UNIVERSIDADE FEDERAL DE VIÇOSA

Conexão de Galois e os tipos de dualidade de Wei

Suzana Carletti Machado
Magister Scientiae

VIÇOSA - MINAS GERAIS
2026

SUZANA CARLETTI MACHADO

Conexão de Galois e os tipos de dualidade de Wei

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

Orientador: Allan de Oliveira Moura

VIÇOSA - MINAS GERAIS
2026

Ficha catalográfica elaborada pela Biblioteca Central da Universidade Federal de Viçosa - Campus Viçosa

T
M149c
2026

Machado, Suzana Carletti, 2002-
Conexão de Galois e os tipos de dualidade de Wei / Suzana Carletti Machado. – Viçosa, MG, 2026.
1 dissertação eletrônica (54 f.): il. (algumas color.).

Orientador: Allan de Oliveira Moura.
Dissertação (mestrado) - Universidade Federal de Viçosa, Departamento de Matemática, 2026.
Referências bibliográficas: f. 53-54.
DOI: https://doi.org/10.47328/ufvbbt.2026.199
Modo de acesso: World Wide Web.

1. Matróides. I. Moura, Allan de Oliveira , 1980-. II. Universidade Federal de Viçosa. Departamento de Matemática. Programa de Pós-Graduação em Matemática. III. Título.

CDD 22. ed. 511.6

Bibliotecário(a) responsável: Euzébio Luiz Pinto CRB-6/3317

SUZANA CARLETTI MACHADO

Conexão de Galois e os tipos de dualidade de Wei

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

APROVADA: 26 de fevereiro de 2026.

Assentimento:

_____

Suzana Carletti Machado
Autora

_____

Allan de Oliveira Moura
Orientador

AGRADECIMENTOS

Em primeiro lugar, não poderia deixar de agradecer a Deus, por me dar força, saúde e amparo em todos os momentos em que estive em Viçosa. Agradeço à Maria Santíssima pela intercessão e acolhimento nesse período. À Santa Terezinha, São Carlo Acutis, Santo Tomás de Aquino e São Josemaria Escrivá, que mais me ouviram nesse tempo.

Agradeço imensamente aos meus pais Rosa e Edivaldo, que sempre me apoiaram em todas as minhas decisões, por todo amor, carinho, compreensão e acalento e por me levarem para outra cidade, de madrugada, todas as vezes que precisava voltar à Viçosa. Agradeço às minhas irmãs Ester e Gabryella, por ficarem felizes pelas minhas conquistas e acreditarem no meu esforço.

Também não posso deixar de agradecer ao meu companheiro, Andrico, que esteve comigo e segurou minha mão, mesmo de longe. Me acalmou, me fortaleceu e celebrou minhas conquistas comigo. Sou grata por sempre estar ao meu lado e por acreditar em mim.

Quero expressar minha gratidão também aos meus amigos que fiz nesse período. Às que vieram comigo da graduação: Paola e Jadyele, e também aos que fiz durante estes dois anos de mestrado. Meu profundo agradecimento à Rebeca, Érik, Luiz, João Paulo, Pedro, Lucas e aos membros do JUSC, vocês fizeram tudo ser mais leve e possível para mim.

Agradeço ao meu orientador Allan de Oliveira Moura, por me proporcionar uma experiência incrível na pesquisa, por estar sempre presente e me dar todo o amparo necessário. Por toda paciência, compreensão e por me dar todas as ferramentas essenciais para concluir este trabalho. Além disso, também agradeço à banca examinadora pelas contribuições para o enriquecimento desta dissertação.

Por fim, agradeço a todos que participaram direta e indiretamente da produção deste trabalho e ao departamento de matemática da Universidade Federal de Viçosa.

Este trabalho foi realizado com o apoio das seguintes agências de pesquisa brasileiras: Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Código de Financiamento 001, Fundação de Amparo à Pesquisa do Estado de Minas Gerais (FAPEMIG) e Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq).

Queres de verdade ser santo? - Cumpre o pequeno dever de cada momento; faz o que deves e está no que fazes."

São Josemaria Escrivá.

RESUMO

MACHADO, Suzana Carletti, M.Sc., Universidade Federal de Viçosa, fevereiro de 2026. **Conexão de Galois e os tipos de dualidade de Wei**. Orientador: Allan de Oliveira Moura.

O famoso Teorema de Dualidade de Wei, apresentado em 1991, estabeleceu uma relação determinística entre os pesos generalizados de Hamming de um código linear e os de seu código dual. Posteriormente, foi-se observado que esta dualidade ocorre de forma intrínseca quando se tem pesos generalizados de Hamming e perfis de dimensão/comprimento de um código linear. Nesta dissertação, apresentaremos a conexão de Galois entre subconjuntos finitos de Z, o qual usaremos para decifrar esta forma intrínseca, uma dualidade do tipo Wei para matroides, demi-matroides, w-demi matroides e w-demi polimatroides.

Palavras-chave: conexão de Galois; dualidade de Wei; w-demi matroides; w-demi polimatroides

ABSTRACT

MACHADO, Suzana Carletti, M.Sc., Universidade Federal de Viçosa, February, 2026. **Galois connection and Wei´s duality types**. Adviser: Allan de Oliveira Moura.

The famous Wei's Duality Theorem, presented in 1991, established a deterministic relationship between the generalized Hamming weights of a linear code and those of its dual code. Subsequently, it was observed that this duality occurs intrinsically when dealing with generalized Hamming weights and dimension/length profiles of a linear code. In this dissertation, we will present the Galois connection between finite subsets of Z, which we will use to decipher this intrinsic form, a Wei-type duality for matroids, demi-matroids, w-demi matroids, and w-demi polymatroids.

Keywords: Galois connection; Wei duality; w-demi matroids; w-demi polymatroids

Lista de ilustrações

Sumário

1 Introdução

Em 1991, Victor K. Wei [19], motivado por aplicações na teoria de informação e segurança, conduziu um estudo da estrutura algébrica de códigos lineares, considerando o peso mínimo de Hamming como uma propriedade mínima de subcódigos unidimensionais, obtendo uma noção generalizada de pesos de Hamming de dimensões superiores para códigos lineares. A motivação original de Wei, foi um esquema de codificação linear para o Canal de Escuta do Tipo II, [14]. Wei também criou técnicas para encontrar tais pesos generalizados e a mais famosa delas é a Dualidade de Wei.

De modo preciso, o citado Canal de Escuta do Tipo II se caracteriza por um cenário composto pelo remetente, prestes a enviar uma mensagem ao destinatário; o destinatário, disposto a receber a mensagem enviada; o canal, por onde esta mensagem será transmitida, e por fim; o adversário, que tem por objetivo, obter as informações contidas na mensagem enviada. O remetente tem k bits de informação para transmitir ao destinatário por meio de m usos do canal. O adversário pode ouvir quaisquer s bits de sua escolha. O foco do problema é evitar que o adversário obtenha informações em excesso.

Para discutirmos a dualidade encontrada por Wei, precisaremos de conceitos importantes. Um conceito de extrema importância a ser utilizado aqui, é o de conexão de Galois. O termo "Conexão de Galois", deriva possivelmente do fato de uma das mais famosas conexões de Galois, ser, justamente, a correspondência de Galois entre os corpos intermediários de uma extensão $\mathbb{K}/\mathbb{F}$ e os subgrupos do grupo de Galois, $\mathrm{Gal}(\mathbb{K}/\mathbb{F})$, conectados por uma conexão de Galois. Neste trabalho, estamos interessados em conexões de Galois entre subconjuntos finitos de $\mathbb{Z}$ com respeito à ordem usual.

Com isso, o objetivo principal deste trabalho é apresentar um estudo que relaciona a conexão de Galois entre conjuntos finitos e a dualidade de Wei. Partindo da observação de que o peso generalizado e o perfil de dimensão/comprimento formam uma conexão de Galois, conseguimos relacionar duas conexões deste tipo a uma dualidade do tipo Wei. Além disso, apresentaremos aplicações deste resultado em estruturas como w-demi matroides e w-demi polimatroides, com $w \in \mathbb{Z}^+$. Durante todo o texto, consideraremos $\mathbb{N} = \mathbb{Z}^+ \cup \{0\}$ e para quaisquer $a, b \in \mathbb{Z}$, usaremos $[a, b]$ para definir o conjunto de todos os números inteiros entre a e b, incluindo os extremos. Aqui, apesar de não apresentarmos resultados novos, muitas demonstrações foram acrescentadas para melhor entendimento do texto.

No primeiro capítulo, exploraremos alguns conceitos que serão fundamentais para a construção de uma base teórica dos resultados principais. Desse modo, veremos definições de códigos lineares, pesos generalizados de Hamming e perfis de dimensão/comprimento

de códigos lineares, conexão de Galois, matroides e demi-matroides. Uma das finalidades deste capítulo, além de introduzir alguns conceitos nem sempre discutidos, é a de darmos uma motivação para o resultado central deste trabalho: a conexão de Galois existente envolvendo o peso generalizado e o perfil de dimensão/comprimento de um código linear.

No segundo capítulo, estabeleceremos condições necessárias para enunciarmos o Teorema Central deste trabalho, o qual cria uma relação a partir de duas conexões de Galois entre conjuntos finitos e a dualidade de Wei, o enunciaremos e apresentaremos uma demonstração para o mesmo. Ainda, neste capítulo, estabeleceremos condições necessárias para enunciarmos o Teorema da Ponte, o qual será de grande auxílio para as aplicações do Teorema Central, também o enunciaremos e assim como para o Teorema Central, apresentaremos uma demonstração para o mesmo.

Por fim, no terceiro e último capítulo, veremos aplicações do Teorema Central para w-demi matroides sobre conjuntos finitos e w-demi polimatroides sobre módulos com série de composições. Aqui, estabeleceremos as condições necessárias para enunciarmos os teoremas de cada aplicação, os enunciaremos e apresentaremos demonstrações para os respectivos.

2 Preliminares

Para uma melhor leitura deste trabalho, é preciso que façamos um apanhado geral, quanto a alguns conceitos necessários para o desenvolvimento do mesmo. Neste capítulo, o objetivo principal é apresentá-los, pois serão de grande importância a posteriori. Apresentaremos, aqui, códigos lineares, pesos generalizados de Hamming e perfis de dimensão/comprimento de um código linear, um pouco da teoria de matroides e demi-matroides e ainda, a conexão de Galois e suas contribuições para nosso estudo. As principais referências utilizadas foram [4],[9], [12], [13], [18], [19] e [20].

2.1 Códigos Corretores de Erros

A teoria que envolve o estudo de códigos corretores de erros foi desenvolvida por C. E. Shannon, em 1948. Muitos pesquisadores se interessaram pelas pesquisas de C. E. Shannon, principalmente a partir dos anos 70, com o advento dos computadores. Atualmente, essa teoria é aplicada consideravelmente em transmissões e armazenamento de dados. Nesta seção, apresentaremos definições fundamentais de códigos corretores de erros. Em particular, veremos o que é um código linear e algumas ferramentas que serão utilizadas no decorrer deste trabalho envolvendo esses códigos.

Para construirmos um código, consideraremos um conjunto finito A, o qual chamaremos de *alfabeto* e cuja cardinalidade seja dada por um número q. Chamamos de *código corretor de erros*, um subconjunto próprio de A^m, em que m seja um inteiro positivo. Aqui, todos os elementos de A^m serão também chamados de *palavras*. Como o próprio nome já diz, o objetivo do nosso código é corrigir o máximo de erros possíveis gerados em transmissões de uma mensagem. Sendo assim, precisamos de uma ideia de distância entre palavras em A^m e, para isso, consideraremos a métrica de Hamming.

Definição 2.1.1. *Consideremos $\boldsymbol{a}, \boldsymbol{b} \in A^m$. Chamamos de distância de Hamming entre $\boldsymbol{a}$ e $\boldsymbol{b}$ o valor $d(\boldsymbol{a}, \boldsymbol{b})$ dado por*

$$d(\boldsymbol{a}, \boldsymbol{b}) = |\{i \in [1, m] \ \ tal\ que\ \ a_i \neq b_i\}|.$$

Exemplo 2.1.1. *Seja um código $C = \{0000, 1110, 1001\}$ sobre o conjunto $\mathbb{Z}_2^4$. Observemos o seguinte:*

$$\begin{aligned} d(0000, 1001) &= 2 \\ d(0000, 1110) &= 3 \\ d(1001, 1110) &= 3. \end{aligned}$$

Agora, para caracterizarmos a *métrica de Hamming*, consideraremos a proposição a seguir.

Proposição 2.1.1. *Ao considerarmos $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c} \in A^m$, as seguintes afirmações são válidas:*

(1) $d(\boldsymbol{a}, \boldsymbol{b}) \geq 0$, *em que* $d(\boldsymbol{a}, \boldsymbol{b}) = 0$ *se, e somente se,* $\boldsymbol{a} = \boldsymbol{b}$;

(2) $d(\boldsymbol{a}, \boldsymbol{b}) = d(\boldsymbol{b}, \boldsymbol{a})$;

(3) $d(\boldsymbol{a}, \boldsymbol{b}) \leq d(\boldsymbol{a}, \boldsymbol{c}) + d(\boldsymbol{c}, \boldsymbol{b})$.

Demonstração. A afirmação (1) deriva da própria definição de distância entre palavras, pois lidamos com uma contagem de coordenadas diferentes. Logo, $d(\mathbf{a}, \mathbf{b})$ resultará em um número não negativo. Agora, se $d(\mathbf{a}, \mathbf{b}) = 0$, então entre as palavras $\mathbf{a}$ e $\mathbf{b}$ não há coordenadas diferentes, ou seja, $\mathbf{a} = \mathbf{b}$. Por outro lado, se $\mathbf{a} = \mathbf{b}$, então as coordenadas de $\mathbf{a}$ são iguais às coordenadas de $\mathbf{b}$, o que os dá exatamente $d(\mathbf{a}, \mathbf{b}) = 0$.

Já para a afirmação (2), podemos ver que

$$\begin{aligned} d(\mathbf{a}, \mathbf{b}) &= |\{i \in [1, m] \text{ tal que } a_i \neq b_i\}| \\ &= |\{i \in [1, m] \text{ tal que } b_i \neq a_i\}| \\ &= d(\mathbf{b}, \mathbf{a}), \end{aligned}$$

como queríamos.

Por fim, em (3), consideraremos as i-ésimas coordenadas de $\mathbf{a}, \mathbf{b}$ e $\mathbf{c}$. Sendo assim, se $a_i = b_i$, então as coordenadas a_i e b_i contribuem 0 para $d(\mathbf{a}, \mathbf{b})$. Por outro lado, as i-ésimas coordenadas de $\mathbf{a}$, $\mathbf{b}$ e $\mathbf{c}$ contribuem 0, 1 ou 2 para $d(\mathbf{a}, \mathbf{c}) + d(\mathbf{c}, \mathbf{b})$, valor menor ou igual à contribuição de a_i e b_i em $d(\mathbf{a}, \mathbf{b})$. Agora, se $a_i \neq b_i$, é falso que $a_i = c_i$ e $c_i = b_i$. Dessa forma, as i-ésimas coordenadas de $\mathbf{a}$, $\mathbf{b}$ e $\mathbf{c}$, contribuem um valor maior ou igual a 1 para $d(\mathbf{a}, \mathbf{c}) + d(\mathbf{c}, \mathbf{b})$, número maior ou igual à contribuição de a_i e b_i em $d(\mathbf{a}, \mathbf{b})$. Portanto, a afirmação é válida. □

A seguir, veremos uma definição de códigos lineares e outros conceitos essenciais para este trabalho, a partir desses códigos. Consideraremos que o leitor já possua um conhecimento em elementos básicos da álgebra linear e corpos finitos.

Definição 2.1.2. *Seja um corpo finito, $\mathbb{F}_q$, com q elementos. Chamamos C de um código linear (m, k) sobre $\mathbb{F}_q$, se C é um $\mathbb{F}_q$-subespaço vetorial de $\mathbb{F}_q^m$ de dimensão k.*

Definição 2.1.3. *Chamamos de subcódigo linear de um código linear C (m,k), o código D (m,r), com $r \leq k$, em que D seja um subespaço vetorial de C.*

Definição 2.1.4. *Para $\boldsymbol{x} \in \mathbb{F}_q^m$, chamaremos de peso de $\boldsymbol{x}$ o seguinte valor:*

$$\omega(\boldsymbol{x}) = |\{i \in [1, m] \text{ tal que } x_i \neq 0\}|.$$

Podemos observar que, o peso de uma palavra $\mathbf{x}$ de um código é o mesmo quando pensamos na distância entre $\mathbf{x}$ e 0.

