2. $d = \omega(C)$

Demonstração: Dados $x, y \in C$ então $\omega(x - y) = d_H(x - y, 0) = d_H(x - y + y, y) = d_H(x, y)$ mostrando assim o primeiro item. Para o segundo item, basta notar que para todos elementos $x, y \in C$ com $x \neq y, x - y = z \in C \setminus \{0\}$ e que $d_H(x, y) = \omega(z)$. \square

Definição 2.1.13. Dizemos que $T : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$ é uma isometria linear para a métrica de Hamming se T é um operador linear de \mathbb{F}_q^n tal que

$$d_H(T(x), T(y)) = d_H(x, y) \quad \forall x, y \in \mathbb{F}_q^n.$$

Equivalentemente, temos que um operador linear T de \mathbb{F}_q^n é uma isometria linear se T preserva o peso de Hamming, isto é,

$$\omega(T(x)) = \omega(x) \quad \forall x \in \mathbb{F}_q^n.$$

É possível simplificar as buscas verificando ao invés de todo $x \in \mathbb{F}_q^n$ apenas para os elementos de uma base qualquer de \mathbb{F}_q^n .

Um operador linear T definido em \mathbb{F}_q^n sendo uma isometria linear é uma bijeção de \mathbb{F}_q^n em si mesmo, segue daí que T possui inversa, mais ainda, o operador inverso T^{-1} é também uma isometria linear. Dessa forma, o conjunto de todas as isometrias lineares de (\mathbb{F}_q^n, d_H) é um grupo. Denotaremos o grupo das isometrias lineares de (\mathbb{F}_q^n, d_H) por $GL_H(\mathbb{F}_q^n)$.

Analogamente, podemos definir uma equivalência entre códigos lineares, como segue:

Definição 2.1.14. *Dois códigos lineares C e C' contidos em \mathbb{F}_q^n são linearmente equivalentes se existir uma isometria linear $T : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$ tal que $T(C) = C'$.*

Explicitaremos agora, assim como feito para códigos equivalentes, como são as classes de equivalência do conjunto dos códigos lineares de comprimento n .

Se π é uma permutação de $\{1, \dots, n\}$ e $x = (x_1, \dots, x_n) \in \mathbb{F}_q^n$ então a aplicação T_π , definida por $T(x) = (x_{\pi(1)}, \dots, x_{\pi(n)})$, é linear. Temos também que, se $f_i : \mathbb{F}_q \rightarrow \mathbb{F}_q$, $i = 1, \dots, n$ são bijeções, então $T_\pi \circ T_{f_1} \circ \dots \circ T_{f_n}$ é linear se, e só se, cada f_i é linear. Sabemos também que $f : \mathbb{F}_q \rightarrow \mathbb{F}_q$ é linear se, e somente se, existe um elemento $c \in \mathbb{F}_q$ tal que $f(x) = cx$, $\forall x \in \mathbb{F}_q$ e tal função é bijetora se e só se $c \neq 0$. Dessa forma, segue do teorema 2.1.10 que dois códigos lineares C e C' em \mathbb{F}_q^n são linearmente equivalentes se, e só se, existem uma permutação de $\{1, 2, \dots, n\}$ e elementos $c_1, c_2, \dots, c_n \in \mathbb{F}_q \setminus \{0\}$ tais que

$$C' = \{(c_1 x_{\pi(1)}, \dots, c_n x_{\pi(n)}) : (x_1, \dots, x_n) \in C\}.$$

A teoria de códigos lineares repousa sobre os espaços vetoriais de dimensão finita sobre corpos finitos. Uma das questões desta teoria (e um dos mais importantes) é encontrar um código linear de comprimento n e de dimensão k sobre \mathbb{F}_q , com a maior distância mínima possível. Existem muitas métricas que podem ser definidas sobre \mathbb{F}_q^n , as mais comuns são a de Hamming e a métrica de Lee* (ver <http://www.ime.unicamp.br/~mfirer/3NotasFoz2006.pdf>).

2.2 Códigos Poset

Para nossos objetivos é suficiente que trabalhem apenas com posets finitos. Dessa forma, podemos assumir $P = [n] := \{1, 2, \dots, n\}$.

Consideremos o espaço vetorial \mathbb{F}_q^n das n -uplas com coeficientes no corpo \mathbb{F}_q e um poset P sobre $[n]$, identificando o conjunto dos índices das n -uplas com P . Usando o conceito de ideais de P podemos induzir uma métrica em \mathbb{F}_q^n da seguinte maneira: Dado $x = (x_1, \dots, x_n) \in \mathbb{F}_q^n$, definimos o *suporte* de x , como sendo o conjunto dos índices das coordenadas de x não nulas, ou seja,

$$\text{supp}(x) = \{i \in [n] : x_i \neq 0\}.$$

Definimos o P -*peso* de x como sendo a cardinalidade do menor ideal de P gerado pelo suporte de x :

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

Usando a função P -peso definimos a P -distância em \mathbb{F}_q^n de modo análogo a propriedade estabelecida anteriormente entre distância e peso de Hamming, mais precisamente:

Definição 2.2.1. Dada uma ordem P sobre $[n]$ e $x, y \in \mathbb{F}_q^n$ definimos a **P -distância** entre x e y por:

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

Os exemplos a seguir ilustram e ajudam a esclarecer essa definição.

- Considere $n = 4$ e $q = 2$ e considere $P = C_4$ o poset cadeia de cardinalidade 4 onde $1 \prec_{C_4} 2 \prec_{C_4} 3 \prec_{C_4} 4$. Dessa forma,
 $d_{C_4}((1, 1, 0, 0), (1, 0, 1, 0)) = 3$ pois, $\omega_{C_4}(0, 1, 1, 0) = |\langle \text{supp}(0, 1, 1, 0) \rangle| = |\langle \{2, 3\} \rangle| = |\{1, 2, 3\}| = 3$
- Se $n = 4$, $q = 2$ e $N = \{1, 2, 3, 4\}$ tal que $1 \prec_N 3, 2 \prec_N 3$ e $2 \prec_N 4$ então
 $d_N((1, 1, 0, 0), (1, 0, 0, 1)) = 2$ pois, $\omega_N(0, 1, 0, 1) = |\langle \text{supp}(0, 1, 0, 1) \rangle| = |\langle \{2, 4\} \rangle| = |\{2, 4\}| = 2$.

Note que, considerando P uma anticadeia, então o P -peso e a P -métrica coincidem com o peso de Hamming e a métrica de Hamming, respectivamente. De fato, basta observar em uma anticadeia P que todo subconjunto de P é um ideal, dessa forma, $\omega_P(x) = |\langle \text{supp}(x) \rangle| = |\text{supp}(x)| = \omega(x)$.

Se P é a união disjunta de cadeias de mesmo comprimento então ω_P e d_P coincidem respectivamente com o peso e a métrica de Rosenbloom-Tsfasman, introduzidas originalmente em [5].

Proposição 2.2.2. [1] Se P é um poset de cardinalidade n , então a P -distância $d_P(\cdot, \cdot)$ é uma métrica em \mathbb{F}_q^n .

Demonstração: É claro que a P -distância é positiva e também simétrica pois $\text{supp}(x - y) = \text{supp}(y - x)$. Sendo assim resta mostrar que d_P satisfaz a desigualdade triangular. Dados $x, y, z \in \mathbb{F}_q^n$ temos que $d_P(x, z) =$

$\omega_P(x - z) = \omega_P(x - y + y - z)$. Escrevendo $u = x - y$ e $v = y - z$ devemos mostrar que $\omega_P(u + v) \leq \omega_P(u) + \omega_P(v)$. Para tanto, note que $\text{supp}(u + v) \subseteq \text{supp}(u) \cup \text{supp}(v)$ e a união de dois ideais é também um ideal, assim

$$\begin{aligned}
\omega_P(u + v) &= |\langle \text{supp}(u + v) \rangle| \\
&\leq |\langle \text{supp}(u) \rangle \cup \langle \text{supp}(v) \rangle| \\
&\leq |\langle \text{supp}(u) \rangle| + |\langle \text{supp}(v) \rangle| \\
&= \omega_P(u) + \omega_P(v)
\end{aligned}$$

□

Chamaremos ω_P e d_P respectivamente de P -peso e P -métrica, respectivamente e chamando ambos $(\mathbb{F}_q^n, \omega_P)$ e (\mathbb{F}_q^n, d_P) de P -espaço. Definimos em (\mathbb{F}_q^n, d_P) as P -bolas e P -esferas de modo análogo ao feito anteriormente para a bola e esfera no espaço com a métrica de Hamming, ou seja,

$$\begin{aligned}
B_P(x, r) &= \{y \in A^n : d_P(x, y) \leq r\} \\
S_P(x, r) &= \{y \in A^n : d_P(x, y) = r\}.
\end{aligned}$$

Proposição 2.2.3. *A cardinalidade de uma esfera de raio i e centro na origem é dada por:*

$$|S_P(0, i)| = \sum_{j=1}^i (q-1)^j q^{(i-j)} \Omega_j(i).$$

Demonstração: Se $i = 0$ nada temos a fazer, já que o único vetor de peso zero é o vetor nulo. Se $i > 0$, seja $v \in S_P(0, i)$, $\langle \text{supp}(v) \rangle$ é um ideal de i

elementos. Agora, dado um ideal $I \subset P$ de cardinalidade i , vamos determinar quantos vetores em (\mathbb{F}_q^n, d_P) satisfazem $\langle \text{supp}(v) \rangle = I$.