Definição 2.1.5. *Dado um código linear C (m,k), a matriz $k \times m$, a qual as linhas são os elementos de uma base de C, é chamada matriz geradora de C.*

Definição 2.1.6. *Chamamos de código linear dual ao código C (m,k), o código $C^{\perp}$ $(m, m-k)$, definido por*

$$C^{\perp} = \{\boldsymbol{x} \in \mathbb{F}^m \ \ tal\ que\ \ \boldsymbol{x} \cdot \boldsymbol{y} = 0, \ \ para\ todo\ \boldsymbol{y} \in C\},$$

em que $\boldsymbol{x} \cdot \boldsymbol{y} = x_1 \cdot y_1 + \cdots + x_m \cdot y_m$.

Definição 2.1.7. *A matriz geradora de $C^{\perp}$ é chamada de matriz teste de paridade de C,.*

Exemplo 2.1.2. *Consideremos o código linear C $(4,2)$ sobre o corpo finito $\mathbb{Z}_2$, dado por:*

$$C = \{0000, 1000, 0001, 1001\}.$$

C é subespaço de $\mathbb{Z}_2^4$ de dimensão 2. De fato, sejam $a, b \in C$ e $\lambda \in \mathbb{Z}_2$. Observemos que existem duas opções para λ, isto é, se $\lambda \in \mathbb{Z}_2$, então $\lambda = 0$ ou $\lambda = 1$. Logo, se $\lambda = 0$, então $a + \lambda b = a \in C$. Agora, no caso em que $\lambda = 1$, teremos $a + \lambda b = a + b$, soma pertencente a C. Observemos que a matriz geradora de C é a matriz:

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

Agora, consideremos o conjunto $D = \{0000, 1001\}$. D é subespaço vetorial de C de dimensão 1, logo, D é um subcódigo linear $(4,1)$ de C.

Para exemplificarmos o peso de uma palavra, consideremos a palavra 1101 em $\mathbb{Z}_2^4$. O peso de 1101 é dado por:

$$\omega(1101) = |\{1, 2, 4\}| = 3.$$

Desse modo, é possível calcularmos todos os pesos das palavras de um código C em $\mathbb{Z}_2^4$.

Vejamos agora, o código dual a C, $C^{\perp}$. Consideremos uma palavra $abcd$ em $C^{\perp}$. Assim, observemos o seguinte:

$$\begin{aligned} abcd \cdot 1000 &= a \cdot 1 + b \cdot 0 + c \cdot 0 + d \cdot 0 = 0 \\ abcd \cdot 0001 &= a \cdot 0 + b \cdot 0 + c \cdot 0 + d \cdot 1 = 0. \end{aligned}$$

Como o conjunto $\{1000, 0001\}$ gera C, basta que analisemos somente estas duas palavras. Dessa forma, pelas equações acima, as posições referentes à a e a d em $C^{\perp}$, precisam ser

zero. Logo, $C^{\perp} = \{0000, 0010, 0100, 0110\}$ e a matriz teste de paridade de C é dada então por:

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

que é a matriz geradora de $C^{\perp}$.

Lema 2.1.1. *Seja G a matriz geradora de um código linear $C \subset \mathbb{F}^m$. Então $C^{\perp}$ subespaço vetorial de $\mathbb{F}^m$ e*

$$\mathbf{x} \in C^{\perp} \quad \textit{se, e somente se,} \quad G\mathbf{x}^t = 0.$$

Demonstração. Sejam $\mathbf{s}$ e $\mathbf{t}$ elementos de $C^{\perp}$ e $\lambda \in \mathbb{F}$. Considerando $\mathbf{x} \in C$, observemos o seguinte:

$$(\mathbf{s} + \lambda\mathbf{t}) \cdot \mathbf{x} = \mathbf{s} \cdot \mathbf{x} + \lambda(\mathbf{t} \cdot \mathbf{x}) = 0.$$

Com isso, vemos que $\mathbf{s} + \lambda\mathbf{t}$ é um elemento de $C^{\perp}$, o que nos dá $C^{\perp}$ como um subespaço de $\mathbb{F}^m$. Agora, sabemos que se $\mathbf{x} \in C^{\perp}$, então $\mathbf{x}$ é ortogonal a todos os elementos de C, em particular, às linhas de G e, logo, $G\mathbf{x}^t = 0$. Por outro lado, se $G\mathbf{x}^t = 0$, então $\mathbf{x}$ é ortogonal a todos os elementos de C e, logo, $\mathbf{x} \in C^{\perp}$. □

Lema 2.1.2. *Para um código linear C (m, k) sobre $\mathbb{F}$, obtemos*

$$\dim_{\mathbb{F}}(C) + \dim_{\mathbb{F}}(C^{\perp}) = m.$$

Ou seja, a soma das dimensões de um código C e de seu código dual $C^{\perp}$, resulta no comprimento de ambos os códigos.

Demonstração. Consideremos uma transformação linear $T : \mathbb{F}_q^m \to \mathbb{F}_q^k$ definida por $T(\mathbf{x}) = G\mathbf{x}^t$, de modo que G seja a matriz geradora do código C. Pelo Lema 2.1.1, $\mathrm{Ker}(T) = C^{\perp}$. Além disso, temos $k = \dim(C) = \dim(\mathrm{Im}(T)) = \textit{posto}(G)$. Desse modo, pelo Teorema do Núcleo e da Imagem, obtemos

$$\begin{aligned} \dim_{\mathbb{F}}(\mathbb{F}^m) = \dim_{\mathbb{F}}(\mathrm{Nuc}(T)) + \dim_{\mathbb{F}}(\mathrm{Im}(T)) &\iff \dim_{\mathbb{F}}(\mathbb{F}^m) = \dim_{\mathbb{F}}(C^{\perp}) + \dim_{\mathbb{F}}(C) \\ &\iff m = \dim_{\mathbb{F}}(C^{\perp}) + \dim_{\mathbb{F}}(C), \end{aligned}$$

como queríamos. □

2.2 Peso generalizado de Hamming e perfil de dimensão/comprimento

Nesta seção, apresentaremos definições de peso generalizado de Hamming e perfis de dimensão/comprimento para um código linear C (m, k), como uma motivação para o resultado central deste trabalho. Aqui, veremos a dualidade de Wei obtida para pesos generalizados de Hamming, e exemplos dessa dualidade em um código linear $(3, 2)$ com pesos generalizados de Hamming e perfis de dimensão/comprimento.

Definição 2.2.1. *Seja C um código linear (m,k) sobre um corpo $\mathbb{F}_q$. Chamamos de suporte de um elemento $\alpha = (\alpha_1, \ldots, \alpha_m) \in C$, o conjunto, denotado por* $\mathrm{supp}(\alpha)$*, definido por*

$$\mathrm{supp}(\alpha) = \{i \in [1,m] \ \ tal\ que \ \ \alpha_i \neq 0\}.$$

Além disso, o suporte de um conjunto A de $\mathbb{F}_q^m$, é dado por $\mathrm{supp}(A) = \bigcup_{a\in A} \mathrm{supp}(a)$.

Observemos que o suporte de uma palavra α em C, coincide com o suporte do subespaço gerado por α. Desse modo, podemos definir os pesos generalizados de Hamming de um código linear C (m,k). Vale ressaltar que a próxima definição também se aplica ao código $(m, m-k)$ dual a C, $C^{\perp}$.

Definição 2.2.2. *Para qualquer $r \in [0,k]$, definimos o r-ésimo peso generalizado de Hamming de C, denotado por $d_r(C)$, como*

$$d_r(C) = \min\{|\,\mathrm{supp}(D)| \ \ tal\ que \ \ D \ é\ um\ subcódigo\ (m,r)\ de\ C\}.$$

Como observado anteriormente, para todo $\alpha \in \mathbb{F}_q^m$, $\mathrm{supp}(\alpha) = \mathrm{supp}(\langle\alpha\rangle)$, em que $\langle\alpha\rangle$ denota o subespaço gerado por α. Assim,

$$\begin{aligned}
\mathrm{d}_1(C) &= \{|\,\mathrm{supp}(D)| \ \text{tal que} \ \ D \text{ é um subcódigo } (m,1) \text{ de } C\} \\
&= \{|\,\mathrm{supp}(\langle\alpha\rangle)| \ \text{tal que} \ \ \alpha \neq 0 \text{ e } \alpha \in C\} \\
&= \{|\,\mathrm{supp}(\alpha)| \ \text{tal que} \ \ \alpha \neq 0 \text{ e } \alpha \in C\} \\
&= \{\omega(\alpha) \ \text{tal que} \ \ \alpha \neq 0 \text{ e } \alpha \in C\}\}
\end{aligned}$$

Desse modo, o peso generalizado de um subespaço gerado por uma palavra de C, coincide com o peso desta palavra.

Os pesos generalizados de Hamming têm sido utilizados em avaliações do desempenho de segurança de códigos lineares, no que se diz respeito a uma conexão segura em redes ou armazenamento de dados, [20]. Em [19], Wei provou um teorema de dualidade conectando os pesos generalizados de C e de $C^{\perp}$, dada pelos conjuntos

$$\mathcal{A} = \{\mathrm{d}_r(C) \ \ \text{tal que} \ \ r \in [1,k]\}, \quad \text{e} \quad \mathcal{B} = \{m+1-\mathrm{d}_r(C^{\perp}) \ \ \text{tal que} \ \ r \in [1,m-k]\}.$$

Percebemos então, que tais conjuntos formam uma partição do conjunto de coordenadas $[1,m]$, de modo que, tendo todos os pesos generalizados do código C, é possível obter, imediatamente, todos os pesos generalizados do código $C^{\perp}$. Estes conjuntos determinam um ao outro.

Exemplo 2.2.1. *Consideremos o código linear sobre $\mathbb{Z}_2$, gerado pela seguinte matriz:*

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

Queremos encontrar todos o pesos generalizados de Hamming do código C e os de seu código dual, $C^{\perp}$.

Aqui, nosso conjunto de coordenadas é $[1,m] = \{1,2,3\}$ e o código C tem dimensão $k = 2$. A partir de nossa matriz geradora, obtemos então, $C = \{000, 101, 100, 001\}$. Ao analisarmos $d_1(C)$, procuramos subcódigos de C de dimensão igual a 1. Dessa forma, examinaremos os seguintes subcódigos: $D_1 = \{000, 101\}$, $D_2 = \{000, 001\}$ e $D_3 = \{000, 100\}$. Agora, analisando o suporte de cada subcódigo, temos $\mathrm{supp}(D_1) = \{1,3\}$, $\mathrm{supp}(D_2) = \{3\}$ e $\mathrm{supp}(D_3) = \{1\}$. Calculando pois, a cardinalidade de cada suporte, vemos que $|\mathrm{supp}(D_1)| = 2$ e $|\mathrm{supp}(D_2)| = |\mathrm{supp}(D_3)| = 1$. Como desejamos o mínimo dessas cardinalidades, chegamos a $d_r(C) = 1$.

Agora, para $d_2(C)$, os sobcódigos de dimensão 2, resultam no próprio código C. Assim, $\mathrm{supp}(C) = \{1,3\}$, o que nos dá $|\mathrm{supp}(C)| = 2$ e, logo, $d_2(C) = 2$. Por fim, falta encontrarmos $d_1(C^{\perp})$. Pela dualidade de Wei, sabemos que os conjuntos

$$\mathcal{A} = \{d_1(C), d_2(C)\} = \{1,2\} \quad e \quad \mathcal{B} = \{m + 1 - d_1(C^{\perp})\}$$

formam uma partição de $[1,3]$. Dessa forma, $\mathcal{B} = \{m + 1 - d_1(C^{\perp})\} = \{3\}$, ou seja, $m + 1 - d_1(C^{\perp}) = 3$, o que nos dá $d_1(C^{\perp}) = 1$, uma vez que $\mathcal{A} \cup \mathcal{B} = [1,3]$ e $\mathcal{A} \cap \mathcal{B} = \emptyset$.

Veremos agora, uma definição para o perfil de dimensão/comprimento, que terá grande relação com o nosso estudo.

Definição 2.2.3. *Para qualquer $l \in [0,m]$, denotamos por $K_l(C)$, o l-ésimo perfil de dimensão/comprimento de C definido como*

$$K_l(C) = \max\{\dim_{\mathbb{F}}(C \cap \delta(J)) \ \ tal\ que \ \ J \subseteq [1,m],\ |J| = l\},$$

em que, para qualquer $J \subseteq [1,m]$, $C \cap \delta(J)$ é um subcódigo de C, cujo $\delta(J)$ denota todos os elementos de $\mathbb{F}^m$, cujas coordenadas fora de J sejam iguais a zero, isto é, $\delta(J) = \{\alpha \in \mathbb{F}^m \ \ tal\ que \ \ \forall i \in [1,m] - J,\ \alpha_i = 0\}$.

Em [8], Forney mostrou que $\mathrm{K}_l(C^{\perp}) = \mathrm{K}_{m-l}(C) + l - k$ para todo $l \in [0,m]$, determinando uma nova dualidade do tipo Wei entre um código linear e seu dual.

Exemplo 2.2.2. *Retomando o exemplo anterior, temos um código $C = \{000, 101, 100, 001\}$ de dimensão $k = 2$, em que $[1,m] = \{1,2,3\}$.*

Vejamos que, se $l = 1$, então $|J| = 1$. Assim, se $J = \{1\}$, então $C \cap \delta(J) = \{000, 100\}$. Agora, se $J = \{2\}$, então $C \cap \delta(J) = \{000\}$. Por fim, se $J = \{3\}$, então $C \cap \delta(J) = \{000, 001\}$. De modo que $K_1(C) = 1$.

Já se $l = 2$, então $|J| = 2$. E assim, se $J = \{1,2\}$, então $C \cap \delta(J) = \{000, 100\}$. Agora, se $J = \{2,3\}$, então $C \cap \delta(J) = \{000, 001\}$. Por fim, $J = \{1,3\}$, então $C \cap \delta(J) = C$. De modo que $K_2(C) = 2$.

Por outro lado, vemos que $K_1(C^\perp) = K_{3-1}(C) + 1 - 2 = 1$. *Observemos pois, que os conjuntos*

$$\mathcal{A} = \{K_1(C), K_2(C)\} = \{1, 2\} \quad e \quad \mathcal{B} = \{3 + 1 - K_1(C^\perp)\} = \{3\}$$

formam uma partição de $[1, 3]$*:* $\mathcal{A} \cup \mathcal{B} = [1, 3]$ *e* $\mathcal{A} \cap \mathcal{B} = \emptyset$.

2.3 Conexão de Galois

Nesta seção, veremos uma definição de uma conexão de Galois e estabeleceremos uma relação entre pesos generalizados de Hamming e perfis de dimensão/comprimento por meio de uma conexão de Galois. Aqui, estamos interessados em conexões entre subconjuntos finitos de $\mathbb{Z}$ com respeito à ordem usual. Dito isto, consideremos P e Q subconjuntos, não vazios, de $\mathbb{Z}$ e vejamos uma definição de uma conexão de Galois entre P e Q.

Definição 2.3.1. *Dados* $T : P \to Q$ *e* $S : Q \to P$, *o par ordenado* (T, S) *é dito uma conexão de Galois entre* P *e* Q *se satisfazem as seguintes condições:*

(1) *Para quaisquer* $a, b \in P$ *e* $c, d \in Q$, *com* $a \leq b$ *e* $c \leq d$, *verifica-se:* $T(a) \leq T(b)$ *e* $S(c) \leq S(d)$, *respectivamente;*

(2) *Para qualquer* $(a, c) \in P \times Q$, *verifica-se:* $a \leq S(c) \iff T(a) \leq c$.

Exemplo 2.3.1. *As funções* $T : [0, 5] \to [0, 10]$ *e* $S : [0, 10] \to [0, 5]$ *definidas por* $T(x) = 2x$ *e* $S(x) = \lfloor x/2 \rfloor$ *formam uma conexão de Galois. De fato, é fácil verificar que* (T, S) *cumprem o item* (1), *pois ambas funções* T *e* S *são crescentes. Além disso, considerando* $(a, c) \in [0, 5] \times [0, 10]$ *observemos que*

$$a \leq S(c) \iff a \leq \lfloor c/2 \rfloor \iff 2a \leq 2\lfloor c/2 \rfloor \leq c \iff T(a) \leq c.$$

Os resultados seguintes sobre a conexão de Galois, serão utilizados com certa frequência nos próximos capítulos.