Assim, seja $v \in S_P(0, i) \subset \mathbb{F}_q^n$, podemos escrever:

$$v = \sum_{k \in M(I)} a_k e_k + \sum_{k \in I \setminus M(I)} b_k e_k + \sum_{k \notin I} c_k e_k$$

onde e_k é o k -ésimo vetor da base canônica de \mathbb{F}_q^n .

Como $v \in S_P(0, i)$ e $I = \langle \text{supp}(v) \rangle$, então, $M(I) \subset \text{supp}(v) \subset I$. Dessa forma, temos para cada v , que cada coordenada a_k cuja posição é maximal (j coordenadas) não pode ser nula, logo restam $(q - 1)$ valores a escolher para cada uma destas coordenadas, ou seja, $(q - 1)^j$ escolhas.

Por sua vez, para as coordenadas b_k que pertencem ao ideal mas não são maximais, $(i - j)$ coordenadas, podemos, para cada uma delas, escolher entre q valores, uma vez que não há restrições para essas coordenadas podendo elas serem nulas ou não, assim temos $q^{(i-j)}$ escolhas.

Por fim, as coordenadas c_k do vetor que não pertence ao ideal, $(n - i)$ coordenadas, necessariamente são nulas, ou seja, há apenas uma possibilidade.

Desde que, o ideal gerado pelo suporte de v pode ter desde 1 elemento maximal até i elementos maximais, segue que, denotando por $\Omega_j^P(i)$ o número de ideais de P com cardinalidade i e contendo exatamente j elementos maximais temos que:

$$|S_P(0, i)| = \sum_{j=1}^i (q - 1)^j q^{(i-j)} \Omega_j^P(i).$$

□

Corolário 2.2.4. *A cardinalidade de uma P – bola de raio r é:*

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

Demonstração: Inicialmente note que dados $x, y \in \mathbb{F}_q^n$ como

$$d_P(x, y) = \omega_P(x - y) = d_P(0, x - y)$$

segue que a cardinalidade de uma P -esfera independe do centro. Observe ainda que,

$$S_P(0, r) \cap S_P(0, s) = \emptyset \quad \text{para } r \neq s.$$

Desta forma, como

$$B_P(0, r) = \bigcup_{i=0}^r S_P(0, i)$$

segue que,

$$|B_P(0, r)| = 1 + \sum_{i=1}^r \sum_{j=1}^i (q-1)^j q^{(i-j)} \Omega_j(i).$$

□

Toda a teoria de códigos teve um ganho bastante considerável com a introdução dessas novas métricas, o ganho mais importante para a teoria foi que muitos códigos que não eram perfeitos, considerando a métrica de Hamming, passam a ser perfeitos considerando novas métricas. Como é o caso do próximo exemplo.

Exemplos 2.2.5 ([1]). *O código de Hamming estendido C em \mathbb{F}_2^8 dado pela*

matriz verificação de paridade

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

é um P -código perfeito se as únicas comparações em $P = \{1, 2, 3, 4, 5, 6, 7, 8\}$ são $1 < i$ com $i = 2, 3, \dots, 8$. Em contrapartida C não é um código perfeito se P é anticadeia, ou seja, C não é um código perfeito com a métrica de Hamming.

Desde 1995 muitos tópicos e questões relevantes no contexto clássico (Hamming) de teoria de códigos tem sido estudados e desenvolvidos no contexto de espaços poset. Dentre as questões pertinentes estão aquelas que mesmo sem lidar diretamente com o estudo dos códigos tratam de aspectos genéricos ou estruturais dos P -espaços. Destacamos que a obtenção de resultados genéricos e independentes da escolha de posets específicos costuma ser árdua. A título de exemplo, citamos a descrição dos grupos de isometrias lineares de tais espaços.

Uma isometria linear em (\mathbb{F}_q^n, d_P) é uma aplicação linear $T : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$ tal que

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

ou equivalentemente, $\omega_P(T(x)) = \omega_P(x)$, $\forall x \in \mathbb{F}_q^n$. Denotaremos o grupo das isometrias lineares de (\mathbb{F}_q^n, d_P) por $GL_P(\mathbb{F}_q^n)$.

A descrição dos grupos de isometrias lineares iniciou em 2003 com o trabalho de Kim e Cho [7] onde é descrito o grupo das isometrias lineares

para a classe de poset coroa $\mathcal{CR} = \mathcal{CR}(2m)$; Lee [8] descreve o grupo das isometrias lineares para a métrica de Rosenbloom-Tsfasman. E então em 2008, Firer, Hyun, Kim e Panek [9] publicam um trabalho com a descrição do $GL_P(\mathbb{F}_q^n)$ onde P é um poset qualquer. A seguir enunciaremos estes resultados:

Proposição 2.2.6 ([9]). *Dados P um poset sobre $[n]$, $\{e_1, \dots, e_n\}$ a base canônica de \mathbb{F}_q^n e $T \in GL_P(\mathbb{F}_q^n)$ uma isometria linear. Então a aplicação $\phi_T : P \rightarrow P$ dada por*

$$\phi_T(i) = \max \langle \text{supp}(T(e_i)) \rangle$$

é um automorfismo de P .

Teorema 2.2.7 ([9]). *Sejam P um poset sobre $[n]$ e $\{e_1, \dots, e_n\}$ a base canônica de \mathbb{F}_q^n . Então, $T \in GL_P(\mathbb{F}_q^n)$ se, e somente se,*

$$T(e_j) = \sum_{i \leq j} x_{ij} e_{\phi_T(i)},$$

onde $\phi_T : P \rightarrow P$ é o automorfismo associado a T como no lema acima e x_{ij} são constantes com $x_{jj} \neq 0$ para todo $j \in \{1, 2, \dots, n\}$. Mais ainda, dado $T \in GL_P(\mathbb{F}_q^n)$, existe um par de bases ordenadas β e β_T de \mathbb{F}_q^n para as quais a isometria linear T é representada por uma matriz $n \times n$ triangular superior $(a_{ij})_{1 \leq i, j \leq n}$ com $a_{jj} \neq 0$ para todo $j \in \{1, 2, \dots, n\}$.

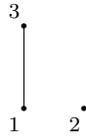
Outra questão estrutural neste contexto é a possibilidade de extensão de isometrias.

Dados códigos (lineares) $C, C' \subset \mathbb{F}_q^n$ e uma P -isometria $f : C \rightarrow C'$, que condições (sobre P ou também sobre C) são necessárias e suficientes para existir

$$F \in GL_P(\mathbb{F}_q^n) \quad \text{tal que} \quad F|_C = f?$$

Nem sempre essa extensão é possível, conforme exemplo abaixo.

Exemplos 2.2.8. *Sejam $C = \{(0, 0, 0), (0, 0, 1)\}$ e $C' = \{(0, 0, 0), (1, 1, 0)\}$ dois códigos em \mathbb{F}_2^3 , $P = \{1, 2, 3\}$ com $1 \preceq 3$ cujo diagrama de Hasse é,*



e $f : C \rightarrow C'$ uma aplicação tal que $f(0, 0, 0) = (0, 0, 0)$ e $f(0, 0, 1) = (1, 1, 0)$.

A aplicação f é uma isometria que não pode ser estendida a todo \mathbb{F}_2^3 .

Com efeito, $\omega_P(f(0, 0, 0)) = \omega_P(0, 0, 0) = 0$ e

$$\begin{aligned} \omega_P(0, 0, 1) &= |\langle \text{supp}(0, 0, 1) \rangle| \\ &= |\langle \{3\} \rangle| \\ &= |\{1, 3\}| \\ &= 2. \end{aligned}$$

$$\begin{aligned} \omega_P(1, 1, 0) &= |\langle \text{supp}(1, 1, 0) \rangle| \\ &= |\langle \{1, 2\} \rangle| \\ &= |\{1, 2\}| \\ &= 2. \end{aligned}$$

No entanto, assumindo que $F \in GL_P(\mathbb{F}_2^3)$ é tal que $F|_C = f$, pela Proposição 2.2.6, devemos ter que $\langle \text{supp}(F(0, 0, 1)) \rangle$ deve ser gerado por um único elemento, o que não ocorre com o ideal $\{1, 2\} = \langle \text{supp}(f(0, 0, 1)) \rangle$.