Lema 2.3.1. *Seja* (T, S) *uma conexão de Galois entre* P *e* Q. *Então, as seguintes afirmações são válidas:*

(1) *Para qualquer* $\lambda \in P$, $T(\lambda) = \min\{b \ \ tal\ que \ \ b \in Q,\ \lambda \leq S(b)\}$;

(2) *Para qualquer* $\mu \in Q$, $S(\mu) = \max\{a \ \ tal\ que \ \ a \in P,\ T(a) \leq \mu\}$;

(3) *Seja* $d_0 = \min(Q)$. *Então* $T^{-1}(d_0) = \{a \ \ tal\ que \ \ a \in P,\ a \leq S(d_0)\}$;

(4) *Seja* $d \in Q$, *em que* $d \neq \min(Q)$, *e considere* $v = \max\{b \ \ tal\ que \ \ b \in Q,\ b \leq d - 1\}$. *Então, para qualquer* $a \in P$, *temos* $d = T(a)$ *se, e somente se,* $S(v) + 1 \leq a \leq S(d)$.

Demonstração. Primeiramente, vejamos que, como P e Q são subconjuntos finitos de $\mathbb{Z}$, as aplicações estão bem definidas. Agora, sigamos com as afirmações.

(1) Seja $\alpha = \min\{b \text{ tal que } b \in Q,\ \lambda \leq S(b)\}$. Assim, $\alpha \in Q$ e $\lambda \leq S(\alpha)$. Dessa forma, como (T, S) é conexão de Galois, temos $T(\lambda) \leq \alpha$. Por outro lado, como $T(\lambda) \leq T(\lambda)$, novamente por (T, S) ser conexão de Galois, temos $\lambda \leq S(T(\lambda))$, e logo, $\alpha \leq T(\lambda)$. Portanto, $T(\lambda) = \alpha$.

(2) Seja $\beta = \max\{a \text{ tal que } a \in P,\ T(a) \leq \mu\}$. Assim, $\beta \in P$ e $T(\beta) \leq \mu$. Dessa forma, como (T, S) é conexão de Galois, temos $\beta \leq S(\mu)$. Por outro lado, como $S(\mu) \leq S(\mu)$, novamente por (T, S) ser conexão de Galois, temos $T(S(\mu)) \leq \mu$, e logo, $S(\mu) \leq \beta$. Portanto, $S(\mu) = \beta$.

(3) Seja $a \in P$. Como (T, S) é conexão de Galois, então $a \leq S(d_0)$ se, e somente se, $T(a) \leq d_0$. E como $d_0 = \min(Q)$, obtemos $T(a) = d_0$.

(4) Considerando $T(a) = d$, temos $T(a) \leq d$. Assim, como (T, S) é conexão de Galois, temos

$$a \leq S(d). \tag{2.1}$$

Agora, se $a \leq S(v)$, temos, pela conexão de Galois, $d = T(a) \leq v$, contradizendo a definição de v, $v \leq d - 1$. Logo, $S(v) < a$, o que nos dá

$$S(v) + 1 \leq a. \tag{2.2}$$

Portanto, de 2.1 e 2.2, temos $S(v) + 1 \leq a \leq S(d)$.

Por outro lado, como $a \leq S(d)$, pela conexão de Galois (T, S), temos $T(a) \leq d$. Suponhamos $T(a) < d$, isto é, $T(a) \leq d - 1$, Logo, $T(a) \in \{b \text{ tal que } b \in Q,\ b \leq d - 1\}$. Dessa forma, pela definição de v, temos $T(a) \leq v$, que pela conexão (T, S), implica $a \leq S(v)$. Mas isto contradiz $S(v) + 1 \leq a$. Logo, $T(a) = d$. □

O objetivo daqui em diante é mostrar que pesos generalizados de Hamming e os perfis de dimensão/comprimento de um código linear C (m, k) formam uma conexão de Galois entre subconjuntos finitos de $\mathbb{Z}$. Para isso, consideremos a matriz teste de paridade de um código linear C (m, k), H, cujos vetores coluna sejam H_i, com $0 \leq i \leq m$ e vejamos, como uma ferramenta, o teorema a seguir, o qual trata-se de uma generalização do Lema 2.1.1 e é um resultado técnico, cuja demonstração não é determinante para a leitura do restante do texto.

Teorema 2.3.1. *Sejam $X \subseteq [1, m]$ e o espaço gerado pelos vetores H_i, $\langle H_i : i \in X\rangle$. Então,*

$$d_r(C) = \min\{|X| \ \textit{tal que}\ r \leq |X| - \textit{posto}(\langle H_i \ \textit{tal que}\ i \in X\rangle)\}.$$

Demonstração. A demonstração deste resultado pode ser encontrada em [19]. □

O teorema seguinte, nos apresenta a relação final entre pesos e perfis que queremos. Para ajudar-nos na demonstração deste resultado, vejamos o lema a seguir.

Lema 2.3.2. *Para um conjunto X (possivelmente infinito), considere as funções $f : X \to P$ e $g : X \to Q$, tais que $\max(P) \in f(X)$ e $\min(Q) \in g(X)$. Defina $T : P \to Q$ como*

$$T(a) = \min\{g(u) \ \text{ tal que } \ u \in X,\ a \leq f(u)\},$$

e $S : Q \to P$ como

$$S(b) = \max\{f(u) \ \text{ tal que } \ u \in X,\ g(u) \leq b\}.$$

Então, (T, S) é uma conexão de Galois entre P e Q.

Demonstração. Verificaremos as condições que devem satisfazer uma conexão de Galois. Desse modo, sejam $a, b \in P$, em que $a \leq b$. Com isso, temos

$$\begin{aligned} T(a) &= \min\{g(u) \ \text{ tal que } \ u \in X,\ a \leq f(u)\} \ \text{ e} \\ T(b) &= \min\{g(u) \ \text{ tal que } \ u \in X,\ b \leq f(u)\}. \end{aligned}$$

Consideremos $u', u'' \in X$, tais que $g(u') = T(a)$ e $g(u'') = T(b)$. Assim, como $a \leq b$, temos $a \leq b \leq f(u'')$, que implica $a \leq f(u'')$ e $g(u'') \in \{g(u) \ \text{ tal que } \ u \in X,\ a \leq f(u)\}$. Logo, $g(u') \leq g(u'')$, ou seja, $T(a) \leq T(b)$. De modo similar, obtemos o mesmo resultado para a função S. Portanto, a condição de que as funções precisam ser crescentes é válida.

Agora, para verificarmos a condição que resta, consideraremos $(a, c) \in P \times Q$, $A = \{f(u) \ \text{ tal que } \ u \in X,\ g(u) \leq c\}$ e $B = \{g(u) \ \text{ tal que } \ u \in X,\ a \leq f(u)\}$. Dessa forma, suponhamos $a \leq S(c)$. Sendo $S(c) = \max(A)$, tomemos u_1, tal que $f(u_1) = S(c)$. Por hipótese, temos $a \leq S(c)$, que implica imediatamente em $a \leq f(u_1)$, e assim, $g(u_1) \in B$ e, consequentemente, $T(a) \leq g(u_1)$. Logo, como $g(u_1) \leq c$, temos $T(a) \leq g(u_1) \leq c$, ou seja, $T(a) \leq c$. Por outro lado, sendo $T(a) = \min(B)$, consideremos $g(u_2) = T(a)$. Por hipótese, temos $T(a) \leq c$, que implica imediatamente em $g(u_2) \leq c$, e assim, $f(u_2) \in A$ e, consequentemente, $f(u_2) \leq S(c)$. Logo, como $a \leq f(u_2)$, temos $a \leq f(u_2) \leq S(c)$, ou seja, $a \leq S(c)$. Portanto, verificamos que (T, S) é conexão de Galois. □

Por fim, podemos enunciar o teorema principal desta seção.

Teorema 2.3.2. *Sejam $\mathbb{F}$ um corpo e C um código linear (m, k) sobre o corpo $\mathbb{F}$. Definamos $T : [0, k] \to [0, m]$ como $T(r) = d_r(C)$, e $S : [0, m] \to [0, k]$ como $S(l) = K_l(C)$. Então, (T, S) é uma conexão de Galois entre $[0, k]$ e $[0, m]$.*

Demonstração. Primeiramente, observemos que, pelo Lema 2.1.2, para o subcódigo $C \cap \delta(J)$ de C, temos $\dim_{\mathbb{F}}(C \cap \delta(J)) + \dim_{\mathbb{F}}((C \cap \delta(J))^{\perp}) = |J|$. Com base no Teorema 2.3.1, temos

$$\mathrm{d}_r(C) = \min\{|J| \ \text{ tal que } \ r \leq |J| - \dim_{\mathbb{F}}((C \cap \delta(J))^{\perp})\}, \tag{2.3}$$

em que $j \subseteq [1, m]$. Desse modo, novamente pelo Teorema 2.3.1, obtemos

$$\mathrm{d}_r(C) = \min\{|J| \text{ tal que } J \subseteq [1, m],\ r \leq \dim_{\mathbb{F}}(C \cap \delta(J))\}.$$

Além disso, por definição, $\mathrm{K}_l(C) = \max\{\dim_{\mathbb{F}}(C \cap \delta(J)) \text{ tal que } J \subseteq [1, m],\ |J| = l\}$. Agora, seja $A = \{\dim_{\mathbb{F}}(C \cap \delta(J)) \text{ tal que } J \subseteq [1, m],\ |J| \leq l\}$, em que $a = \max(A)$. Dessa forma, existe $J_1 \subseteq [1, m]$, tal que $|J_1| \leq l$ e $a = \dim_{\mathbb{F}}(C \cap \delta(J_1))$. Caso $|J_1| = l_1 < l$, tomemos $j_1 \in [1, m] - J_1$ e $J_2 = J_1 \cup \{j_1\}$. Com isso, como $|J_1| < l$, temos $|J_1| + 1 \leq l$. Assim, como $|J_1| + 1 = |J_2|$, temos $|J_2| \leq l$, e portanto, $\dim_{\mathbb{F}}(C \cap \delta(J_2)) \in A$. Sendo assim, como $a = \max(A)$, temos

$$a = \dim_{\mathbb{F}}(C \cap \delta(J_1)) \geq \dim_{\mathbb{F}}(C \cap \delta(J_2)) = b.$$

Porém, como $J_2 = J_1 \cup \{j_1\}$, temos

$$b = \dim_{\mathbb{F}}(C \cap \delta(J_2)) = \dim_{\mathbb{F}}(C \cap \delta(J_1 \cup \{j_1\})) \geq \dim_{\mathbb{F}}(C \cap \delta(J_1)) = a.$$

Portanto, $a = b$, de modo a considerarmos $b = \max(A)$, com $|J_2| = |J_1| + 1 \leq l$. Isto posto, caso $|J_2| < l$, substituindo J_1 por J_2 e repetindo o processo feito, podemos considerar $j_2 \in [1, m] - J_2$ e $J_3 = J_2 \cup \{j_2\}$, em que $|J_3| = |J_2| + 1 \leq l$. Sendo assim, podemos repetir este mesmo processo até que $\max(A) = \dim_{\mathbb{F}}(C \cap \delta(J))$, em que $|J| = l$. Logo, conseguimos

$$S(l) = \mathrm{K}_l(C) = \max\{\dim_{\mathbb{F}}(C \cap \delta(J)) \text{ tal que } J \subseteq [1, m],\ |J| \leq l\}.$$

Assim, considerando $f : \mathcal{P}([1, m]) \to [0, k]$ e $g : \mathcal{P}([1, m]) \to [0, m]$, funções definidas por $f(J) = \dim_{\mathbb{F}}(C \cap \delta(J))$ e $g(J) = |J|$, respectivamente, podemos aplicar o Lema 2.3.2, o que nos dá (T, S) como uma conexão de Galois entre $[0, k]$ e $[0, m]$. □

2.4 Matroide

Veremos, nesta seção, a dualidade de Wei aplicada em estruturas mais gerais, como as estruturas de matroide e demi-matroide. O nome "matroide", dá-se pela relação de independência entre colunas de uma matriz, surgindo na tentativa de formalização das definições de independências linear e algébrica, [18]. Desse modo, podemos encontrar diversas relações da álgebra linear na teoria de matroides. Na literatura existem mais de uma definição formal para matroides, as quais apresentaremos duas destas. Aqui, para não carregarmos a notação, de modo recorrente usaremos, por exemplo, $X \cup x$ e $X - x$ em vez de $X \cup \{x\}$ e $X - \{x\}$, respectivamente.

Definição 2.4.1. *Um matroide M sobre um conjunto finito E de n elementos, consiste em um par ordenado $(E, \mathcal{I})$, em que $\mathcal{I}$ é uma coleção de subconjuntos de E, satisfazendo as seguintes propriedades:*

(1) $\emptyset \in \mathcal{I}$;

(2) *Se* $Y \in \mathcal{I}$ *e* $X \subseteq Y$, *então* $X \in \mathcal{I}$;

(3) *Se* $X, Y \in \mathcal{I}$ *com* $|X| \leq |Y|$, *então existe um elemento* y *em* $Y - X$, *tal que* $X \cup y \in \mathcal{I}$.

Os subconjuntos de E pertencentes à coleção $\mathcal{I}$, são chamados de *conjuntos independentes* de M. Já os subconjuntos de E que não pertencem à $\mathcal{I}$, são chamados de *conjuntos dependentes* do matroide M.

Exemplo 2.4.1. *Consideremos a seguinte matriz sobre o corpo* $\mathbb{Z}_2$:

$$\begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$
$$\begin{matrix} a & b & c & d \end{matrix}$$

O par ordenado $(E, \mathcal{I})$, *com* $E = \{a, b, c, d\}$ *e a coleção de subconjuntos*

$$\mathcal{I} = \{\emptyset, \{b\}, \{c\}, \{d\}, \{b, c\}, \{b, d\}, \{c, d\}, \{b, c, d\}\}$$

é um matroide, cujos conjuntos dependente são $\{a\}, \{a, b\}, \{a, c\}, \{a, d\}$ *e por último,* $\{X \subseteq E \text{ tal que } |X| \geq 3\} - \{b, c, d\}$.

Para as próximas definições que apresentaremos, consideraremos um conjunto finito E e o conjunto $\mathcal{P}(E)$ como sendo o *conjunto das partes de* E, ou seja, $\mathcal{P}(E)$ é o conjunto de todos os subconjuntos de E. Agora definiremos uma função, chamada *posto*.

Definição 2.4.2. *Chamamos de função posto, a função* $p : \mathcal{P}(E) \to \mathbb{Z}$, *que satisfaz as seguintes propriedades:*

(1) *Se* $X \subseteq E$, *então* $0 \leq p(X) \leq |X|$;

(2) *Se* $X \subseteq Y \subseteq E$, *então* $p(X) \leq p(Y)$;

(3) *Se* X *e* Y *são subconjuntos de* E, *então* $p(X \cup Y) + p(X \cap Y) \leq p(X) + p(Y)$.

Nosso objetivo agora é estabelecer uma relação entre os conjuntos independentes e a função posto. Para isso, consideraremos o lema e teorema seguintes.

Lema 2.4.1. *Consideremos uma função posto* p. *Assim, se os subconjuntos de* E, X *e* Y, *são tais que* $p(X \cup e) = p(X)$, *para todo* $e \in Y - X$, *então* $p(X \cup Y) = p(X)$.

Demonstração. Consideremos o conjunto $Y - X = \{e_1, e_2, \ldots, e_k\}$. Conduziremos esta demonstração por uma indução sobre k. Observemos que, se $k = 1$, então $Y - X = \{e_1\}$,

o que nos dá $X \cup Y = X \cup e$ e, com isso $p(X \cup Y) = p(X)$. Agora, suponhamos que isso seja válido quando $k = n$, isto é, $p(X) = p(X \cup \{e_1, \ldots, e_n\})$. Veremos se é válido quando $k = n + 1$. Observemos que $p(X) = p(X \cup e_{n+1})$ e que pela terceira condição da função posto, temos

$$\begin{aligned} p(X) + p(X) &= p(X \cup \{e_1, \ldots, e_n\}) + p(X \cup e_{n+1}) \\ &\geq p((X \cup \{e_1, \ldots, e_n\}) \cup (p(X \cup e_{n+1})) \\ &+ p((X \cup \{e_1, \ldots, e_n\}) \cap (p(X \cup e_{n+1})) \\ &= p(X \cup \{e_1, \ldots, e_{n+1}\}) + p(X) \\ &\geq p(X) + p(X), \end{aligned}$$

já que $X \subset X \cup \{e_1, \ldots, e_{n+1}\}$. Como a primeira e última somas são iguais, obtemos a igualdade sobre todas as parcelas da expressão. Dessa forma, $p(X \cup \{e_1, \ldots, e_{n+1}\}) = p(X)$. Portanto, por indução, obtemos o que queríamos. □

Teorema 2.4.1. *Consideremos $\mathcal{I}$ uma coleção de subconjuntos de um conjunto finito E, em que, para todo $X \in \mathcal{I}$, temos $p(X) = |X|$, sendo p uma função posto. Então, o par ordenado $(E, \mathcal{I})$ é um matroide com função posto p.*

Demonstração. Observemos que, pela primeira condição de p, temos $0 \leq p(\emptyset) \leq |\emptyset| = 0$, logo $p(\emptyset) = |\emptyset|$ e $\emptyset \in \mathcal{I}$. Agora, suponhamos $Y \in \mathcal{I}$, e $X \subseteq Y$. Sabemos que $p(Y) = |Y|$ e, assim, considerando a terceira condição de p e os conjuntos X e $Y - X$, temos os seguinte:

$$p(X \cup (Y - X)) + p(X \cap (Y - X)) \leq p(X) + p(Y - X),$$

o que nos dá

$$p(Y) + p(\emptyset) \leq p(X) + p(Y - X).$$

Porém, sabemos que $p(Y) = |Y|$ e $p(\emptyset) = 0$ e, pela segunda condição de p, que $p(X) \leq |X|$ e $p(Y - X) \leq |Y - X|$. Desse modo,

$$|Y| \leq p(X) + p(Y - X) \leq |X| + |Y - X| = |Y|.$$

Portanto, pela igualdade final, temos $p(X) = |X|$ e logo, $X \in \mathcal{I}$. Por fim, suponhamos, por contradição, que considerando $X, Y \in \mathcal{I}$, com $|X| < |Y|$, tais que para todo $y \in Y - X$, o conjunto $X \cup y$ não esteja em $\mathcal{I}$. Sendo assim, temos $p(X \cup y) \neq |X \cup y|$. Com isso, pelas condições de p e como $X \in \mathcal{I}$ e $X \subset X \cup y$, temos

$$|X| + 1 > p(X \cup y) \geq p(X) = |X|,$$

o que nos dá $p(X \cup y) = |X|$. Pelo Lema 2.4.1, obtemos $p(X \cup Y) = |X|$, porém $p(X) = |X|$ e como $Y \subseteq X \cup Y$, temos $p(X \cup Y) \geq p(Y) = |Y|$, então $|X| \geq |Y|$, o

que é uma contradição. Logo, a terceira condição de conjuntos independentes, vale para conjuntos em $\mathcal{I}$. Portanto, $(E, \mathcal{I})$ é um matroide. □

Observamos que todo matroide tem uma função posto a ele associado, digamos t. Tal função t é igual a função posto do teorema acima. A demonstração deste fato pode ser encontrada no Teorema 1.3.2 do livro "Matroid theory" de James G. Oxley, [13]. Podemos visualizar este resultado como uma equivalência entre p e os conjuntos independentes. Sendo assim, temos X um conjunto independente se, e somente se, $p(X) = |X|$, para alguma função posto. Com isso, obtemos uma outra definição para matroides.

Definição 2.4.3. *Um matroide M sobre E, consiste em um par ordenado (E, p), em que E é um conjunto de n elementos, $n \in \mathbb{N}$, e $p : \mathcal{P}(E) \to \mathbb{Z}$, é uma função, chamada função posto, que satisfaz as seguintes propriedades:*

(1) *Se $X \subseteq E$, então $0 \leq p(X) \leq |X|$;*

(2) *Se $X \subseteq Y \subseteq E$, então $p(X) \leq p(Y)$;*

(3) *Se X e Y são subconjuntos de E, então $p(X \cup Y) + p(X \cap Y) \leq p(X) + p(Y)$.*

Definição 2.4.4. *Seja um matroide $M = (E, p)$. O matroide dual é um matroide M^* sobre E cuja função posto p^* é definida por*

$$p^*(X) = |X| + p(E - X) - p(E)$$

para todo $X \subseteq E$.

Definição 2.4.5. *Dizemos que o matroide $M = (E, p)$ é auto-dual se $p = p^*$, em que p^* é a função posto do matroide dual a M, $M^* = (E, p^*)$.*

Outro exemplo de um matroide é o *Matroide de Vàmos*, introduzido por Peter Vàmos em 1968, o qual denotamos por V_8.

Exemplo 2.4.2. *O Matroide de Vàmos é um matroide de posto 4, definido sobre um conjunto de 8 elementos $E = \{1, 2, 3, 4, 5, 6, 7, 8\}$. Neste matroide, se $X \subseteq E$ com $|X| \geq 5$, então $p(X) = 4$. Aqui, todos os conjuntos de três ou menos elementos são independentes, ou seja, se $X \subseteq E$ com $|X| \leq 3$, então $p(X) = |X| = 3$. Além disso, se $|X| = 4$, 65 dos 70 conjuntos possíveis, são independentes, ou seja, $p(X) = |X| = 4$, sendo as exceções, apenas cinco conjuntos dependentes em que $p(X) = 3 < 4 = |X|$. Na Figura 1, os cinco conjuntos dependentes são representados pelos vértices de cada um dos cinco paralelogramos retratados.*

Observemos, a partir disso, que há uma dualidade entre conjuntos formados a partir de nossa concepção de matroides. Em favor disso, consideremos o matroide $M = (E, p)$, de

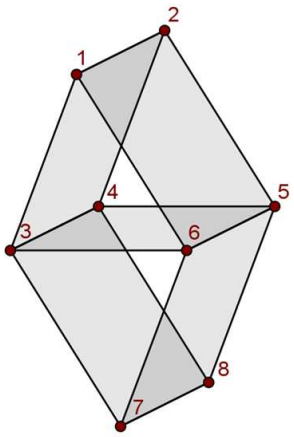

Figura 1 – V_8

posto k, sobre um conjunto finito E de n elementos. Definimos então, para cada $i \in [0,k]$ e $j \in [0, n-k]$, os seguintes elementos:

$$\begin{aligned} f_i &= \max\{|X| \text{ tal que } X \subseteq E,\ p(X) = i\}; \\ f_j^* &= \max\{|X| \text{ tal que } X \subseteq E,\ p^*(X) = j\}. \end{aligned}$$

E também os conjuntos:

$$\begin{aligned} \mathcal{A}_M &= \{n - f_{k-1}, \ldots, n - f_0\}; \\ \mathcal{B}_M &= \{f_0^* + 1, \ldots, f_{n-k-1}^* + 1\}. \end{aligned}$$

Com isso, obtemos o seguinte teorema de dualidade para matroides:

Teorema 2.4.2. *$\mathcal{A}_M \cup \mathcal{B}_M = \{1, \ldots, n\}$ e $\mathcal{A}_M \cap \mathcal{B}_M = \emptyset$.*

Demonstração. A demonstração deste teorema, dá-se de modo semelhante ao que faremos para o Teorema 2.4.5. □

Exemplo 2.4.3. *Consideremos o matroide V_8^+ sobre $E = \{1,2,3,4,5,6,7,8\}$. Este, deriva do Matroide de Vàmos V_8, desta vez com o conjunto $\{1,2,7,8\}$, de acordo com a Figura 1, como mais um dos cinco conjuntos dependentes de quatro elementos e posto 3. O matroide V_8^+ é auto-dual. De fato, considerando $X \subseteq E$ e*

$$\begin{aligned} L &= p^*(X) - p(X) \\ &= |X| + p(E - X) - p(E) - p(X), \end{aligned}$$

observemos que, se $p(X) = 1$:

$$L = 1 + p(E - X) - 4 - 1.$$

Neste caso, $E - X$ é um conjunto de 7 elementos, ou seja, $p(E - X) = 4$, o que nos dá $L = 0$.

Agora, se $p(X) = 2$*:*

$$L = 2 + p(E - X) - 4 - 2.$$

Neste caso, $E - X$ *é um conjunto de* 6 *elementos, ou seja,* $p(E - X) = 4$*, o que nos dá* $L = 0$*.*

Ainda, se $p(X) = 3$*:*

$$L = 3 + p(E - X) - 4 - 3.$$

Neste caso, $E - X$ *é um conjunto de* 5 *elementos, ou seja,* $p(E - X) = 4$*, o que nos dá* $L = 0$*.*

Por fim, se $p(X) = 4$*:*

$$\begin{aligned} L &= |X| + p(E - X) - 4 - 4 \\ &= |X| + p(E - X) - 8 \end{aligned}$$

Neste caso, X *pode ser um conjunto de* $4, 5, 6, 7$ *ou* 8 *elementos. Assim, se* $|X| = 4$*:*

$$|X| + p(E - X) - 8 = p(E - X) - 4$$

Neste caso, $E - X$ *é um conjunto de* 4 *elementos. Ora, suponhamos que* $p(E - X) \neq 4$*. Sendo assim, por definição, temos* $p(E - X) = 3$ *e desse modo, de acordo com a Figura 1, os possíveis conjuntos para* $E - X$ *são* $\{1, 2, 5, 6\}$*,* $\{5, 6, 7, 8\}$*,* $\{3, 4, 5, 6\}$*,* $\{3, 4, 7, 8\}$*,* $\{1, 2, 3, 4\}$ *e* $\{1, 2, 7, 8\}$*. Observemos, a partir disso, que se* $E - X$ *for algum dos conjuntos ditos, então* X *também o será, o que é uma contradição, pois* $p(X) = 4$*. Portanto,* $p(E - X) = 4$*, o que nos dá* $L = 0$*.*

Agora, se $|X| = 5$*:*

$$|X| + p(E - X) - 8 = p(E - X) - 3$$

Neste caso, $E - X$ *é um conjunto de* 3 *elementos, ou seja,* $p(E - X) = 3$*, o que nos dá* $L = 0$*.*

Ainda, se $|X| = 6$*:*

$$|X| + p(E - X) - 8 = p(E - X) - 2$$

Neste caso, $E - X$ *é um conjunto de* 2 *elementos, ou seja,* $p(E - X) = 2$*, o que nos dá* $L = 0$*.*

Já se $|X| = 7$*:*

$$|X| + p(E - X) - 8 = p(E - X) - 1$$

Neste caso, $E - X$ é um conjunto de 1 elemento, ou seja, $p(E - X) = 1$, o que nos dá $L = 0$.

Por fim, se $|X| = 8$:

$$|X| + p(E - X) - 8 \;=\; p(E - X)$$

Neste caso, $E - X$ é o conjunto vazio, ou seja, $p(E - X) = 0$, o que nos dá $L = 0$. E, portanto, em todos os casos possíveis, chegamos a $p^*(X) = p(X)$.

Por consequência, conseguimos $(f_0, f_1, f_2, f_3) = (f_0^*, f_1^*, f_2^*, f_3^*)$ e, desse modo, basta calcularmos f_0, f_1, f_2 e f_3. Sabendo que $f_3 = \max\{|X| \text{ tal que } X \subseteq E,\ p(X) = 3\}$, todos os conjuntos de três elementos têm posto 3 e que há seis conjuntos de quatro elementos de posto 3, obtemos $f_3 = 4$, ou seja, o maior conjunto de posto 3 neste matroide, possui quatro elementos, pois todos de cardinalidade maior ou igual a 5, têm posto 4. Os elementos f_0, f_1 e f_2 são obtidos de forma imediata. Ao final, conseguimos $(f_0, f_1, f_2, f_3) = (f_0^*, f_1^*, f_2^*, f_3^*) = (0, 1, 2, 4)$, o que nos dá $\mathcal{A}_M = \{4, 6, 7, 8\}$ e $\mathcal{B}_M = \{1, 2, 3, 5\}$. Portanto, $\mathcal{A}_M \cup \mathcal{B}_M = \{1, 2, 3, 4, 5, 6, 7, 8\}$ e $\mathcal{A}_M \cap \mathcal{B}_M = \emptyset$.

Uma outra definição de considerável importância para o nosso estudo posterior, é a definição de demi-matroides.

Definição 2.4.6. *Um demi-matroide é uma tripla $D = (E, s, t)$ sobre um conjunto finito E, composto por duas funções $s, t : \mathcal{P}(E) \to \mathbb{N}_0$, em que para todos subconjuntos $X \subseteq Y \subseteq E$, satisfazem*

(R) $0 \leq s(X) \leq s(Y) \leq |Y|$ *e* $0 \leq t(X) \leq t(Y) \leq |Y|$;

(D) $|E - X| - s(E - X) = t(E) - t(X)$.

Na definição acima, podemos ver que por (R), $s(\emptyset) = t(\emptyset) = 0$. Dessa forma, pelo item (D), temos $|E - \emptyset| - s(E - \emptyset) = t(E) - t(\emptyset)$, o que implica $t(E) = |E| - s(E)$. Além disso, também pelo item (D), conseguimos $|E-(E-X)|-s(E-(E-X)) = t(E)-t(E-X)$, o que implica $t(E - X) = t(E) + s(X) - |X|$. Dessa forma, observemos o seguinte:

$$\begin{aligned} |E - X| - t(E - X) &= |E - X| - t(E) - s(X) + |X| \\ &= |E| - t(E) - s(X) \\ &= |E| - |E| + s(E) - s(X) \\ &= s(E) - s(X). \end{aligned}$$

Portanto, item (D) é equivalente a $|E - X| - t(E - X) = s(E) - s(X)$.

Neste ponto, observemos que, para qualquer matroide $M = (E, p)$ sobre E, a tripla (E, p, p^*) é um demi-matroide, já que a condição (R) nos é dada pela definição de função

posto e para a condição (D) temos:

$$\begin{aligned} p^*(E) - p^*(X) &= |E| + p(E-E) - p(E) - (|X| + p(E-X) - p(E)) \\ &= |E| + p(\emptyset) - p(E) - |X| - p(E-X) + p(E) \\ &= |E| - |X| - p(E-X) \\ &= |E-X| - p(E-X). \end{aligned}$$

Porém, a recíproca desta afirmação não é verdadeira, como veremos no exemplo a seguir.

Exemplo 2.4.4. *Consideremos $E = \{a, b\}$ e definamos $s(E) = 1$ e $s(X) = 0$ para $X = \emptyset, \{a\}, \{b\}$. Podemos ver que a tripla (E, s, s) é um demi-matroide, mas s não é função posto de qualquer matroide sobre E. De fato,*

$$1 = s(\{a\} \cup \{b\}) + s(\{a\} \cap \{b\}) \leq s(\{a\}) + s(\{b\}) = 0,$$

o que é uma contradição.

Há uma dualidade referente a conjuntos formados a partir de demi-matroides. Para conseguirmos essa dualidade, precisamos de alguns passos importantes. Consideremos $D = (E, s, t)$ um demi-matroide sobre E, em que $s(E) = k$. Por (D), chegamos à relação: $s(E) + t(E) = n$.

Lema 2.4.2. *$s(X - x) \geq s(X) - 1$ e $t(X - x) \geq t(X) - 1$ para todo $X \subseteq E$ e $x \in E$.*

Demonstração. Por (R) e (D),

$$\begin{aligned} t(X-x) &= t(E) - |E - (X-x)| + s(E - (X-x)) \\ &\geq t(E) - |E - X| - 1 + s(E-X) \\ &= t(X) - 1. \end{aligned}$$

De modo similar, obtemos $s(X - x) \geq s(X) - 1$. □

Também precisamos das definições de um conjunto parcialmente ordenado, seu dual e ideias de ordem:

Definição 2.4.7. *Uma relação de ordem parcial sobre um conjunto E, é uma relação binária $\preceq$ satisfazendo as seguintes condições:*

(1) *Reflexiva: $i \preceq j$, $\forall i \in E$;*

(2) *Antissimétrica: dados $i, j \in E$, se $i \preceq j$ e $j \preceq i$, então $i = j$;*

(3) *Transitiva: dados $i, j, k \in E$, se $i \preceq j$ e $j \preceq k$, então $i \preceq k$.*

O par $P = (E, \preceq)$, consistindo de um conjunto não vazio E e uma ordem parcial $\preceq$ sobre E, é chamado conjunto parcialmente ordenado (poset).