No contexto desta questão, extensão de isometrias, nos deparamos com uma outra questão de carácter amplo, o problema da determinação da métrica a partir da distribuição de pesos, que apresentamos e desenvolvemos no próximo capítulo.

Capítulo 3

Distribuição de pesos

3.1 Distribuição de pesos de algumas classes de posets

Dado um poset P e i , $1 \leq i \leq n$, seja $A_{i,P} := |\{x \in \mathbb{F}_q^n, \omega_P(x) = i\}|$ o número de vetores em \mathbb{F}_q^n cujo P -peso é i (usamos a notação A_i quando não houver ambiguidades). Em outras palavras, considerando que $\omega_P(x) = d_P(x, 0)$ e a cardinalidade da P -esfera independe do centro, $A_{i,P}$ é a cardinalidade de uma P -esfera de raio i , ou seja, $A_{i,P} = |S_P(0, i)|$. Diremos que a sequência ordenada finita

$$\mathcal{D}_P = (A_{1,P}, A_{2,P}, \dots, A_{n,P})$$

é a *distribuição de P -pesos (DP)* de $(\mathbb{F}_q^n, \omega_P)$.

Segue então da Proposição 2.2.3, segue que:

$$A_{i,P} = \sum_{j=1}^i (q-1)^j q^{(i-j)} \Omega_j^P(i).$$

Ao longo desta seção apresentaremos uma série de exemplos tratando do problema central deste trabalho, **o problema da distribuição de pesos**:

Sob quais condições podemos garantir que dois espaços poset (\mathbb{F}_q^n, d_P) e (\mathbb{F}_q^n, d_Q) com $\mathcal{D}_P = \mathcal{D}_Q$, são isométricos ou equivalentemente, quando P e Q são posets isomorfos?

Começamos com uma proposição que segue diretamente da definição de DP e que nos será muito útil durante as demonstrações dos resultados que seguem.

Proposição 3.1.1. *Dado um P -espaço (\mathbb{F}_q^n, d_P) , onde P é um poset sobre $[n]$, então, $A_1 = |N_1^P|(q - 1)$, onde N_1^P é o primeiro nível do poset P .*

Demonstração: De fato, se $x \in \mathbb{F}_q^n$ é tal que $\omega_P(x) = 1$ então $|\langle \text{supp}(x) \rangle| = 1$ logo $x = (0, \dots, 0, x_j, 0, \dots, 0)$ para algum j , tal que $|\langle j \rangle| = 1$ e $x_j \neq 0$, ou seja, j pertence ao primeiro nível de P ; como x_j é não nulo, ele pode assumir $(q - 1)$ valores em \mathbb{F}_q . Portanto, temos que $A_{1,P} = |N_1^P|(q - 1)$. \square

Vamos começar apresentando a distribuição de pesos das principais famílias de posets introduzidas no primeiro capítulo. A menos que mencionamos o(s) autor(es), os resultados, exemplos, proposições e teoremas que aparecerão de agora em diante, são todos originais, obtidos neste trabalho.

Exemplos 3.1.2 (Anticadeia ou Hamming (H)). *Desde que em uma anticadeia temos que $\langle \text{supp}(\text{dot}) \rangle = \text{supp}(\text{dot})$, segue da proposição acima que se um poset H é uma anticadeia de cardinalidade n , então $\mathcal{D}_H = \left(\binom{n}{i} (q - 1)^i \right)_{i=1}^n$. Com efeito, basta observar que em uma anticadeia todos os elementos estão*

no primeiro nível e aí a procura pela \mathcal{D}_H se torna um simples problema de contagem.

Exemplos 3.1.3 (Cadeia ou linear (\mathcal{C}_n)). *Seja \mathcal{C}_n o poset cadeia de cardinalidade n . Então a distribuição de pesos do espaço $(\mathbb{F}_q^n, \omega_{\mathcal{C}_n})$ é dada por $\mathcal{D}_{\mathcal{C}_n} = ((q-1)q^{i-1})_{i=1}^n$. De fato, como \mathcal{C}_n é uma cadeia, se $x = (x_1, x_2, \dots, x_n) \in \mathbb{F}_q^n$ possui peso i e k é a maior coordenada não nula de x , ou seja, $k = \max\{j : x_j \neq 0\}$. Então $\omega(x) = |\langle k \rangle| = i$, ou seja, k pertence ao i -ésimo nível de P e, como $x_k \neq 0$, esta coordenada pode assumir $(q-1)$ valores em \mathbb{F}_q . Quanto às $(i-1)$ coordenadas de x que estão nos níveis inferiores ao i -ésimo, esses não interferem no peso de x e conseqüentemente podem assumir qualquer valor em \mathbb{F}_q . Portanto, $A_i = (q-1) \cdot q^{i-1}$.*

O próximo exemplo, não tão simples como os apresentados até agora, nos mostra que a DP de um espaço peso pode ser um problema um tanto difícil. A DP para o poset coroa, foi demonstrada por Kim e Cho em trabalho publicado em 2007.

Exemplos 3.1.4 (Coroa (CR)). [6] *Seja CR o poset Coroa definido sobre $[2m]$. Para este caso, temos que a distribuição de pesos é dada por:*

$$A_{j,CR} = \frac{1}{(2m-j)!} \sum_{(i_1, i_2, \dots, i_m)} \binom{2m-j}{i_1 i_2 \dots i_m} Tr(M^{(i_1)} M^{(i_2)} \dots M^{(i_m)})$$

onde a soma percorre todas as m -uplas de inteiros (i_1, i_2, \dots, i_m) satisfazendo

$$0 \leq i_1, \dots, i_m \leq 2 \text{ e } i_1 + i_2 + \dots + i_m = 2m - j,$$

$$\binom{2m-j}{i_1 i_2 \dots i_m} = \binom{2m-j}{i_1} \binom{2m-j-i_1}{i_2} \dots \binom{2m-j-i_1-i_2-\dots-i_{m-1}}{i_m}$$

é o coeficiente multinomial usual, Tr é a função traço de matriz quadrada, e

$$M^{(0)} = \begin{bmatrix} 0 & 0 \\ (q-1)q^2 & (q-1)q \end{bmatrix}, M^{(1)} = \begin{bmatrix} q-1 & 1 \\ 0 & 0 \end{bmatrix}, M^{(2)} = \begin{bmatrix} 2 & 0 \\ 0 & 0 \end{bmatrix}.$$

Para ilustrar este caso, afim de torná-lo mais claro determinaremos a $\mathcal{D}_{\mathcal{CR}}$ para o \mathcal{CR} -espaço 6-dimensional sobre o corpo binário. De acordo com a expressão acima, a distribuição de pesos $\{A_j\}_{j=1}^6$ de $(\mathbb{F}_2^6, \omega_{\mathcal{CR}})$ é dada por,

$$A_{j,\mathcal{CR}} = \frac{1}{(6-j)!} \sum \binom{6-j}{i_1 i_2 i_3} Tr(M^{(i_1)} M^{(i_2)} M^{(i_3)})$$

onde $M^{(0)} = \begin{bmatrix} 0 & 0 \\ 4 & 2 \end{bmatrix}$, $M^{(1)} = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$ e $M^{(2)} = \begin{bmatrix} 2 & 0 \\ 0 & 0 \end{bmatrix}$.

Segue então que:

Se $j = 0$, (i_1, i_2, i_3) percorre o conjunto $\{(2, 2, 2)\}$ e

$$A_{0,\mathcal{CR}} = \frac{1}{6!} \sum \binom{6}{2 \ 2 \ 2} Tr(M^{(2)} M^{(2)} M^{(2)}) \quad (3.1)$$

$$= \frac{1}{6!} \cdot 90 \cdot 8 = 1. \quad (3.2)$$

Se $j = 1$, (i_1, i_2, i_3) percorre o conjunto $\{(1, 2, 2), (2, 1, 2), (2, 2, 1)\}$ e

$$\begin{aligned} A_{1,\mathcal{CR}} &= \frac{1}{5!} \sum \binom{5}{1 \ 2 \ 2} \cdot 3 \cdot Tr(M^{(1)} M^{(2)} M^{(2)}) \\ &= \frac{1}{5!} \cdot 30 \cdot 3 \cdot 4 = 3 \end{aligned}$$

Se $j = 2$, (i_1, i_2, i_3) percorre o conjunto

$$\{(2, 1, 1), (1, 2, 1), (1, 1, 2), (0, 2, 2), (2, 0, 2), (2, 2, 0)\}$$

e

$$\begin{aligned} A_{2, \mathcal{CR}} &= \frac{1}{4!} \left\{ \binom{4}{2 \ 1 \ 1} \cdot 3 \cdot \text{Tr}(M^{(2)} M^{(1)} M^{(1)}) \right. \\ &\quad \left. + \binom{4}{0 \ 2 \ 2} \cdot 3 \cdot \text{Tr}(M^{(0)} M^{(2)} M^{(2)}) \right\} \\ &= \frac{1}{4!} (12 \cdot 3 \cdot 2 + 6 \cdot 3 \cdot 0) = 3. \end{aligned}$$

Se $j = 3$, (i_1, i_2, i_3) percorre o conjunto

$$\{(1, 1, 1), (0, 1, 2), (2, 0, 1), (1, 2, 0), (0, 2, 1), (1, 0, 2), (2, 1, 0)\}$$

e

$$\begin{aligned} A_{\mathcal{CR}, 3} &= \frac{1}{3!} \left\{ \binom{3}{1 \ 1 \ 1} \cdot \text{Tr}(M^{(1)} M^{(1)} M^{(1)}) \right. \\ &\quad + \binom{3}{0 \ 2 \ 2} \cdot 3 \cdot \text{Tr}(M^{(0)} M^{(1)} M^{(2)}) \\ &\quad \left. + \binom{3}{0 \ 2 \ 1} \cdot 3 \cdot \text{Tr}(M^{(0)} M^{(2)} M^{(1)}) \right\} \\ &= \frac{1}{3!} (6 \cdot 1 + 3 \cdot 3 \cdot 0 + 3 \cdot 3 \cdot 8) = 13. \end{aligned}$$

Se $j = 4$, (i_1, i_2, i_3) percorre o conjunto

$$\{(0, 1, 1), (1, 0, 1), (1, 1, 0), (2, 0, 0), (0, 2, 0), (0, 0, 2)\}$$

e

$$\begin{aligned} A_{4, \mathcal{CR}} &= \frac{1}{2!} \left\{ \binom{2}{0 \ 1 \ 1} \cdot 3 \cdot \text{Tr}(M^{(0)} M^{(1)} M^{(1)}) \right. \\ &\quad \left. + \binom{2}{2 \ 0 \ 0} \cdot 3 \cdot \text{Tr}(M^{(2)} M^{(0)} M^{(0)}) \right\} \\ &= \frac{1}{2!} (2 \cdot 3 \cdot 4 + 1 \cdot 3 \cdot 0) = 12. \end{aligned}$$

Se $j = 5$, (i_1, i_2, i_3) percorre $\{(1, 0, 0), (0, 1, 0), (0, 0, 1)\}$ e

$$\begin{aligned} A_{5,CR} &= \frac{1}{1!} \binom{1}{1 \ 0 \ 0} \cdot 3 \cdot \text{Tr}(M^{(1)}M^{(0)}M^{(0)}) \\ &= 3 \cdot 8 = 24. \end{aligned}$$

Finalmente, se $j=6$ então $(i_1, i_2, i_3) = (0, 0, 0)$ e

$$A_{6,CR} = \frac{1}{0!} \binom{0}{0 \ 0 \ 0} \cdot \text{Tr}(M^{(0)}M^{(0)}M^{(0)}) = 8.$$

E portanto, a distribuição de pesos do espaço $(\mathbb{F}_2^6, \omega_{CR})$ é

$$\mathcal{D}_{CR} = (1, 3, 3, 13, 12, 24, 8).$$

Exemplos 3.1.5 (Hierárquico (H)). *Se agora considerarmos o poset Hierárquico \mathcal{H} definido no primeiro capítulo, podemos ver que a distribuição de pesos de $(\mathbb{F}_q^n, d_{\mathcal{H}})$ é:*

$$A_{j,\mathcal{H}} = \begin{cases} 1 & \text{se } j = 0 \\ \binom{n_{l+1}}{j-k_l} (q-1)^{j-k_l} q^{k_l} & \text{se } k_l < j \leq k_{l+1} \end{cases}$$

onde $k_l = n_1 + \dots + n_l$ e $k_0 = 0$.

Com efeito, inicialmente note que se $0 < j \leq n_1$ e $x \in F_q^n$ é um vetor tal que $\omega_{\mathcal{H}}(x) = j$ então $\langle \text{supp}(x) \rangle \subseteq N_1^{\mathcal{H}}$ e como $N_1^{\mathcal{H}}$ é uma anticadeia segue do Exemplo 3.1.2 nossa afirmação, neste caso. Considere então que $k_l < j \leq k_{l+1}$ e $x \in \mathbb{F}_q^n$ é um vetor tal que $\omega_{\mathcal{H}}(x) = j$ então devemos ter $\text{supp}(x) \subseteq \cup_{s=1}^{l+1} N_s^{\mathcal{H}}$ pois, se $\text{supp}(x) \subseteq \cup_{s=1}^l N_s^{\mathcal{H}}$, como $|\cup_{s=1}^l N_s^{\mathcal{H}}| = k_l$ obtemos que $\omega_{\mathcal{H}}(x) = |\langle \text{supp}(x) \rangle| \leq k_l$, um absurdo. Agora, se $\langle \text{supp}(x) \rangle \cap N_{l+2}^{\mathcal{H}} \neq \emptyset$ deveríamos ter $\omega_{\mathcal{H}}(x) \geq k_{l+1} + 1$, novamente, um absurdo. Como $\text{supp}(x) \subseteq \cup_{s=1}^{l+1} N_s^{\mathcal{H}}$ e em \mathcal{H} todo elemento de um determinado nível é maior que cada elemento dos níveis inferiores temos que $\langle \text{supp}(x) \rangle \subseteq \langle N_{l+1}^{\mathcal{H}} \rangle$ e

também $\text{supp}(x)$ possui $j - k_l$ elementos maximais. Agora para os $j - k_l$ índices de x que são elementos maximais do $\langle \text{supp}(x) \rangle$ existem $|N_{l+1}^{H_i}| = n_l$ possibilidades e como cada entrada com estes índices deve ser não nula existem $(q - 1)^{j - k_l}$ possibilidades para estas. Para as outras k_l coordenadas de x que estão nos níveis inferiores estas não interferem no peso de x e portanto podem assumir q^{k_l} valores em \mathbb{F}_q .

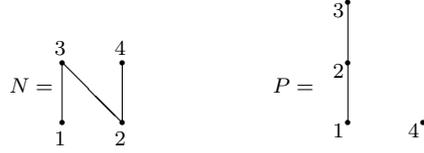
3.2 Determinação da ordem via distribuição de pesos

Esta seção será dedicada exclusivamente a mostrar os resultados obtidos (neste trabalho) sobre a questão da determinação da ordem através da distribuição de pesos:

Sob quais condições podemos garantir que dois espaços poset (\mathbb{F}_q^n, d_P) e (\mathbb{F}_q^n, d_Q) com $\mathcal{D}_P = \mathcal{D}_Q$, são isométricos ou equivalentemente, quando P e Q são posets isomorfos?

Iniciamos esta seção com um contra-exemplo para o caso geral, obtendo que de modo geral a distribuição de pesos de um P -espaço não determina a ordem P . Com efeito:

Exemplos 3.2.1. *Sejam $N = \{1, 2, 3, 4 : 1 \preceq_N 3, 2 \preceq_N 3, 2 \preceq_N 4\}$ e $P = \{1, 2, 3, 4 : 1 \preceq_P 2, 2 \preceq_P 3, 1 \preceq_P 3\}$ dois posets sobre $[4]$. Cujos diagramas de Hasse são respectivamente os seguintes*



Note que para o N -espaço (\mathbb{F}_2^4, d_N) as esferas de centro na origem são:

$$S_N(0_{\mathbb{F}_2^4}, 0) = \{0_{\mathbb{F}_2^4}\}$$

$$S_N(0_{\mathbb{F}_2^4}, 1) = \{(1, 0, 0, 0), (0, 1, 0, 0)\}$$

$$S_N(0_{\mathbb{F}_2^4}, 2) = \{1, 1, 0, 0), (0, 0, 0, 1), (0, 1, 0, 1)\}$$

$$S_N(0_{\mathbb{F}_2^4}, 3) = \{(0, 0, 1, 0), (1, 0, 1, 0), (0, 1, 1, 0), (1, 1, 1, 0), (1, 0, 0, 1), (1, 1, 0, 1)\}$$

$$S_N(0_{\mathbb{F}_2^4}, 4) = \{(0, 0, 1, 1), (1, 0, 1, 1), (0, 1, 1, 1), (1, 1, 1, 1)\}$$

e para o P -espaço (\mathbb{F}_2^4, d_P) as esferas são:

$$S_P(0_{\mathbb{F}_2^4}, 0) = \{0_{\mathbb{F}_2^4}\}$$

$$S_P(0_{\mathbb{F}_2^4}, 1) = \{(1, 0, 0, 0), (0, 0, 0, 1)\}$$

$$S_P(0_{\mathbb{F}_2^4}, 2) = \{1, 0, 0, 1), (0, 1, 0, 0), (1, 1, 0, 0)\}$$

$$S_P(0_{\mathbb{F}_2^4}, 3) = \{(0, 0, 1, 0), (1, 0, 1, 0), (0, 1, 1, 0), (1, 1, 1, 0), (0, 1, 0, 1), (1, 1, 0, 1)\}$$

$$S_P(0_{\mathbb{F}_2^4}, 4) = \{(0, 0, 1, 1), (1, 0, 1, 1), (0, 1, 1, 1), (1, 1, 1, 1)\}.$$

Como $A_{i,P} = |S_P(0, i)|$ segue que $\mathcal{D}_P = (1, 2, 3, 6, 4) = \mathcal{D}_N$. Agora, como N é conexo, P é desconexo e isomorfismos preservam conexidade temos que N e P são não isomorfos.