Definição 2.4.8. *O dual de P é o poset $\overline{P}$ sobre E, com relação de ordem $\preceq_{\overline{P}}$ definida para todo $x, y \in E$ por $x \preceq_{\overline{P}} y$ se, e somente se, $y \preceq_P x$.*

Uma definição de suma importância para nós, é a definição de ideal de ordem, que veremos a seguir.

Definição 2.4.9. *Para cada subconjunto $X \subseteq E$, definimos o ideal de ordem como o conjunto $\langle X \rangle_P = \{x \in E \text{ tal que } x \preceq_P y \text{ para algum } y \in X\}$.*

Desta vez, para cada $i \in [0, k]$ e $j \in [0, n-k]$, definamos então os seguintes elementos:

$$\begin{aligned}
\sigma_i^P &= \min\{|\langle X \rangle_P| \text{ tal que } X \subseteq E,\ s(X) \geq i\};\\
\tau_j^{\overline{P}} &= \min\{|\langle X \rangle_{\overline{P}}| \text{ tal que } X \subseteq E,\ t(X) \geq j\};\\
s_i^P &= \max\{|E - \langle E - X \rangle_P| \text{ tal que } X \subseteq E,\ s(X) \leq i\};\\
t_j^{\overline{P}} &= \max\{|E - \langle E - X \rangle_{\overline{P}}| \text{ tal que } X \subseteq E,\ t(X) \leq j\}.
\end{aligned}$$

O próximo lema, nos dá que estes elementos definidos com $s(X) \geq i$ ou $s(X) \leq i$ e $t(X) \geq j$ ou $t(X) \leq j$, são equivalentes aos elementos quando consideramos $s(X) = i$ e $t(X) = j$, respectivamente.

Lema 2.4.3. *Para cada $i \in [0, k]$ e $j \in [0, n-k]$,*

$$\begin{aligned}
\sigma_i^P &= \min\{|\langle X \rangle_P| \text{ tal que } X \subseteq E,\ s(X) = i\};\\
\tau_j^{\overline{P}} &= \min\{|\langle X \rangle_{\overline{P}}| \text{ tal que } X \subseteq E,\ t(X) = j\};\\
s_i^P &= \max\{|E - \langle E - X \rangle_P| \text{ tal que } X \subseteq E,\ s(X) = i\};\\
t_j^{\overline{P}} &= \max\{|E - \langle E - X \rangle_{\overline{P}}| \text{ tal que } X \subseteq E,\ t(X) = j\}.
\end{aligned}$$

Demonstração. A prova deste resultado segue por um processo semelhante ao feito para $K_l(C)$ na demonstração do Teorema 2.3.2. □

Antes de seguirmos para o próximo lema, precisamos definir o que é um elemento maximal em um poset $P = (E, \preceq)$ sobre o conjunto finito E de n elementos.

Definição 2.4.10. *Dizemos que $x \in E$ é um elemento maximal no poset P se dado $y \in E$ com $x \preceq_P y$, então $x = y$.*

Lema 2.4.4 (Monotonicidade)**.** *São válidas as seguintes inequações:*

$$\begin{aligned} 0 &= \sigma_0^P < \sigma_1^P < \sigma_2^P < \cdots < \sigma_k^P \leq n; \\ 0 &= \tau_0^{\overline{P}} < \tau_1^{\overline{P}} < \tau_2^{\overline{P}} < \cdots < \tau_{n-k}^{\overline{P}} \leq n; \\ 0 &\leq s_0^P < s_1^P < s_2^P < \cdots < s_k^P = n; \\ 0 &\leq t_0^{\overline{P}} < t_1^{\overline{P}} < t_2^{\overline{P}} < \cdots < t_{n-k}^{\overline{P}} = n. \end{aligned}$$

Demonstração. Para esta demonstração, apresentaremos aqui, uma versão para o elemento σ_i^P, pois por um processo semelhante, chegamos à mesma relação para os demais. Dessa forma, consideremos $X \subseteq E$ tal que $|\langle X\rangle_P| = \sigma_i^P$ e $s(X) \geq i$, para qualquer $i \in [0,k]$. Como $s(\emptyset) = 0$, obtemos $\sigma_0^P = 0$ e, desse modo, podemos supor $s(X) \geq 1$ e $X \neq \emptyset$. Tomemos um elemento $x \in X$ que seja maximal em P. Assim, $\langle X - x\rangle_P \subsetneq \langle X\rangle_P$. Pelo Lema 2.4.2, temos $s(X-x) \geq s(X)-1 \geq i-1$. Logo $\sigma_{i-1}^P \leq |\langle X-x\rangle_P| < |\langle X\rangle_P| = \sigma_i^P$. □

Definição 2.4.11. *O dual de um demi-matroide $D = (E, s, t)$ é a tripla $D^* = (E, t, s)$.*

Definição 2.4.12. *Para qualquer função real $\varphi : \mathcal{P}(E) \to \mathbb{R}$, considere $\overline{\varphi}$ dada por*

$$\overline{\varphi}(X) = \varphi(E) - \varphi(E - X).$$

A partir disso, sabemos que $\overline{\overline{\varphi}}(X) = \overline{\varphi}(E) - \overline{\varphi}(E - X) = \varphi(X) - \varphi(\emptyset)$. Dessa forma, observemos que, se $\varphi(\emptyset) = 0$, então $\varphi = \overline{\overline{\varphi}}$. Esta observação é importante para a demonstração do próximo teorema.

Teorema 2.4.3. *A tripla $\overline{D} = (E, \overline{s}, \overline{t})$ é um demi-matroide. Além disso, $D = \overline{\overline{D}}$ e $\overline{D^*} = \overline{D}^*$. O demi-matroide $\overline{D}$ é chamado de suplementar de D.*

Demonstração. Sabemos que $D = (E, s, t)$ é um demi-matroide. Vejamos agora, as condições (R) e (D) para a tripla $\overline{D} = (E, \overline{s}, \overline{t})$. Temos, por definição, que $\overline{s}(X) = s(E) - s(E - X)$, em que $X \subseteq E$. Dessa forma, consideremos $X, Y \subseteq E$, tais que $X \subseteq Y$. Com isso, temos $E - Y \subseteq E - X$. Daí,

$$\begin{aligned} s(E-Y) \leq s(E-X) &\iff -s(E-X) \leq -s(E-Y) \\ &\iff s(E) - s(E-X) \leq s(E) - s(E-Y) \\ &\iff \overline{s}(X) \leq \overline{s}(Y). \end{aligned}$$

Além disso, como $E - X \subseteq E$, temos $s(E - X) \leq s(E)$. Assim, $0 \leq s(E) - s(E - X)$, o que equivale $0 \leq \overline{s}(X)$. Notemos que

$$\overline{s}(Y) = s(E) - s(E - Y) \leq |E| - |E - Y| = |Y|.$$

E, portanto, $0 \leq \overline{s}(X) \leq \overline{s}(Y) \leq |Y|$. De modo similar, conseguimos $0 \leq \overline{t}(X) \leq \overline{t}(Y) \leq |Y|$. Por fim, observemos o seguinte:

$$\begin{aligned} |E-X| - \overline{s}(E-X) &= |E-X| - (s(E) - s(E-(E-X))) \\ &= |E-X| - (s(E) - s(X)) \\ &= |E-X| - (|E-X| - t(E-X)) \\ &= t(E-X) \\ &= t(E) - t(E-E) - (t(E) - t(E-X)) \\ &= \overline{t}(E) - \overline{t}(X). \end{aligned}$$

Logo, $|E-X| - \overline{s}(E-X) = \overline{t}(E) - \overline{t}(X)$, e portanto, $\overline{D}$ é um demi-matroide. Por sua vez, como $s(\emptyset) = t(\emptyset) = 0$, pela observação feita anteriormente, é imediato que $\overline{\overline{D}} = (E, \overline{\overline{s}}, \overline{\overline{t}}) = (E, s, t) = D$. E ainda, $\overline{D^*} = (E, \overline{t}, \overline{s}) = ((E, \overline{s}, \overline{t}))^* = \overline{D}^*$. □

Neste contexto, definamos para cada $i \in [0,k]$ e $j \in [0, n-k]$, os elementos

$$\begin{aligned} \overline{\sigma}_i^P &= \min\{|\langle X\rangle_P| \text{ tal que } X \subseteq E,\ \overline{s}(X) \geq i\}; \\ \overline{\tau}_j^{\overline{P}} &= \min\{|\langle X\rangle_{\overline{P}}| \text{ tal que } X \subseteq E,\ \overline{t}(X) \geq j\}; \\ \overline{s}_i^P &= \max\{|E - \langle E-X\rangle_P| \text{ tal que } X \subseteq E,\ \overline{s}(X) \leq i\}; \\ \overline{t}_j^{\overline{P}} &= \max\{|E - \langle E-X\rangle_{\overline{P}}| \text{ tal que } X \subseteq E,\ \overline{t}(X) \leq j\}. \end{aligned}$$

Lema 2.4.5. *Para cada $i \in [0,k]$ e $j \in [0, n-k]$,*

$$\begin{aligned} s_i^P &= n - \overline{\sigma}_{k-i}^P; \quad t_j^{\overline{P}} = n - \overline{\tau}_{n-k-j}^{\overline{P}}; \\ \sigma_i^P &= n - \overline{s}_{k-i}^P; \quad \tau_j^{\overline{P}} = n - \overline{t}_{n-k-j}^{\overline{P}}. \end{aligned}$$

Demonstração. Para esta demonstração, faremos para o caso $s_i^P = n - \overline{\sigma}_{k-i}^P$, pois por um processo semelhante, chegamos à mesma relação para os demais. Relembremos as definições de s_i^P e $\overline{\sigma}_{k-i}^P$:

$$\begin{aligned} s_i^P &= \max\{|E - \langle E-X\rangle_P| \text{ tal que } X \subseteq E,\ s(X) = i\} \\ \overline{\sigma}_i^P &= \min\{|\langle X\rangle_P| \text{ tal que } X \subseteq E,\ \overline{s}(X) = i\}, \end{aligned}$$

em que para $\overline{\sigma}_i^P$, também é válido o Lema 2.4.3. Com isso, consideremos $Y = E - X$ e observemos o seguinte:

$$\begin{aligned} s_i^P &= \max\{|E - \langle E-X\rangle_P| \text{ tal que } X \subseteq E,\ s(X) = i\} \\ &= \max\{|E - \langle Y\rangle_P| \text{ tal que } E-Y \subseteq E,\ s(E-Y) = i\} \\ &= \max\{|E - \langle Y\rangle_P| \text{ tal que } Y \subseteq E,\ s(E-Y) = i\} \\ &= n - \min\{|\langle Y\rangle_P| \text{ tal que } Y \subseteq E,\ \overline{s}(Y) = k-i\} \\ &= n - \overline{\sigma}_{k-i}^P, \end{aligned}$$

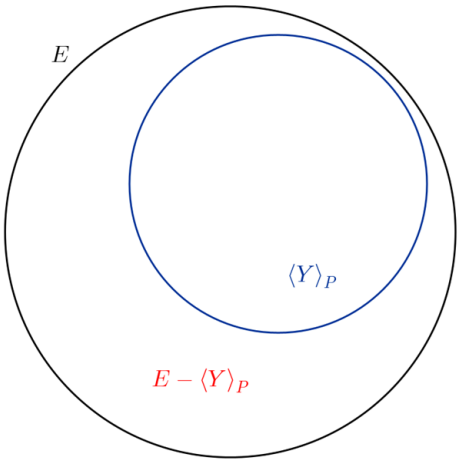

Figura 2 – Lema 2.4.5

em que $X = E - Y$ e $\overline{s}(Y) = s(E) - s(E - Y) = k - i$. □

Para fins ilustrativos, observemos na Figura 2.4.5, que quanto maior o conjunto $E - \langle Y\rangle_P$, menor será $\langle Y\rangle_P$, nos dando o resultado que queríamos.

A partir disso, consideremos os conjuntos

$$\begin{aligned}
\mathcal{U}_D^P &= \{n - s_{k-1}^P, \ldots, n - s_0^P\};\\
\mathcal{V}_D^{\overline{P}} &= \{t_0^{\overline{P}} + 1, \ldots, t_{n-k-1}^{\overline{P}} + 1\};\\
\mathcal{A}_D^P &= \{\sigma_1^P, \ldots, \sigma_k^P\};\\
\mathcal{B}_D^{\overline{P}} &= \{n + 1 - \tau_{n-k}^{\overline{P}}, \ldots, n + 1 - \tau_1^{\overline{P}}\}.
\end{aligned}$$

E, depois de todas as devidas considerações, chegamos enfim, aos teoremas de dualidade para demi-matroides.

Teorema 2.4.4. $\mathcal{U}_D^P \cup \mathcal{V}_D^{\overline{P}} = \{1, \ldots, n\}$ *e* $\mathcal{U}_D^P \cap \mathcal{V}_D^{\overline{P}} = \emptyset$.

Demonstração. A demonstração deste teorema, dá-se de modo semelhante ao que faremos para o Teorema 2.4.5. □

Teorema 2.4.5. $\mathcal{A}_D^P \cup \mathcal{B}_D^{\overline{P}} = \{1, \ldots, n\}$ *e* $\mathcal{A}_D^P \cap \mathcal{B}_D^{\overline{P}} = \emptyset$.

Demonstração. Por contradição, suponhamos que $\mathcal{A}_D^P \cap \mathcal{B}_D^{\overline{P}} \neq \emptyset$, ou seja existem algum $i \in [0, k]$ e algum $j \in [n - k]$, tais que $\sigma_i^P = n + 1 - \tau_j^{\overline{P}}$. Desse modo, consideremos um subconjunto $X \subseteq E$ que satisfaça $|\langle X\rangle_P| = \sigma_i^P$ e $s(X) \geq i$ e tomemos $Y = E - \langle X\rangle_P$. Podemos afirmar que Y é ideal em $\overline{P}$. De fato, tomando $u \in E$ e $v \in Y$, observamos que, pela definição de poset dual, $u \leq_{\overline{P}} v \iff v \leq_P u$. Assim, se $u \in \langle X\rangle_P$, isso implicaria $v \in \langle X\rangle_P$, contradizendo $v \in Y$ e, logo, $u \notin \langle X\rangle_P$, ou seja, $u \in Y$. Com isso, $|\langle Y\rangle_{\overline{P}}| = |Y| = n - \sigma_i^P = \tau_j^{\overline{P}} - 1$. Dessa forma, $t(Y) \leq j - 1$, pois se caso $t(Y) \geq j$, então

teríamos $\tau_j^{\overline{P}} \leq |\langle Y \rangle_{\overline{P}}| = \tau_j^{\overline{P}} - 1$, o que é impossível. Assim sendo, por (R) e (D), temos o seguinte:

$$\begin{aligned} n - k - \sigma_i^P + i &\leq t(E) - |\langle X \rangle_P| + s(X) \\ &\leq t(E) - |\langle X \rangle_P| + s(\langle X \rangle_P) \\ &= t(E) - |E - Y| + s(E - Y) \\ &= t(Y) \\ &\leq j - 1. \end{aligned}$$

De modo similar, chegamos a $n - (n - k) - \tau_j^{\overline{P}} + j \leq i - 1$. Portanto, somando as desigualdades, obtemos $-1 = n - \sigma_i^P - \tau_j^{\overline{P}} \leq -2$, o que é uma contradição. Desse modo, segue que $\sigma_i^P \neq n + 1 - \tau_j^{\overline{P}}$, para todo i, j e o teorema está provado. □

3 Principais Resultados

Neste capítulo, apresentaremos o Teorema Central deste trabalho, o qual nos mostra que, a partir de duas conexões de Galois entre subconjuntos finitos de $\mathbb{Z}$, é possível obter uma dualidade do tipo Wei. Após isso, veremos o Teorema da Ponte, que será de grande utilidade quanto às aplicações destes resultados. A principal referência utilizada foi [20].

3.1 O Teorema Central

Veremos, nesta seção, o Teorema Central deste trabalho e uma demonstração do mesmo. Consideraremos $k, m \in \mathbb{N}$ e $w \in \mathbb{Z}^+$.

Lema 3.1.1. *Seja (T, S) uma conexão de Galois entre $[0, k]$ e $[0, m]$, tal que $S(0) = 0$ e $S(l) - S(l-1) \leq w$, para todo $l \in [1, m]$. Definamos $\eta : [0, m] \to \mathbb{Z}$ como*

$$\eta(l) = S(m - l) + wl - k.$$

Desse modo, são válidas as seguintes afirmações:

(1) *$\eta(m) = wm - k$ e $\eta(0) = 0$;*

(2) *$0 \leq \eta(l) - \eta(l-1) \leq w$, para todo $l \in [1, m]$;*

(3) *Existe $\tau : [0, wm - k] \to [0, m]$, tal que (τ, η) é uma conexão de Galois entre $[0, wm - k]$ e $[0, m]$. Além disso, para todo $u \in [0, k]$ e $v \in [0, wm - k]$, em que $T(u) + \tau(v) = m + 1$, é válido que $u \not\equiv v + k \mod w$.*

Demonstração. Comecemos nossa demonstração pela afirmação (1). Sendo assim, da forma como η está definida, temos

$$\eta(0) = S(m - 0) + w \cdot 0 - k = S(m) - k.$$

Como $Im(T) \subseteq [0, m]$, então $T(k) \leq m$. Assim, como (T, S) é conexão de Galois, para $(k, m) \in [0, k] \times [0, m]$, temos $k \leq S(m)$ se, e somente se, $T(k) \leq m$. E visto que $Im(S) \subseteq [0, k]$, por consequência, $S(m) \leq k$. Logo, $S(m) = k$ e, como resultado, $\eta(0) = 0$. Por fim, temos

$$\eta(m) = S(m - m) + w \cdot m - k = S(0) + w \cdot m - k,$$

e como $S(0) = 0$, obtemos $\eta(m) = wm - k$.

Agora, para a afirmação (2), consideremos $l \in [1, m]$ e observemos o seguinte:

$$\begin{aligned}\eta(l) - \eta(l-1) &= S(m-l) + wl - k - (S(m-(l-1)) + w(l-1) - k) \\ &= S(m-l) + wl - k - S(m-(l-1)) - w(l-1) + k \\ &= S(m-l) - S(m-(l-1)) + w.\end{aligned}$$

Como $m - l \leq m - (l-1) = m - l + 1$, temos $S(m-l) \leq S(m-(l-1))$. Assim, $S(m-l) - S(m-(l-1)) \leq 0$ e, desse modo,

$$\begin{aligned}\eta(l) - \eta(l-1) &= S(m-l) - S(m-(l-1)) + w \\ &\leq 0 + w \\ &= w.\end{aligned}$$

Além disso, pela definição de S, temos $S(m-(l-1)) - S(m-l) \leq w$, o que nos dá $S(m-l) - S(m-(l-1)) \geq -w$. Logo,

$$\begin{aligned}\eta(l) - \eta(l-1) &= S(m-l) - S(m-(l-1)) + w \\ &\geq -w + w \\ &= 0.\end{aligned}$$

Portanto, $0 \leq \eta(l) - \eta(l-1) \leq w$, para todo $l \in [1, m]$.

Por fim, para a afirmação (3), definamos uma função $\tau : [0, wm-k] \to [0, m]$ como

$$\tau(a) = \min\{b \text{ tal que } b \in [0, m],\ a \leq \eta(b)\}.$$

Observemos que τ está bem definida. De fato, o conjunto $[0, m]$ é finito e devido ao princípio da boa ordem, existe elemento mínimo b, tal que $a \leq \eta(b)$. Além disso, (τ, η) é uma conexão de Galois entre $[0, wm-k]$ e $[0, m]$. Com efeito, dados $c, d \in [0, wm-k]$, com $c \leq d$, consideremos $\tau(c) = \gamma$ e $\tau(d) = \gamma'$. Desse modo, como $c \leq d$, temos $c \leq d \leq \eta(\gamma')$, que implica $c \leq \eta(\gamma')$ e $\gamma' \in \{b \text{ tal que } b \in [0, m],\ c \leq \eta(b)\}$. Logo, $\gamma \leq \gamma'$, ou seja, $\tau(c) \leq \tau(d)$. E ainda, pelos itens (1) e (2), vistos anteriormente, temos η também crescente. Além disso, considerando $(c, e) \in [0, wm-k] \times [0, m]$ e supondo $c \leq \eta(e)$, por definição de τ, obtemos $\tau(c) \leq e$. Por outro lado, se $\tau(c) = f \leq e$, obtemos $f \in [0, m]$ e $c \leq \eta(f)$. Como η é crescente, $c \leq \eta(f) \leq \eta(e)$. Logo, $c \leq \eta(e)$.

Agora, sejam $u \in [0, k]$ e $v \in [0, wm-k]$, tais que $T(u) + \tau(v) = m + 1$. Com isso, temos $\tau(v) = m + 1 - T(u)$, em que $T(u) \in [1, m]$. Pelo item (4) do Lema 2.3.1, considerando a conexão de Galois (τ, η), temos

$$\eta(m - T(u)) + 1 \leq v \leq \eta(m + 1 - T(u)),$$

sendo $m - T(u) = \max\{b \text{ tal que } b \in [0, m],\ b \leq (m + 1 - T(u)) - 1\}$. Com isso, pela definição de η, temos

$$S(m-(m-T(u))) + w(m-T(u)) - k + 1 \leq v \leq S(m-(m+1-T(u))) + w(m+1-T(u)) - k,$$

ou melhor

$$S(T(u)) + w(m - T(u)) - k + 1 \leq v \leq S(T(u) - 1) + w(m + 1 - T(u)) - k.$$

Como resultado imediato do item (1) do Lema 2.3.1, temos $u \leq S(T(u))$. Além disso, $S(T(u) - 1) \leq u - 1$, já que $S(T(u) - 1) = \max\{a \text{ tal que } a \in [0, m],\ T(a) \leq T(u) - 1\}$, pois caso $S(T(u) - 1) > u - 1$, isto é, $S(T(u) - 1) \geq u$, pela conexão de Galois, deveríamos ter $T(u) \leq T(u) - 1$, o que é uma contradição. Dessa forma, obtemos

$$u + w(m - T(u)) - k + 1 \leq v \leq u - 1 + w(m + 1 - T(u)) - k.$$

que implica

$$1 \leq v + k - u - w(m - T(u)) \leq w - 1.$$

Sendo assim, $v + k - u \not\equiv 0 \mod w$ e, logo, $u \not\equiv v + k \mod w$, como queríamos. □

A próxima proposição será fortemente utilizada na demonstração do Teorema Central.

Proposição 3.1.1. *Seja (T, S) uma conexão de Galois entre $[0, k]$ e $[0, m]$. Então, as afirmações abaixo são equivalentes:*

(1) $S(l) - S(l - 1) \leq w$, *para todo* $l \in [1, m]$;

(2) $|T^{-1}(l)| \leq w$, *para todo* $l \in [1, m]$;

(3) $T(r) + 1 \leq \max\{T(r + w), 1\}$, *para todo* $r \in [0, k - w]$.

Além disso, se $S(0) = 0$, então, para todo $a \in [1, k]$, $T(a) \in [1, m]$ e (1), (2) e (3) são equivalentes a

(4) $T(r) + 1(r + w)$, *para todo* $r \in [0, k - w]$.

Demonstração. (1) $\iff$ (2) Consideremos $l \in [1, m]$. Observemos que $l \neq \min([0, m])$ e $l - 1 = \max\{b \text{ tal que } b \in [0, m],\ b \leq l - 1\}$. Dessa forma, pelo item (4) do Lema 2.3.1, temos

$$T(a) = l \iff S(l - 1) + 1 \leq a \leq S(l).$$

Além disso, se $T(a) = l$, então $a \in T^{-1}(l)$, em que $T^{-1}(l) = \{d \text{ tal que } d \in [0, k],\ d \leq S(l)\}$. Logo,

$$\begin{aligned} |T^{-1}(l)| &= S(l) - (S(l - 1) + 1) + 1 \\ &= S(l) - S(l - 1). \end{aligned}$$

Portanto, $S(l) - S(l - 1) \leq w$ se, e somente se, $|T^{-1}(l)| \leq w$.

(1) $\Longrightarrow$ (3) Consideremos $r \in [0, k-w]$. Se $T(r+w) \leq 0$, então

$$T(r) + 1 \leq T(r+w) + 1 \leq 1,$$

o que implica $T(r) + 1 \leq \max\{T(r+w), 1\}$. Agora, se $T(r+w) \geq 0$, por hipótese, temos o seguinte:

$$S(T(r+w)) - S(T(r+w) - 1) \leq w.$$

Além disso, pelo item (1) do Lema 2.3.1, temos $r + w \leq S(T(r+w))$, o que junto à nossa hipótese, nos dá

$$r + w \leq S(T(r+w)) \leq w + S(T(r+w) - 1)$$

que implica

$$r \leq S(T(r+w) - 1).$$

Assim, como (T, S) é conexão de Galois, temos

$$T(r) \leq T(r+w) - 1,$$

o que nos dá $T(r) + 1 \leq T(r+w) = \max\{T(r+w), 1\}$, como desejado.

(3) $\Longrightarrow$ (1) Consideremos $l \in [1, m]$. Se $S(l) \leq w$, como $Im(S) \subseteq [0, k]$, então $S(l-1) \geq 0$, o que nos dá $S(l) - S(l-1) \leq w$. Agora, se $S(l) \geq w$, então $S(l) - w \in [0, k-w]$. Assim, por hipótese, temos

$$\begin{aligned} T(S(l) - w) + 1 &\leq \max\{T((S(l) - w) + w), 1\} \\ &= \max\{T(S(l)), 1\}. \end{aligned}$$

Além disso, pelo item (2) do Lema 2.3.1, obtemos $T(S(l)) \leq l$. Daí, como $l \geq 1$, temos $l \geq \max\{T(S(l)), 1\}$. Assim,

$$T(S(l) - w) + 1 \leq \max\{T(S(l)), 1\} \leq l,$$

que implica

$$T(S(l) - w) \leq l - 1$$

e que pela conexão de Galois (T, S), nos dá

$$S(l) - w \leq S(l-1).$$

Portanto, $S(l) - S(l-1) \leq w$, como desejado. □

Posto isso, podemos agora, apresentar demonstrar o Teorema Central.

Teorema 3.1.1. *Sejam (T, S) uma conexão de Galois entre $[0, k]$ e $[0, m]$, tal que $S(0) = 0$ e $S(l) - S(l-1) \leq w$, para todo $l \in [1, m]$ e também (τ, η) uma conexão de Galois entre $[0, wm - k]$ e $[0, m]$. Para qualquer $\gamma \in \mathbb{Z}$, defina os conjuntos $\mathcal{A}_\gamma$ e $\mathcal{B}_\gamma$ como*

$$\mathcal{A}_\gamma = \{T(u) \ \text{ tal que } \ u \in [1, k], \ u \equiv \gamma + k \mod w\} \ e$$

$$\mathcal{B}_\gamma = \{m + 1 - \tau(v) \ \text{ tal que } \ v \in [1, wm - k], \ v \equiv \gamma \mod w\}.$$

Então, as seguintes afirmações são equivalentes:

(1) *Para todo* $l \in [0, m]$, $\eta(l) = S(m-l) + wl - k$;

(2) $\eta(0) = 0$, $0 \leq \eta(l) - \eta(l-1) \leq w$, *para todo* $l \in [1, m]$ *e para todo* $(u, v) \in [0, k] \times [0, wm - k]$, *em que* $T(u) + \tau(v) = m + 1$, *é válido que* $u \not\equiv v + k \mod w$;

(3) *Para qualquer* $\gamma \in \mathbb{Z}$, $\mathcal{A}_\gamma \cap \mathcal{B}_\gamma = \emptyset$ *e* $\mathcal{A}_\gamma \cup \mathcal{B}_\gamma = [1, m]$;

(4) *Para qualquer* $\gamma \in \mathbb{Z}$, $\mathcal{A}_\gamma \cup \mathcal{B}_\gamma = [1, m]$.

Demonstração. Primeiramente, para qualquer $\gamma \in \mathbb{Z}$, consideremos os conjuntos abaixo:

$$\begin{aligned} \mathcal{U}_\gamma &= \{u \text{ tal que } u \in [1, k],\ u \equiv \gamma + k \mod w\}, \\ \mathcal{V}_\gamma &= \{v \text{ tal que } v \in [1, wm - k],\ v \equiv \gamma \mod w\} \end{aligned}$$

e observemos o seguinte:

$$\begin{aligned} \mathcal{U}_\gamma &= \{u \text{ tal que } u \in [1, k],\ u \equiv \gamma + k \mod w\} \\ &= \{u \text{ tal que } u \in [1, k],\ u \equiv \gamma + k + wm \mod w\}\} \\ &= \{u \text{ tal que } u \in [1, k],\ u - k - wm \equiv \gamma \mod w\}\} \end{aligned}$$

Com isso, consideremos o conjunto $\mathcal{U}_\gamma^* = \{a \text{ tal que } a \in [wm - k + 1, wm],\ a \equiv \gamma \mod w\}$. Dessa forma, podemos ver que $\mathcal{U}_\gamma$ tem uma correspondência biunívoca com $\mathcal{U}_\gamma^*$, pois

$$u \equiv \gamma + k \mod w \quad \text{se, e somente se,} \quad wm - k + u \equiv \gamma \mod w,$$

o que nos dá $|\mathcal{U}_\gamma| = |\mathcal{U}_\gamma^*|$. Por outro lado, vejamos o grupo finito $\mathbb{Z}_{wm} = [0, wm - 1]$. Observemos que $\mathbb{Z}_{wm} = [1, wm-k] \cup [wm-k+1, wm]$, em que esta, é uma união disjunta. Além disso, $\mathcal{V}_\gamma \subseteq [1, wm - k]$ e $\mathcal{U}_\gamma^* \subseteq [wm - k + 1, wm]$, de modo que $\mathcal{U}_\gamma^* \cup \mathcal{V}_\gamma$ é a classe de γ em $\mathbb{Z}_{wm}$, com $\mathcal{U}_\gamma^* \cap \mathcal{V}_\gamma = \emptyset$. Os restos de divisão por w possíveis são $0, 1, \ldots, w - 1$, assim, teremos w classes de congruência. Dessa maneira, obtemos o seguinte:

$$\begin{aligned} |\mathcal{U}_\gamma| + |\mathcal{V}_\gamma| &= |\mathcal{U}_\gamma^*| + |\mathcal{V}_\gamma| \\ &= |\mathcal{U}_\gamma^* \cup \mathcal{V}_\gamma| \\ &= \frac{|\mathbb{Z}_{wm}|}{w} \\ &= m. \end{aligned}$$

Portanto, $|\mathcal{U}_\gamma| + |\mathcal{V}_\gamma| = m$. E, com isso, seguiremos com as implicações.

(1) $\Longrightarrow$ (2) Segue imediatamente do Lema 3.1.1.

(2) $\Longrightarrow$ (3) Fixemos $\gamma \in \mathbb{Z}$ e consideremos $u \in \mathcal{U}_\gamma$ e $v \in \mathcal{V}_\gamma$. Assim, como $v \equiv \gamma \mod w$, temos $u \equiv v + k \mod w$ e, por hipótese, $T(u) \neq m + 1 - \tau(v)$. Logo, $\mathcal{A}_\gamma \cap \mathcal{B}_\gamma = \emptyset$. Pela Proposição 3.1.1, como $S(0) = 0$, então $T(a) \in [1, m]$, para todo $a \in [1, k]$ e $T(r) + 1 \leq T(r + w)$, para todo $r \in [0, k - w]$, o que implica $\mathcal{A}_\gamma \subseteq [1, m]$ e

$|\mathcal{A}_\gamma| = |\mathcal{U}_\gamma|$, pois r e $r+w$ pertencem à mesma classe de congruência módulo w, mas $T(r) < T(r+w)$, ou seja, se $a \equiv b \equiv \gamma + k \mod w$, em que $a \neq b$, então $T(a), T(b) \in \mathcal{A}_\gamma$ e $T(a) \neq T(b)$. Agora, novamente pela Proposição 3.1.1, como $\eta(0) = 0$, então $\tau(a) \in [1, m]$, para todo $a \in [0, wm - k]$ e $\tau(r) + 1 \leq \tau(r + w)$, para todo $r \in [0, w(m-1) - k]$, o que implica $\mathcal{B}_\gamma \subseteq [1, m]$ e $|\mathcal{B}_\gamma| = |\mathcal{V}_\gamma|$, pela mesma justificativa dada anteriormente. Logo, $|\mathcal{A}_\gamma| + |\mathcal{B}_\gamma| = |\mathcal{U}_\gamma| + |\mathcal{V}_\gamma| = m$. Assim, como $\mathcal{A}_\gamma \cap \mathcal{B}_\gamma = \emptyset$, obtemos $|\mathcal{A}_\gamma \cup \mathcal{B}_\gamma| = m$. Por fim, como $\mathcal{A}_\gamma \cup \mathcal{B}_\gamma \subseteq [1, m]$, obtemos $\mathcal{A}_\gamma \cup \mathcal{B}_\gamma = [1, m]$, como queríamos.