O exemplo acima mostra que a DP é um invariante mais fraco que o poset que induz a métrica. Assim, precisamos buscar condições que possam

garantir a determinação de métrica e de poset a partir da distribuição de pesos.

O primeiro tipo de restrições refere-se a fixar a classe da ordem P . Se considerarmos P uma das ordens de algumas das importantes famílias que introduzimos no primeiro capítulo (anti-cadeia, cadeia, coroa ou hierárquico) podemos garantir que a distribuição de pesos determina a ordem.

Observamos que estas classes de posets são as mais relevantes e muitas vezes tratadas de modo particular ([6], [7] e [11], a título de exemplo), no que tange o estudo de códigos com estrutura poset.

Apesar de a classe de poset hierárquicos conter as classes de posets cadeia e anti-cadeia, vamos demonstrar cada um destes casos separadamente, pois estes casos iniciais introduzem os tipos de argumentos que são utilizados posteriormente.

Proposição 3.2.2 (Hamming). *Sejam H o poset anti-cadeia sobre $[n]$ e P um poset sobre $[n]$ tal que a DP do P -espaço (\mathbb{F}_q^n, d_P) coincide com a DP do H -espaço (\mathbb{F}_q^n, d_H) , ou seja, $\mathcal{D}_H = \mathcal{D}_P$. Então, P é também uma anticadeia e consequentemente P é isomorfo a H .*

Demonstração: Neste caso o H -peso coincide com o peso de *Hamming*. Agora, sendo

$$|N_1^P|(q-1) = A_{1,P} = A_{1,H} = n(q-1)$$

da Proposição 3.1.1 segue que $|N_1^P| = n$, donde P possui n elementos em N_1^P , em outras palavras, todos os elementos de P são mínimos. Consequentemente, P é uma anticadeia de cardinalidade n e logo P é isomorfo a H . □

Note que na demonstração acima foi usado apenas que $A_{1,P} = A_{1,H}$. Dessa forma, no enunciado da proposição acima poderia ser exigido apenas que $A_{1,P} = A_{1,H}$ ao invés de $\mathcal{D}_H = \mathcal{D}_P$, no entanto, como estamos interessados em condições de suficiência para que o problema da determinação de pesos tenha uma resposta afirmativa o enunciado foi mantido para explicitar que se restringirmos a questão a essa classe de ordem (antidadeia) conseguimos uma resposta afirmativa.

O raciocínio acima nos permite concluir o seguinte resultado:

Lema 3.2.3. *Sejam P e Q dois posets sobre $[n]$ tais que $A_{1,P} = A_{1,Q}$. O número de elementos mínimos de P coincide com o número de elementos mínimos de Q , ou seja $|N_1^P| = |N_1^Q|$.*

Demonstração: A demonstração segue diretamente da hipótese $A_{1,P} = A_{1,Q}$ e da Proposição (3.1.1), a qual afirma que $A_{1,P} = |N_1^P| \cdot (q - 1)$. \square

Proposição 3.2.4 (Cadeia (ou linear)). *Sejam C_n o poset cadeia sobre $[n]$ e P um poset sobre $[n]$ tal que a DP do P -espaço (\mathbb{F}_q^n, d_P) coincide com a DP do C_n -espaço $(\mathbb{F}_q^n, d_{C_n})$, ou seja, $\mathcal{D}_{C_n} = \mathcal{D}_P$. Então, P é também uma cadeia e conseqüentemente P é isomorfo a C_n .*

Demonstração: Vimos no exemplo 3.1.3 que $A_{i,C_n} = (q - 1)q^{i-1}$ e como $A_{1,P} = A_{1,C_n}$ temos que $A_{1,P} = (q - 1)$, o que implica que P possui apenas um elemento mínimo (ou seja, P possui apenas um elemento no primeiro nível). Assim, $A_{2,P} = \binom{|N_1^P|}{2}(q - 1)^2 + |N_{2,2}^P|(q - 1)q = |N_{2,2}^P|(q - 1)q$ (pois, $\binom{|N_1^P|}{2} = 0$) e como $A_{2,P} = A_{2,C_n}$ segue que $|N_{2,2}^P| = |N_{2,2}^{C_n}| = 1$. Note agora que $|N_{2,j}^P| = 0$ para $j > 2$. De fato, se $N_{2,j}^P \neq \emptyset$, devem existir ao menos

$j - 1 > 1$ elementos em N_1^P , o que sabemos que não ocorre. O mesmo raciocínio é utilizado indutivamente para os níveis superiores. Com efeito, usaremos indução sobre i para fazer a demonstração.

Suponhamos agora que para todo $i \leq k - 1$ temos $|N_{i,i}^P| = 1$ e $|N_{i,j}^P| = 0$ para todo $j > i$.

Assim, $A_{k,P} = |N_{k,k}^P|(q - 1)q^{k-1}$, mas $A_{k,P} = A_{k,C} = (q - 1)q^{k-1}$ donde $|N_{k,k}^P| = 1$ e também $|N_{k,k+j}^P| = 0$ para todo $j \geq 1$, pois se $l \in N_{k,k+j}^P$ então $l \in N_k^P$ e $|\langle l \rangle| = k + j$, logo $\langle l \rangle = \{l, l_2, l_3, \dots, l_{k+j}\}$ onde $l_2, l_3, \dots, l_{k+j} \in \bigcup_{t=1}^{k-1} N_t^P$, mas $|\bigcup_{t=1}^{k-1} N_t^P| = k - 1$ donde segue que existem j elementos repetidos em $\langle l \rangle$ e daí $|\langle l \rangle| = k$, o que é absurdo. Portanto P tem apenas um elemento em cada nível. Consequentemente P é uma cadeia. \square

Proposição 3.2.5 (Coroa $\mathcal{CR} = \mathcal{CR}[2m]$). *Sejam \mathcal{CR} o poset coroa sobre $[2m]$ e P um poset sobre $[2m]$ tal que a DP do P -espaço (\mathbb{F}_q^n, d_P) coincide com a DP do \mathcal{CR} -espaço $(\mathbb{F}_q^n, d_{\mathcal{CR}})$, ou seja, $\mathcal{D}_{\mathcal{CR}} = \mathcal{D}_P$. Então, P possui também a estrutura de coroa e conseqüentemente P é isomorfo a \mathcal{CR} .*

Demonstração: Do Lema 3.2.3 e do fato $A_{1,P} = A_{1,\mathcal{CR}} = m(q - 1)$ temos que P possui m elementos mínimos.

Afirmamos que $P = N_1^P \cup N_{2,3}^P$ e $|N_{2,3}^P| = m$. De fato, $A_{2,P} \geq \binom{m}{2}(q - 1)^2$ já que m coordenadas de peso 1 (os elementos do primeiro nível de P) contribuem com $\binom{m}{2}(q - 1)^2$ elementos de peso 2, no entanto, $A_{2,P} = A_{2,\mathcal{CR}} = \binom{m}{2}(q - 1)^2$ logo P não possui elementos no nível 2 de peso 2, ou seja, $N_{2,2}^P = \emptyset$. Como $A_{3,P} = \binom{m}{3}(q - 1)^3 + (|N_{2,3}^P| + |N_{3,3}^P|)(q - 1)q^2$ e $A_{3,P} = A_{3,\mathcal{CR}} =$

$\binom{m}{3}(q-1)^3 + m(q-1)q^2$ então $(|N_{2,3}^P| + |N_{3,3}^P|) = m$. Entretanto, $|N_{3,3}^P| = 0$, pois $|N_{2,2}^P| = 0$. Com efeito, se $i \in N_{3,3}^P$ então $i \in N_3^P$ e $|\langle i \rangle| = 3$, logo $\langle i \rangle = \{i, r, s\}$ onde $s \prec_{\mathcal{CR}} r \prec_{\mathcal{CR}} i$, dessa forma teríamos que $|\langle r \rangle| = 2$, um absurdo já que P não possui ideal principal de cardinalidade 2. Assim $|N_{2,3}^P| = m$ e conseqüentemente, $P = N_1^P \cup N_{2,3}^P$.

Seja

$$\alpha := |\{i \in N_{2,3}^P : \exists j \neq i \in N_{2,3}^P \text{ com } |\langle i \rangle \cap \langle j \rangle| = 2\}|.$$

Então

$$A_{4,P} = \binom{m}{4}(q-1)^4 + m(m-2)(q-1)^2q^2 + \alpha(q-1)^2q^2$$

no entanto, por hipótese,

$$A_{4,P} = A_{4,\mathcal{CR}} = \binom{m}{4}(q-1)^4 + m(m-2)(q-1)^2q^2$$

donde $\alpha = 0$, isto é, em P não existem dois ideais principais cuja interseção possua dois elementos, concluimos que os ideais principais gerados por elementos distintos do segundo nível de P ou são disjuntos ou se intersectam em um único elemento.

Seja

$$\beta := |\{i \in N_{2,3}^P : \exists j \in N_{2,3}^P \text{ com } |\langle i \rangle \cap \langle j \rangle| = 1\}|.$$

Então

$$A_{5,P} = \binom{m}{5}(q-1)^5 + m \binom{m-2}{2}(q-1)^3q^2 + \beta(q-1)^2q^3$$

e como por hipótese

$$A_{5,P} = A_{5,\mathcal{CR}} = \binom{m}{5}(q-1)^5 + m \binom{m-2}{2}(q-1)^3q^2 + m(q-1)^2q^3$$

segue que $\beta = m$, ou seja, para todo $i \in N_2^P$ existe ao menos um $j \in N_2^P$ distinto de i tal que $|\langle i \rangle \cap \langle j \rangle| = 1$.

Seja

$$\gamma := |\{i \in N_{2,3}^P : \exists j, k \in N_{2,3}^P \text{ com } |\langle i \rangle \cap \langle j \rangle \cap \langle k \rangle| = 1\}|.$$

Então

$$A_{7,P} = \binom{m}{7} (q-1)^{7+m} \binom{m-2}{4} (q-1)^5 q^2 + m \binom{m-3}{2} (q-1)^4 q^3 + [m(m-2)(m-4) + \gamma] (q-1)^3 q^4.$$

Ao compararmos esta igualdade com a expressão $A_{7,\mathcal{CR}}$ vemos que $\gamma = 0$, ou seja, dados $i, j, k \in N_2^P$ distintos então $\langle i \rangle \cap \langle j \rangle \cap \langle k \rangle = \emptyset$.

Resumindo, sabemos sobre P :

1. $P = N_1^P \cup N_{2,3}^P$;
2. Dados $i, j \in N_{2,3}^P$ distintos então $|\langle i \rangle \cap \langle j \rangle| \leq 1$;
3. Se $i, j, k \in N_{2,3}^P$ são distintos então $\langle i \rangle \cap \langle j \rangle \cap \langle k \rangle = \emptyset$.

Vamos mostrar agora que um poset com essas propriedades deve ser isomorfo ao coroa. Com efeito, considere a matriz $A = (a_{ij})_{m \times m}$ obtida de P fazendo, $i \in N_1^P$, $j \in N_2^P$ e

$$a_{ij} = \begin{cases} 1 & \text{se } i \preceq_P j \\ 0 & \text{se } i \not\preceq_P j \end{cases}$$

As propriedades acima se traduzem em termos de A no seguinte modo:

1. Cada coluna de A possui exatamente duas entradas não nulas;
2. A não possui duas colunas iguais;

3. Toda linha de A tem no máximo duas entradas não nulas.

Como cada coluna possui exatamente dois elementos iguais a 1, temos que a matriz A possui $2m$ entradas não nulas. Como A tem $2m$ entradas não nulas e cada linha tem no máximo 2 entradas não nulas, conclui-se que cada linha tem exatamente 2 entradas não nulas, isso implica que cada elemento de N_1^P é menor que exatamente dois elementos de $N_{2,3}^P$, o que implica que P pode ser obtido de CR por uma permutação dos elementos que deixa invariante cada nível. Portanto, P é isomorfo a CR . \square

Antes de demonstrarmos a próxima proposição precisamos introduzir alguns conceitos.

Seja

$$\Lambda_j^P(i) := \{I \subseteq P : I \text{ é ideal}, |I| = i \text{ e } |M(I)| = j\}$$

onde $M(I) := \{\text{elementos maximais de } I\}$ e seja $\Omega_j^P(i) = |\Lambda_j^P(i)|$.

Relembremos que a distribuição de pesos num espaço poset arbitrário é dada por:

$$A_i^P = \sum_{j=1}^i \Omega_j^P(i) (q-1)^j q^{i-j}. \quad (3.3)$$

A título de ilustração retomamos o Exemplo 3.2.1, onde obtemos

$$\begin{array}{ll} \Omega_1^N(1) = 2 & \Omega_1^P(1) = 2 \\ \Omega_1^N(2) = 1 & \Omega_1^P(2) = 1 \\ \Omega_1^N(3) = 1 & \Omega_1^P(3) = 1 \\ \Omega_1^N(4) = 0 & \Omega_1^P(4) = 0 \end{array}$$

$$\begin{array}{ll}
\Omega_2^N(2) = 1 & \Omega_2^P(2) = 1 \\
\Omega_2^N(3) = 1 & \Omega_2^P(3) = 1 \\
\Omega_2^N(4) = 1 & \Omega_2^P(4) = 1 \\
\Omega_3^N(3) = 0 & \Omega_3^P(3) = 0 \\
\Omega_3^N(4) = 0 & \Omega_3^P(4) = 0 \\
\Omega_4^N(4) = 0 & \Omega_4^P(4) = 0
\end{array}$$

que os coeficientes são todos iguais de P e de N.

Como a distribuição de pesos é univocamente determinada pelos coeficientes $\Omega_j(i)$, temos que $\mathcal{D}_P = \mathcal{D}_N$.

Proposição 3.2.6 (Hierárquico). *Sejam \mathcal{H} o poset hierárquico sobre $[n]$ e P um poset sobre $[n]$ tal que a DP do P -espaço (\mathbb{F}_q^n, d_P) coincide com a DP do \mathcal{H} -espaço $(\mathbb{F}_q^n, d_{\mathcal{H}})$, ou seja, $\mathcal{D}_{\mathcal{H}} = \mathcal{D}_P$. Então, P possui também a estrutura de hierárquico e conseqüentemente P é isomorfo a \mathcal{H} .*

Demonstração: Desde que \mathcal{H} contem n_1 elementos mínimos, pelo Lema 3.2.3 P também possui n_1 elementos mínimos. Dividimos a prova em várias afirmações, como segue.

- **Afirmção 1:** Vale a igualdade $N_2^P = \Lambda_1^P(n_1 + 1)$, ou seja, $i \in N_2^P$ se e somente se $|\langle i \rangle| = n_1 + 1$.

Com efeito, é claro que se $i \in N_2^P$, $2 \leq |\langle i \rangle| \leq n_1 + 1$. Suponhamos então que exista $i \in N_2^P$ com $|\langle i \rangle| = r$ onde $2 \leq r \leq n_1$. Como P possui n_1 elementos no primeiro nível temos que

$$A_{r,P} \geq \binom{n_1}{r} (q-1)^r + \alpha_r (q-1) q^{r-1}, \quad (1)$$

onde $\alpha_r := |\{i \in N_2^P : |\langle i \rangle| = r\}|$. No entanto, do exemplo 3.1.5 sabemos

$$A_{j,P} = \binom{n_{l+1}}{j - k_l} (q-1)^{j-k_l} q^{k_l} \quad \text{para } k_l < j \leq k_{l+1}$$

onde $k_l = n_1 + n_2 + \dots + n_l$. Assim,

$$A_{r,P} = A_{r,\mathcal{H}} = \binom{n_1}{r} (q-1)^r$$

logo, da desigualdade (1) obtemos $\alpha = 0$, donde não existe tal i . Concluimos que se $i \in N_2^P$ então $|\langle i \rangle| = n_1 + 1$. Além disto se $i \in N_j^P$, $j > 2$ deve existir $i' \in N_2^P$ com $i' \preceq_P i$ donde $|\langle i \rangle| \geq |\langle i' \rangle| + j - 2 > n_1 + 1$. Mostrando assim nossa primeira afirmação.

Observamos em particular que

$$\Omega_1^P(2) = \dots = \Omega_1^P(n_1) = 0.$$

- **Afirmação 2:** Vale a igualdade $|N_2^{\mathcal{H}}| = |N_2^P|$.

Note inicialmente que $\Omega_2^P(n_1 + 1) = \dots = \Omega_{n_1+1}^P(n_1 + 1) = 0$. De fato, seja $I = \{i_1, \dots, i_{n_1+1}\}$ um ideal de P de cardinalidade $n_1 + 1$. Como $|I| > |N_1^P|$ existe ao menos um índice j tal que $i_j \in I$ e $i_j \notin N_1^P$. Note que, $i_j \in N_2^P$, pois do contrário existiria $k \in N_2^P$ tal que $k \preceq_P i_j$ e teríamos, $|I| \geq |\langle i_j \rangle_P| > |\langle k \rangle_P| = n_1 + 1$, um absurdo.