(3) $\Longrightarrow$ (4) Segue de forma imediata.

(4) $\Longrightarrow$ (3) Fixemos $\gamma \in \mathbb{Z}$. Da forma em que os conjuntos $\mathcal{A}_\gamma, \mathcal{U}_\gamma, \mathcal{B}_\gamma$ e $\mathcal{V}_\gamma$ foram definidos, temos de imediato $|\mathcal{A}_\gamma| \leq |\mathcal{U}_\gamma|$ e $|\mathcal{B}_\gamma| \leq |\mathcal{V}_\gamma|$. Como $|\mathcal{U}_\gamma| + |\mathcal{V}_\gamma| = m$ e, por hipótese, $\mathcal{A}_\gamma \cup \mathcal{B}_\gamma = [1, m]$, temos então $|\mathcal{A}_\gamma| + |\mathcal{B}_\gamma| \leq m = |\mathcal{A}_\gamma \cup \mathcal{B}_\gamma|$. Mas, observemos o seguinte:

$$m \leq |\mathcal{A}_\gamma \cup \mathcal{B}_\gamma| + |\mathcal{A}_\gamma \cap \mathcal{B}_\gamma| \leq |\mathcal{A}_\gamma| + |\mathcal{B}_\gamma| \leq |\mathcal{U}_\gamma| + |\mathcal{V}_\gamma| = m.$$

Logo, $|\mathcal{A}_\gamma \cup \mathcal{B}_\gamma| + |\mathcal{A}_\gamma \cap \mathcal{B}_\gamma| = m$, e como $|\mathcal{A}_\gamma \cup \mathcal{B}_\gamma| = m$, temos $|\mathcal{A}_\gamma \cap \mathcal{B}_\gamma| = 0$, o que nos dá $\mathcal{A}_\gamma \cap \mathcal{B}_\gamma = \emptyset$, como queríamos.

(3) $\Longrightarrow$ (1) Pelo Lema 3.1.1, sabemos que existe uma conexão de Galois (ξ, ζ) entre $[0, wm - k]$ e $[0, m]$, tal que $\zeta(l) = S(m - l) + wl - k$, para todo $l \in [0, m]$ e $\zeta(0) = 0$. Assim, pela Proposição 3.1.1, temos

$$\xi(r) + 1 \leq \xi(r + w), \text{ para todo } r \in [0, w(m-1) - k]. \tag{3.1}$$

Dito isto, definamos o conjunto $\mathcal{L}_\gamma = \{m + 1 - \xi(v) \text{ tal que } v \in \mathcal{V}_\gamma\}$, para um $\gamma \in \mathbb{Z}$ fixo. Assim, com um processo semelhante ao feito com a conexão (τ, η) no passo (2) $\Longrightarrow$ (3), desta vez com a conexão (ξ, ζ), temos $\mathcal{A}_\gamma \cap \mathcal{L}_\gamma = \emptyset$ e $\mathcal{A}_\gamma \cup \mathcal{L}_\gamma = [1, m]$. Com isso, como $\mathcal{A}_\gamma \cap \mathcal{B}_\gamma = \emptyset$ e $\mathcal{A}_\gamma \cup \mathcal{B}_\gamma = [1, m]$, temos $\mathcal{L}_\gamma = \mathcal{B}_\gamma$. Agora, definamos as funções $f : \mathcal{V}_\gamma \to \mathbb{Z}$ e $g : \mathcal{V}_\gamma \to \mathbb{Z}$, como $f(v) = m + 1 - \tau(v)$ e $g(v) = m + 1 - \xi(v)$, respectivamente. Dessa forma, obtemos

$$Im(f) = \mathcal{B}_\gamma = \mathcal{L}_\gamma = Im(g).$$

Como τ e ξ preservam a ordem usual, para quaisquer $a, b \in \mathcal{V}_\gamma$, em que $a \leq b$, temos $f(a) \geq f(b)$ e $g(a) \geq g(b)$. Além disso, como 3.1 acontece, temos g como uma função injetora. Assim, $f = g$. De fato, consideremos $\mathcal{V}_\gamma = \{v_1, v_2, \ldots, v_n\}$, tal que $v_1 < v_2 < \cdots < v_n$ e desse modo, $g(v_1) > g(v_2) > \cdots > g(v_n)$. Agora, suponhamos que exista $v_i \in \mathcal{V}_\gamma$, tal que $f(v_j) = g(v_j)$, para $v_j < v_i$ e $f(v_i) \neq g(v_i)$. Dessa forma, obtemos os seguintes dois casos:

(1) $f(v_i) > g(v_i)$. Como $Im(f) = Im(g)$, existe $v_l \in \mathcal{V}_\gamma$, tal que $f(v_i) = g(v_l)$. Assim, obtemos $g(v_l) > g(v_i)$, o que implica $v_l < v_i$ e $f(v_l) = g(v_l)$, ou seja,

$$f(v_l) = g(v_l) = f(v_i), \text{ com } v_l < v_i.$$

Logo, existe $c \in Im(g)$, tal que $c \notin Im(f)$, o que é uma contradição, pois $|Im(f)| = |Im(g)| = |\mathcal{V}_\gamma|$.

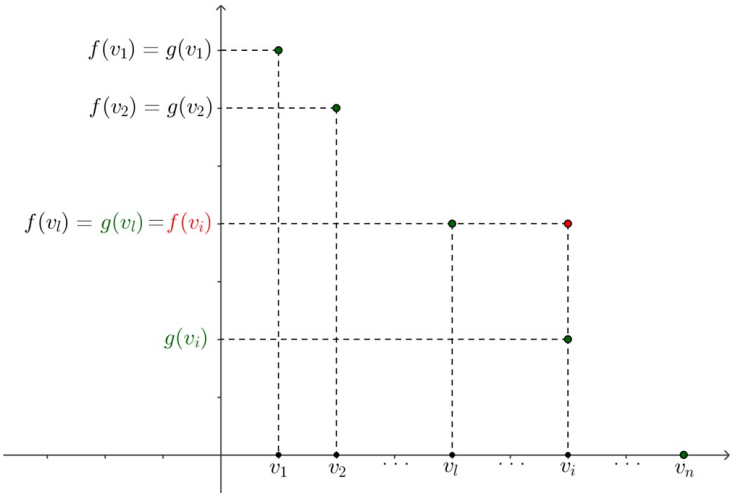

Figura 3 – $f(v_i) > g(v_i)$.

(2) $f(v_i) < g(v_i)$. Neste caso, $g(v_i) \in Im(g)$, mas $g(v_i) \notin Im(f)$, já que f é decrescente, o que é uma contradição, pois $Im(f) = Im(g)$.

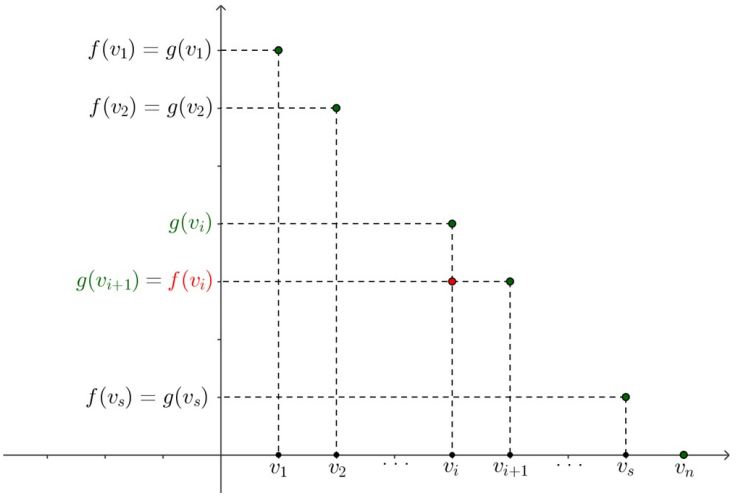

Figura 4 – $f(v_i) < g(v_i)$.

Com isso, $\tau(v) = \xi(v)$, para todo $v \in [1, wm - k]$, com $v \equiv \gamma \mod w$. Assim, pela arbitrariedade de γ, temos $\tau(v) = \xi(v)$, para todo $v \in [1, wm - k]$. Agora, pelo item (3) do Lema 2.3.1, observemos o seguinte:

$$\xi^{-1}(0) = \{a \text{ tal que } a \in [0, wm - k],\ a \leq \zeta(0)\}.$$

Já, pelo item (1), do Lema 3.1.1, temos $\zeta(0) = 0$, o que nos dá $\xi(0) = 0$. De modo semelhante,

$$\tau^{-1}(0) = \{a \text{ tal que } a \in [0, wm - k],\ a \leq \eta(0)\},$$

mas $\eta(0) \in [0, wm-k]$, logo $0 \in \tau^{-1}(0)$, o que nos dá $\tau(0) = 0$. Isso implica $\tau = \xi$. Em razão de, (τ, η) e (ξ, ζ) serem conexões de Galois entre $[0, wm-k]$ e $[0, m]$, pelo item (2) do Lema 2.3.1, para qualquer $\mu \in [0, m]$, temos o seguinte:

$$\begin{aligned}\eta(\mu) &= \max\{a \text{ tal que } a \in [0, wm-k],\ \tau(a) \leq \mu\} \\ &= \max\{a \text{ tal que } a \in [0, wm-k],\ \xi(a) \leq \mu\} \\ &= \zeta(\mu).\end{aligned}$$

Portanto, $\eta = \zeta$, o que nos dá (1), como queríamos. □

3.2 O Teorema da Ponte

Nesta seção, estabeleceremos condições para a prova do Teorema da Ponte, o enunciaremos e veremos uma demonstração para o mesmo. O Teorema da Ponte será de grande ajuda para aplicações do Teorema Central que apresentaremos neste trabalho. Para os resultados apresentados nesta seção, consideraremos conjuntos não vazios Y e X, $m, k \in \mathbb{N}$, $w \in \mathbb{Z}^+$, uma função sobrejetiva $g : Y \to [0, m]$, uma função $f : Y \to [0, k]$ que satisfaz:

$$\forall y \in Y,\ g(y) = 0 \Rightarrow f(y) = 0; \tag{3.2}$$

$$\forall y \in Y,\ wg(y) - f(y) \leq wm - k; \tag{3.3}$$

$$\forall u \in Y, \text{ tal que } g(u) \leq m-1,\ \exists\, v \in Y \text{ tal que } g(v) = g(u)+1,\ \ f(u) \leq f(v); \tag{3.4}$$

$$\forall v \in Y, \text{ tal que } g(v) \geq 1,\ \exists\, u \in Y \text{ tal que } g(u) = g(v)-1,\ \ f(v) - f(u) \leq w, \tag{3.5}$$

e ainda, uma função sobrejetiva $\sigma : X \to Y$.

Agora, definamos as funções $\mu : X \to [0, m]$ como

$$\mu(t) = m - g(\sigma(t)), \tag{3.6}$$

e $h : X \to \mathbb{Z}$ como

$$h(t) = f(\sigma(t)) + w\mu(t) - k. \tag{3.7}$$

A partir disso, com relação à (g, f) definamos as funções $T : [0, k] \to [0, m]$ como

$$T(a) = \min\{g(u) \text{ tal que } u \in Y,\ a \leq f(u)\}, \tag{3.8}$$

e $S : [0, m] \to [0, k]$ como

$$S(b) = \max\{f(u) \text{ tal que } u \in Y,\ g(u) \leq b\}. \tag{3.9}$$

E, de modo semelhante, agora com relação à (μ, h), definamos as funções $\tau : [0, wm-k] \to [0, m]$ como

$$\tau(a) = \min\{\mu(t) \text{ tal que } t \in X,\ a \leq h(u)\}, \tag{3.10}$$

e $\eta : [0, m] \to [0, wm - k]$ como

$$\eta(b) = \min\{h(t) \text{ tal que } t \in X,\ \mu(t) \leq b\}. \tag{3.11}$$

Antes de apresentarmos o teorema principal desta seção e uma demonstração para o mesmo, façamos algumas considerações a respeito das funções g, f, μ e h definidas acima.

(i) Se $y \in Y$ com $g(y) = m$, como $Im(f) \subseteq [0, k]$, $f(y) \leq k$ e por 3.3, temos $wm - f(y) \leq wm - k$, o que nos dá, $-f(y) \leq -k$, ou seja, $f(y) \geq k$. Logo, $f(y) = k$. Portanto, para qualquer $y \in Y$ com $g(y) = m$, temos $f(y) = k$;

(ii) Percebamos que g e σ são funções sobrejetivas e, por consequência, a composição $g \circ \sigma$ também é. Desse modo, como $Im(g \circ \sigma)$ percorre por todo elemento de $[0, m]$, μ também percorrerá e portanto, a função $\mu : X \to [0, m]$ é sobrejetiva. Agora, utilizando novamente o argumento de g ser uma função sobrejetiva, existe $y \in Y$, tal que $g(y) = 0$, digamos $y = \sigma(t)$, para algum $t \in X$. Desse modo,

$$\begin{aligned} h(t) &= f(\sigma(t)) + w\mu(t) - k \\ &= 0 + wm - k, \end{aligned}$$

pois, por 3.2, $f(\sigma(t)) = 0$. Logo, $wm - k \in Im(h)$ e, mais ainda, este é o maior valor que h pode atingir. Como, por 3.3, $f(\sigma(t)) - wg(\sigma(t)) \geq -wm + k$, temos

$$\begin{aligned} h(t) &= f(\sigma(t)) + w\mu(t) - k \\ &= f(\sigma(t)) - wg(\sigma(t)) + wm - k \\ &\geq 0. \end{aligned}$$

E, portanto, $Im(h) \subseteq [0, wm - k]$.

(iii) Por fim, seja $c \in X$, com $\mu(c) \leq m - 1$. A partir disso, obtemos $m - g(\sigma(c)) \leq m - 1$, o que nos dá $g(\sigma(c)) \geq 1$. Assim, por 3.3 e por σ ser uma função bijetiva, existe $\sigma(d) \in Y$, tal que $g(\sigma(d)) = g(\sigma(c)) - 1$ e $f(\sigma(c)) - f(\sigma(d)) \leq w$. Com isso, $\mu(d) = \mu(c) + 1$ e

$$\begin{aligned} h(c) &= f(\sigma(c)) + w\mu(c) - k \\ &= f(\sigma(c)) - wg(\sigma(c)) + wm - k \\ &\leq w + f(\sigma(d)) - wg(f(\sigma(d))) - w + wm - k \\ &= f(\sigma(d)) - wg(f(\sigma(d))) + wm - k \\ &= f(\sigma(d)) + w\mu(d) - k \\ &= h(d) \end{aligned}$$

Portanto, para qualquer $c \in X$ com $\mu(c) \leq m-1$, existe $d \in X$ tal que $\mu(d) = \mu(c)+1$ e $h(c) \leq h(d)$.

Isto posto, podemos agora, enunciar e provar o Teorema da Ponte.