Suponhamos agora que exista $k \neq j$ tal que $i_k \in I \cap N_2^P$. Segue da Afirmação 1 que $|\langle i_k \rangle| = n_1 + 1$ logo, como $\langle i_k \rangle \cap \langle i_j \rangle \subset I$ segue que $|I| > n_1 + 1$ o que contradiz nossa hipótese, logo existe apenas um elemento máximo em I , e portanto, $I = \langle i_j \rangle$.

Mostramos assim que $\Omega_2^P(n_1 + 1) = \cdots = \Omega_{n_1+1}^P(n_1 + 1) = 0$ e, pela Afirmação 1,

$$\begin{aligned} A_{n_1+1,P} &= \Omega_1^P(n_1 + 1)(q - 1)q^{n_1} \\ &= |N_2^P|(q - 1)q^{n_1}. \quad (\text{por 1}) \end{aligned}$$

Como

$$\begin{aligned} A_{n_1+1,P} &= A_{n_1+1,\mathcal{H}} \\ |N_2^P|(q - 1)q^{n_1} &= n_2(q - 1)q^{n_1} \end{aligned}$$

segue que

$$|N_2^P| = n_2 = |N_2^{\mathcal{H}}|.$$

Vamos assumir que $|N_t^P| = |N_t^{\mathcal{H}}|$ e $N_t^P = \Lambda_1^P(k_{t-1} + 1)$ para todo $t \leq r$, como hipótese de indução para mostrar as duas afirmações seguintes.

- **Afirmação 3:** Vale a igualdade $N_{r+1}^P = \Lambda_1^P(k_r + 1)$, ou seja, se $i \in N_{r+1}^P$ então $|\langle i \rangle| = k_r + 1$.

De fato, se $i \in N_{r+1}^P$ então existe $j \in N_r^P$ com $j \in \langle i \rangle$. Como $j \in N_r$, usando a hipótese de indução,

$$|\langle j \rangle| = n_1 + \cdots + n_{r-1} + 1 = k_{r-1} + 1,$$

donde segue que

$$k_{r-1} + 2 \leq |\langle i \rangle| \leq k_{r-1} + n_r + 1.$$

Afim de mostrarmos que

$$|\langle i \rangle| = k_{r-1} + n_r + 1$$

suponhamos por absurdo que $|\langle i \rangle| < k_{r-1} + n_r + 1$ e seja s tal que $|\langle i \rangle| = k_{r-1} + s$ onde $s \in \{2, \dots, n_r\}$. Como

$$A_{k_{r-1}+s}^P \geq \binom{n_r}{s} (q-1)^s q^{k_{r-1}} + \Omega_1^P(k_{r-1} + s) (q-1) q^{k_{r-1}+s-1},$$

usando agora a hipótese $A_{k_{r-1}+s}^P = A_{k_{r-1}+s}^{\mathcal{H}} = \binom{n_r}{s} (q-1)^s q^{k_{r-1}}$, temos que $\Omega_1^P(k_{r-1} + s) = 0$ ou seja, não existe algum ideal de P de cardinalidade $(k_{r-1} + s)$ contendo 1 elemento maximal. Conseqüentemente, $|\langle a \rangle| = k_{r-1} + n_r + 1 = k_r + 1$. Além disto se $i \in N_j^P$, $j > r$ deve existir $i' \in N_r^P$ com $i' \preceq_P i$ donde $|\langle i \rangle| \geq |\langle i' \rangle| + j - r > k_r + 1$.

- **Afirmção 4:** Vale a igualdade $|N_{r+1}^{\mathcal{H}}| = |N_{r+1}^P|$

A argumentação usada aqui será a mesma que foi usada para mostrarmos a Afirmção 2. Começamos observando que

$$\Omega_2^P(k_r + 1) = \dots = \Omega_{k_r+1}^P(k_r + 1) = 0 \quad (3.4)$$

De fato, considere $I = \{i_1, \dots, i_{k_r+1}\}$ um ideal de P de cardinalidade $k_r + 1$. Como $|I| > \sum_{s=1}^r |N_s^P|$ existe ao menos um $i_j \in I$ tal que $i_j \notin \bigcup_{s=1}^r N_s^P$. Note também que, $i_j \in N_{r+1}^P$, caso contrário, se $i_j \notin N_{r+1}^P \cup \bigcup_{s=1}^r N_s^P$ então existiria $l \in N_{r+1}^P$ tal que $l \in \langle i_j \rangle$ e como (pela Afirmção 3) $|\langle l \rangle| = k_r + 1$ seguiria que $|\langle i_j \rangle| > k_r + 1$ donde $|I| > k_r + 1$, um absurdo.

Suponhamos agora que exista $k \neq j$ tal que $i_k \in I \cap N_{r+1}^P$. Da Afirmção 3, $|\langle i_k \rangle| = k_r + 1$ logo, como $\langle i_k \rangle \cup \langle i_j \rangle \subset I$ segue que $|I| > k_r + 1$, o que contradiz nossa hipótese; logo existe apenas um elemento máximo em I , e portanto, $I = \langle i_j \rangle$. Isso demonstra as igualdades em (3.4).

Temos então que:

$$\begin{aligned} A_{k_r+1,P} &= \Omega_1^P(k_r + 1)(q - 1)q^{k_r} \\ &= |N_{r+1}^P|(q - 1)q^{k_r}. \end{aligned}$$

E ainda, como $A_{k_r+1,P} = A_{k_r+1,\mathcal{H}} \stackrel{\text{por 3.1.5}}{=} n_{r+1}(q - 1)q^{k_r}$, segue que $|N_{r+1}^P| = n_{r+1} = |N_{r+1}^{\mathcal{H}}|$.

Observe agora que as Afirmações 3 e 4 são suficientes para mostrar que P é isomorfo a \mathcal{H} . Com efeito, na Afirmação 3 mostramos que

$$P = N_1^P \oplus N_2^P \oplus \cdots \oplus N_{t'}^P,$$

enquanto que na observação 4 obtemos que cada nível de P possui a mesma cardinalidade que o nível correspondente em \mathcal{H} . Note também que da observação 4 segue que P possui tantos níveis quanto o poset \mathcal{H} . Assim, é claro que \mathcal{H} e P são isomorfos, para tanto, basta notar que P pode ser obtido de \mathcal{H} a partir de uma bijeção (permutação), $\pi : \mathcal{H} \rightarrow P$ tal que $|\pi^{-1}(N_i^P)| = n_i = |N_i^{\mathcal{H}}|$.

□

3.3 Conjecturas (descartadas e mantidas)

Além dos casos apresentados na seção anterior, que configuram condições suficientes sobre P para o problema de distribuição de pesos, consideramos condições adicionais, como candidatas a ser hipótese de suficiência para o problema.

Uma condição foi a de termos dois posets P e Q com $\mathcal{D}_P = \mathcal{D}_Q$ e mesmos coeficientes $\Omega_j(i)$ (quantidade de ideais de cardinalidade i contendo exatamente j elementos maximais).

À essa primeira condição conseguimos obter uma resposta conclusiva, negativa, mas que no entanto, é apresentada na forma de um resultado que achamos ser interessante por si só.

A expressão 3.3 (página 39)

$$A_i^P = \sum_{j=1}^i \Omega_j^P(i)(q-1)^j q^{i-j},$$

nos revela que a distribuição de pesos de um espaço P -métrico depende do conjunto dos ideais de P e do corpo \mathbb{F}_q escolhido:

Imaginamos a princípio que a hipótese de dois posets terem a mesma quantidade de ideais com as características prescritas fosse suficiente para garantir o isomorfismo entre os posets, ou seja, imaginamos que $\Omega_j^P(i) = \Omega_j^Q(i)$ para todos i, j implicasse em termos $P \approx Q$. O resultado seguinte nos mostra que isso não vale e mais, não apenas a distribuição de pesos $\mathcal{D}_P = (A_1^P, \dots, A_n^P)$ é determinada por $\Omega_j^P(i)$ $i, j = 1, \dots, n$, como também determina estes coeficientes.

Teorema 3.3.1. *Dado um poset P , se Q é um poset que induz sobre \mathbb{F}_q^n , para todo corpo \mathbb{F}_q , a mesma distribuição de pesos determinada por P , então $\Omega_j^P(i) = \Omega_j^Q(i)$ para $i = 1, \dots, n$ e $1 \leq j \leq i$.*

Demonstração: Note inicialmente que a distribuição de pesos de \mathbb{F}_q^n induzida por P é

$$A_i^P = \sum_{j=1}^i \Omega_j^P(i)(q-1)^j q^{i-j} \tag{3.5}$$

e é uma função que depende essencialmente de $\Omega_j^P(i)$ (que provém de P) e de q (que depende apenas do corpo \mathbb{F}_q escolhido). Estendendo o binômio $(q-1)^j$ em

$$\sum_{k=0}^j \binom{j}{k} (-1)^k q^{j-k}$$

podemos rescrever (3.5) como

$$\sum_{j=1}^i \sum_{k=0}^j (-1)^k \binom{j}{k} \Omega_j^P(i) q^{i-k}.$$

Assim, se $A_i^P = A_i^Q$ para cada corpo \mathbb{F}_q então podemos analisar os A_i^Q como polinômios em q e então, da igualdade de polinômios, e denotando $\Omega_j^Q(i)$ por x_{ji} , segue que,

$$\sum_{j=1}^i (-1)^k \binom{j}{k} \Omega_j^P(i) = \sum_{j=1}^i (-1)^k \binom{j}{k} x_{ji}.$$

De onde obtemos o seguinte sistema homogêneo,

$$Ax^t = 0$$

onde, $A = (a_{kl})_{i+1 \times i}$ tal que $a_{kl} = (-1)^{k-1} \binom{l}{k-1}$ e $x = (x_{1i} - \Omega_1^P(i), x_{2i} - \Omega_2^P(i), \dots, x_{ii} - \Omega_i^P(i))$.

Observe que A é da forma:

$$A = (a_{kl})_{i+1 \times i} = \begin{bmatrix} \binom{1}{0} & \binom{2}{0} & \cdots & \binom{i}{0} \\ -\binom{1}{1} & -\binom{2}{1} & \cdots & -\binom{i}{1} \\ \vdots & \vdots & \cdots & \vdots \\ (-1)^{i+1} \binom{1}{i} & (-1)^{i+1} \binom{2}{i} & \cdots & (-1)^{i+1} \binom{i}{i} \end{bmatrix}_{i+1, i}.$$

Como $\binom{l}{k-1} = 0$ para $l < k-1$ e $\binom{l}{k-1} = 1$ para $l = k-1$ segue que $a_{kl} = 0$ para $l < k-1$ e $a_{kl} = (-1)^{k-1}$ para $l = k-1$. Temos então que a

matriz A é na verdade:

$$A = (a_{kl})_{i+1 \times i} = \begin{bmatrix} \binom{1}{0} & \binom{2}{0} & \cdots & \binom{i}{0} \\ -1 & -\binom{2}{1} & \cdots & -\binom{i}{1} \\ 0 & 1 & \cdots & \binom{i}{2} \\ \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & (-1)^{i+1} \end{bmatrix}_{i+1, i} .$$

Note que a primeira linha da matriz A é combinação linear das demais linhas, que são claramente linearmente independentes, assim podemos retirar deste sistema a primeira linha sem alterar a sua solução.

O novo sistema obtido possui i linhas linearmente independentes donde se obtém que o sistema possui apenas a solução trivial. Com efeito, a matriz $B = (b_{kl})_{i \times i}$ obtida é triangular superior com 1's e -1's na diagonal, pois $b_{kj} = (-1)^k \binom{j}{k} = 0$ para $k > j$ e $a_{kk} = (-1)^k \binom{k}{k} = 1$, ou seja,

$$B = (b_{kl})_{i \times i} = \begin{bmatrix} -1 & -\binom{2}{1} & \cdots & -\binom{i}{1} \\ 0 & 1 & \cdots & \binom{i}{2} \\ \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & (-1)^i \end{bmatrix}_{i, i} .$$

Sendo assim, o determinante de B é não nulo e dessa forma o sistema $Bx^t = 0$ possui apenas a solução trivial $x = 0$. Portanto, $x_{ji} = \Omega_j(i)$ é a única solução do sistema. \square

3.3.1 Conjectura assumindo a hipótese de reconstrução

Suspeitamos que o problema da determinação de ordem via distribuição de pesos esteja relacionado com o problema de “reconstrução de ordem” (ver

[13]), um problema que surgiu inicialmente para grafos no final da década de 70 e mais tarde foi introduzido na teoria de conjuntos parcialmente ordenados (veja [14] e [15] para mais detalhes da história do problema).

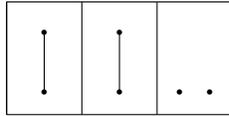
Dado um poset P sobre $[n]$, a *plataforma* de P é a família, $(P - \{i\})_{i \in P}$ de subposets de P obtidos retirando-se de $[n]$ o elemento i e todas as relações que o envolvem. Cada elemento da plataforma será chamado *carta*. Um poset P é dito *reconstrutível* se, dado um poset Q com mesma plataforma de P , então P e Q são isomorfos, ou seja, se existe uma bijeção $\sigma : P \rightarrow Q$ tal que para cada $i \in P$ temos que $P - \{i\}$ é isomorfo a $Q - \{\sigma(i)\}$ então $Q \approx P$ (e neste caso é possível escolher σ como um isomorfismo de ordem). Diversos artigos vem sendo publicados desde 1985 com contra-exemplos para o caso geral e a solução deste problema para diversas classes particulares de ordens. O artigo [16] de Rampon (2005) oferece um panorama amplo e relativamente atual sobre o problema de reconstrução de ordem.

As quatro classes de posets, anticadeia, cadeia, coroa e hierárquico, que mostramos garantir uma resposta positiva ao problema de distribuição de pesos, são classes de posets *reconstrutíveis*, o que pode ser demonstrado utilizando-se os teoremas 27, 30 e 32 de [16]. Além disto, todos os contra-exemplos que obtivemos de posets que não garantem isomorfismos apenas a partir da distribuição de pesos são posets não *reconstrutíveis*. O contra-exemplo 3.2.1 apresentado na seção 3.2 tem ainda a seguinte peculiaridade: os posets N e P tem a mesma distribuição de pesos mas plataformas diferentes.

Também existem exemplos nos quais ocorre o contrário: os posets cujos diagramas de Hasse são



tem a mesma plataforma, a saber,



mas distribuições de pesos distintas.

Tudo isto nos leva a formular duas conjecturas que parecem plausíveis, possíveis de serem abordadas em trabalho futuro.

Conjectura 3.3.2. *Dado P um poset sobre $[n]$, se P é reconstrutível e $A_P(k) = A_Q(k)$ para todo $k = 1, \dots, n$, então $P \approx Q$.*

Uma conjectura mais fraca que esta é a seguinte:

Conjectura 3.3.3. *Dados P, Q dois posets sobre $[n]$, se $\mathcal{D}_Q = \mathcal{D}_P$ e P e Q possuem a mesma plataforma, isto é, se Q é uma reconstrução de P , então $P \approx Q$.*

Referências Bibliográficas

- [1] R. Brualdi, J. S. Graves e M. Lawrence, *Codes with a poset metric*, Discrete Mathematics 147 (1995) 57-72.
- [2] H. Niederreiter, *Point sets and sequences with small discrepancy*, Discrete Math. 104 (1987) 273-337.
- [3] H. Niederreiter, *A combinatorial problem for vector spaces over finite fields*, Discrete Math. 96 (1991) 221-228.
- [4] H. Niederreiter, *Orthogonal arrays and other combinatorial aspects in the theory of uniform point distributions in unit cubes*, Discrete Math. 106-107 (1992) 361-367.
- [5] M. Yu Rosenbloom e M. A. Tsfasman, *Codes for the m -metric*, Probl. Inf. Transm. 33 (1997) 45-52.
- [6] D. S. Kim e S. H. Cho, *Weight distribution of the crown-weight space*, European Journal of Combinatorics. Volume 28, Issue 1, January (2007), 356-370.
- [7] D. S. Kim e S. H. Cho, *Automorphism group of the crown-weight space*, European Journal of Combinatorics. Volume 27, Issue 1, (2006), 90-100.

- [8] K. Lee, *Automorphism group of the Rosenbloom-Tsfasman space*, European Journal of Combinatorics. Volume 24, (2003), 607-612.
- [9] L. Panek, M. Firer, H. K. Kim e J. Y. Hyun, *Groups of linear isometries on poset structures*, Discrete Mathematics. 308 (2008) 4116-4123.
- [10] A. Hefez e M. L. T. Villela, *Códigos Corretores de Erros*, Rio de Janeiro, IMPA, (2002).
- [11] H. K. Kim e D. Y. Oh, *A classification of Posets Admitting the MacWilliams identity*, IEEE Transactions on Information Theory, Vol. 51, No. 4, (2005).
- [12] C. E. Shannon, *A mathematical theory of communication*, Bell Systems Technical Journal 27 (1948) 379-423. 623-656.
- [13] D. Kratsch e J. X. Rampon, *Towards the reconstruction of posets*, Order 11 (4), (1994), 317-341.
- [14] C.St.J.A. Nash-Williams, *The reconstruction problem*, Selected Topics in Graph theory, Vol.1, New York, (1978), 205-236.
- [15] J.A. Bondy e R.L. Hemminger, *Graph reconstruction - a survey*, Journal of Graph Theory **1**, (1977), 227-268.
- [16] J. X. Rampon, *What is reconstruction for ordered set*, Discrete Mathematics. Volume 291, Issues 1-3, (2005), 191-233.
- [17] J. Neggers e H.S. Kim, *Basic Posets*, World Scientific, (1998).