Teorema 3.2.1. *As funções T, S, τ e η estão bem definidas. Além disso:*

(1) *(T, S) é conexão de Galois entre $[0, k]$ e $[0, m]$;*

(2) *Para todo $b \in [0, m]$, $S(b) = \max\{f(u)$ tal que $u \in Y$, $g(u) = b\}$;*

(3) *$S(0) = 0$, e para qualquer $l \in [1, m]$, temos $S(l) - S(l-1) \leq w$;*

(4) *(τ, η) é conexão de Galois entre $[0, wm - k]$ e $[0, m]$;*

(5) *Para todo $b \in [0, m]$, $\eta(b) = \max\{h(t)$ tal que $t \in X$, $\mu(u) = b\}$;*

(6) *Para qualquer $l \in [0, m]$, $\eta(l) = S(m - l) + wl - k$;*

(7) *Para qualquer $\gamma \in \mathbb{Z}$, definamos*

$$\mathcal{A}_\gamma = \{T(u) \text{ tal que } u \in [1, k],\ u \equiv \gamma + k \mod w\} \text{ e}$$

$$\mathcal{B}_\gamma = \{m + 1 - \tau(v) \text{ tal que } v \in [1, wm - k],\ v \equiv \gamma \mod w\}.$$

E então, $\mathcal{A}_\gamma \cap \mathcal{B}_\gamma = \emptyset$ e $\mathcal{A}_\gamma \cup \mathcal{B}_\gamma = [1, m]$.

Demonstração. Temos g como uma função sobrejetora e, por (i), que $k \in Im(f)$. Desse modo, as funções T e S estão bem definidas. E ainda, por (ii), temos as funções τ e η também bem definidas. Observemos pois, que os itens (1) e (4) seguem do Lema 2.3.2. Além disso, o item (2) pode ser obtido por um processo similar ao feito na demonstração do Teorema 2.3.2. Desta vez, para o item (3), primeiro observemos que, da forma que temos definido S, $S(0) = \max\{f(u)$ tal que $u \in Y$, $g(u) \leq 0\}$. Assim, como $Img \subseteq [0, m]$, então $g(u) = 0$, o que por 3.2, nos dá $f(u) = 0$. Logo, $S(0) = 0$. Agora, tomemos $l \in [1, m]$. Temos, por definição, $S(l) = \max\{f(v)$ tal que $v \in X$, $g(v) \leq l\}$. Pelo item (2), para todo $b \in [0, m]$, temos $S(b) = \max\{f(u)$ tal que $u \in Y$, $g(u) = b\}$. Daí, como $l \geq 1$, obtemos $g(v) \geq 1$. Com isso, por 3.5, existe $u \in Y$ tal que $g(u) = g(v) - 1$ e $f(v) - f(u) \leq w$. Assim, observemos o seguinte:

$$g(u) \leq l \Longrightarrow g(u) + 1 \leq l \Longrightarrow g(u) \leq l - 1.$$

E assim, $S(l-1) = \max\{f(u)$ tal que $u \in Y$, $g(u) \leq l - 1\}$. Considerando $S(l) = f(v)$ e $S(l-1) = f(u)$, temos $S(l) - S(l-1) \leq w$. Ademais, assim como o item (2), o item (5) pode ser obtido por um processo similar ao feito na demonstração do Teorema 2.3.2. Por fim, tomemos algum $l \in [0, m]$. Como $\sigma : X \to Y$ é uma função bijetiva, em particular é sobrejetiva, e logo, podemos considerar o conjunto

$$\{\sigma(t) \text{ tal que } t \in X,\ \mu(t) = l\} = \{u \text{ tal que } u \in Y,\ g(u) = m - l\}.$$

Logo, pelos itens (2) e (5), temos o seguinte:

$$\begin{aligned}
\eta(l) &= \max\{f(\sigma(t)) + w\mu(t) - k \text{ tal que } t \in X,\ \mu(t) = l\} \\
&= \max\{f(\sigma(t)) + wl - k \text{ tal que } t \in X,\ \mu(t) = l\} \\
&= \max\{f(\sigma(t)) \text{ tal que } t \in X,\ \mu(t) = l\} + wl - k \\
&= \max\{f(u) \text{ tal que } u \in Y,\ g(u) = m - l\} + wl - k \\
&= S(m - l) + wl - k,
\end{aligned}$$

o que nos dá exatamente o item (6). Por fim, pelos itens $(1), (3), (4)$ e (6), e aplicando o Teorema 3.1.1, obtemos o item (7) de modo imediato. □

4 Aplicações dos Principais Resultados

Neste capítulo, apresentaremos aplicações do Teorema Central para w-demi matroides e w-demi polimatroides. Estas estruturas, são generalizações de demi-matroide, que vimos anteriormente neste trabalho. Aqui, veremos w-demi matroides definidos sobre conjuntos finitos e w-demi polimatroides definidos sobre módulos com série de composições. As principais referências utilizadas foram [5], [15] e [20].

4.1 w-Demi matroides

Nesta seção, veremos a definição de w-demi matroide e uma aplicação do Teorema Central para esta estrutura. Consideremos E como um conjunto finito de m elementos e $\mathcal{P}(E)$ o *conjunto das partes de* E, isto é, o conjunto formado por todos os subconjuntos de E.

Definição 4.1.1. *Para quaisquer função* $f : \mathcal{P}(E) \to \mathbb{Z}$ *e* $w \in \mathbb{Z}^+$, *o par* (E, f) *é dito um* w*-demi matroide se*

(1) $f(\emptyset) = 0$

(2) *Para quaisquer* $A, B \subseteq E$, *com* $A \subseteq B$, *temos* $0 \leq f(B) - f(A) \leq w(|B| - |A|)$.

A proposição a seguir, nos introduz a noção de um w-demi matroide dual ao w-demi matroide (E, f).

Proposição 4.1.1. *Para* $w \in \mathbb{Z}^+$ *e um* w*-demi matroide* (E, f), *defina a função* $h : \mathcal{P}(E) \to \mathbb{Z}$ *como* $h(A) = f(E - A) + w|A| - f(E)$. *Então,* (E, h) *é um* w*-demi matroide com* $h(E) = wm - f(E)$.

Demonstração. Primeiro, vejamos que

$$h(\emptyset) = f(E - \emptyset) + w|\emptyset| - f(E) = f(E) + w \cdot 0 - f(E) = 0.$$

Logo, a primeira condição para w-demi matroide é válida. Além disso, consideremos $A \subseteq B \subseteq E$. Dessa forma, vejamos o seguinte:

$$\begin{aligned} h(B) - h(A) &= f(E - B) + w|B| - f(E) - (f(E - A) + w|A| - f(E)) \\ &= f(E - B) + w|B| - f(E - A) - w|A| \\ &= f(E - B) - f(E - A) + w(|B| - |A|). \end{aligned}$$

Com isso, observemos que $E - B \subseteq E - A$, e assim, $f(E - B) - f(E - A) \leq 0$. Ademais, $f(E-A)-f(E-B) \leq w(|E-A|-|E-B|) = w(|B|-|A|)$, ou seja, $f(E-B)-f(E-A) \geq -w(|B| - |A|)$. Portanto, $0 \leq h(B) - h(A) \leq w(|B| - |A|)$, o que nos dá, (E, h), um w-demi matroide. □

A proposição anterior, determina um novo w-demi matroide, (E, h), que pode ser considerado como o w-demi matroide dual de (E, f). Por sua vez, o w-demi matroide (E, f) também pode ser considerado como o w-demi matroide dual de (E, h). Agora, para que possamos, neste contexto, definir o peso generalizado e o perfil de dimensão/comprimento, precisaremos da definição de um subconjunto $\mathcal{C}$ de $\mathcal{P}(E)$ chamado *abundante*.

Definição 4.1.2. *Um conjunto $\mathcal{C} \subseteq \mathcal{P}(E)$ é dito abundante se $\mathcal{C} \neq \emptyset$ e as seguintes condições são satisfeitas:*

(1) *Para qualquer $A \in \mathcal{C}$ com $A \subsetneq E$, existe $B \in \mathcal{C}$, tal que $A \subseteq B$ e $|B| = |A| + 1$.*

(2) *Para qualquer $B \in \mathcal{C}$ com $B \neq \emptyset$, existe $A \in \mathcal{C}$, tal que $A \subseteq B$ e $|A| = |B| - 1$.*

É imediato percebermos a condição de que se $\mathcal{C} \subseteq \mathcal{P}(E)$ é abundante, então os conjuntos $\emptyset$ e E pertencem a $\mathcal{C}$ e para todo $r \in [0, m]$, existe $A \in \mathcal{C}$ com $|A| = r$. E ainda, que o conjunto $\mathcal{D} = \{E - A \text{ tal que } A \in \mathcal{C}\}$ é abundante se, e somente se, $\mathcal{C}$ é abundante.

Além disso, assumiremos um poset P, sobre o conjunto E e ordem $\preceq_P$. Observemos pois, que o conjunto dos ideais de ordem, o qual denotaremos por $\mathcal{I}(P)$, é abundante. Com efeito, seja $\langle A\rangle_P \in \mathcal{I}(P)$, com $\langle A\rangle_P \subsetneq E$. Assim, existe $x \in E$ tal que $x \notin \langle A\rangle_P$ e não exista nenhum outro elemento de E entre x e algum elemento de $\langle A\rangle_P$. Logo, existe um ideal de ordem $\langle B\rangle_P$ tal que $\langle B\rangle_P = \langle A\rangle_P + x$, ou seja, $\langle A\rangle_P \subseteq \langle B\rangle_P$ e $|\langle B\rangle_P| = |\langle A\rangle_P| + 1$. E ainda, seja $\langle B\rangle_P \in \mathcal{I}(P)$, com $\langle B\rangle_P \neq \emptyset$. Com isso, há pelo menos um elemento máximo em $\langle B\rangle_P$, digamos x. Dessa forma, seja $y \in E$ tal que $y \preceq_P x$. Assim, existe um ideal $\langle A\rangle_P$, tal que $|\langle A\rangle_P| = |\langle B\rangle_P| - 1$. Se y não existir, temos $\langle A\rangle_P = \emptyset$. A partir disso, obtemos $\mathcal{I}(\overline{P}) = \{E - \langle B\rangle_P \text{ tal que } \langle B\rangle_P \in \mathcal{I}(P)\}$, sendo $\overline{P}$ o poset dual a P.

Agora, tendo em vista a definição de um conjunto abundante, podemos seguir utilizando-a para determinarmos pesos generalizados e perfis para um w-demi matroide.

Definição 4.1.3. *Para $w \in \mathbb{Z}^+$, seja (E, f) um w-demi matroide com $f(E) = k$.*

(1) *Seja $\mathcal{C} \subseteq \mathcal{P}(E)$, um conjunto abundante. Para qualquer $a \in [0, k]$, o a-ésimo peso generalizado de $(f, \mathcal{C})$, denotado por $d_a(f, \mathcal{C})$, é definido como*

$$d_a(f, \mathcal{C}) = \min\{|B| \text{ tal que } B \in \mathcal{C},\ a \leq f(B)\},$$

e para qualquer $b \in [0, m]$, o b-ésimo perfil de $(f, \mathcal{C})$, denotado por $K_b(f, \mathcal{C})$, é definido como

$$K_b(f, \mathcal{C}) = \max\{f(B) \text{ tal que } B \in \mathcal{C},\ |B| = b\}.$$

(2) *Seja $P = (E, \preceq_P)$ um poset. Para qualquer $a \in [0, k]$, o a-ésimo peso generalizado de (f, P) é definido como $d_a(f, P) = d_a(f, \mathcal{I}(P))$, e para qualquer $b \in [0, m]$, o b-ésimo perfil de $(f, \mathcal{C})$, é definido como $K_b(f, P) = K_b(f, \mathcal{I}(P))$.*

Sendo assim, podemos agora, apresentar o teorema principal desta seção.

Teorema 4.1.1. *Seja $w \in \mathbb{Z}^+$. Consideremos (E, f) um w-demi matroide, com $f(E) = k$ e um poset $P = (E, \preceq_P)$. Definamos uma função $h : \mathcal{P}(E) \to \mathbb{Z}$ como $h(B) = f(E - B) + w|B| - k$ e assumamos o conjunto abundante $\mathcal{C} \subseteq \mathcal{P}(E)$ e $\mathcal{D} = \{E - A \text{ tal que } A \in \mathcal{C}\}$. Desse modo, as seguintes condições são válidas:*

(1) *Para qualquer $l \in [0, m]$, $K_l(h, \mathcal{D}) = K_{m-l}(f, \mathcal{C}) + wl - k$;*

(2) *Para qualquer $\gamma \in \mathbb{Z}$, defina*

$$\mathcal{A}_\gamma = \{d_u(f, \mathcal{C}) \text{ tal que } u \in [1, k],\ u \equiv \gamma + k \mod w\} \text{ e}$$

$$\mathcal{B}_\gamma = \{m + 1 - d_v(h, \mathcal{D}) \text{ tal que } v \in [1, wm - k],\ v \equiv \gamma \mod w\}.$$

E então, temos $\mathcal{A}_\gamma \cap \mathcal{B}_\gamma = \emptyset$ e $\mathcal{A}_\gamma \cup \mathcal{B}_\gamma = [1, m]$;

(3) *Para qualquer $l \in [0, m]$, $K_l(h, \overline{P}) = K_{m-l}(f, P) + wl - k$;*

(4) *Para qualquer $\gamma \in \mathbb{Z}$, defina*

$$\mathcal{G}_\gamma = \{d_u(f, P) \text{ tal que } u \in [1, k],\ u \equiv \gamma + k \mod w\} \text{ e}$$

$$\mathcal{H}_\gamma = \{m + 1 - d_v(h, \overline{P}) \text{ tal que } v \in [1, wm - k],\ v \equiv \gamma \mod w\}.$$

E então, temos $\mathcal{G}_\gamma \cap \mathcal{H}_\gamma = \emptyset$ e $\mathcal{G}_\gamma \cup \mathcal{H}_\gamma = [1, m]$.

Demonstração. Definamos uma função $g : \mathcal{C} \to [0, m]$, em que $g(A) = |A|$. Como $\mathcal{C}$ é abundante, g é uma função sobrejetiva. Além disso, como (E, f) é um w-demi matroide com $f(E) = k$, a função f restrita à $\mathcal{C}$, $f|_{\mathcal{C}}$, é uma função de $\mathcal{C}$ à $[0, k]$, em que $k \in \mathbb{N}$. Dessa forma, considerando as funções g e $f|_{\mathcal{C}}$, as condições 3.2 à 3.5 são válidas. Agora, definamos uma função $\sigma : \mathcal{D} \to \mathcal{C}$, em que $\sigma(B) = E - B$. Pela definição do conjunto $\mathcal{D}$, temos, de imediato, σ como uma função bijetiva. Além disso, definamos também uma função $\mu : \mathcal{D} \to \mathbb{Z}$, em que $\mu(B) = m - g(\sigma(B))$ e consideremos $h|_{\mathcal{D}} : \mathcal{D} \to \mathbb{Z}$. Desse modo,

$$\mu(B) = m - g(E - B) = m - |E - B| = m - |E| + |B| = |B|$$

e com isso, temos

$$h|_{\mathcal{D}}(B) = f|_{\mathcal{C}}(\sigma(B)) + w \cdot \mu(B) - k.$$

Nestas circunstâncias, definamos, por fim, as funções T, S, τ e η, tais como nas condições de 3.8 à 3.11, desta vez considerando $(g, f|_{\mathcal{C}})$ e $(\mu, h|_{\mathcal{D}})$, respectivamente. Logo, pela

Definição 4.1.3, $T(a) = \mathrm{d}_a(f, \mathcal{C})$, para $a \in [0, k]$ e $S(b) = \mathrm{K}_b(f, \mathcal{C})$, para $b \in [0, m]$. E ainda, $\tau(a) = \mathrm{d}_a(h, \mathcal{D})$, para $a \in [0, wm - k]$ e $\eta(b) = \mathrm{K}_b(h, \mathcal{D})$, para $b \in [0, m]$. Portanto, aplicando o Teorema da Ponte (3.2.1), temos exatamente o que queríamos para as condições (1) e (2). As condições (3) e (4) seguem de modo semelhante ao feito para (1) e (2), juntamente com o item (2) da Definição 4.1.3. □

4.2 w-Demi polimatroides

Nesta seção, veremos uma definição de w-demi polimatroide e uma aplicação do Teorema Central para esta estrutura. Antes de começarmos, devemos fazer algumas considerações, as quais usaremos ao longo do texto. Deste modo, considerando A e B anéis com unidade, utilizaremos da estrutura de módulos sobre um anel com unidade, definidos da seguinte forma:

Definição 4.2.1. *Um módulo à esquerda M sobre um anel com unidade A, ou um A-módulo à esquerda, é um grupo abeliano $(M, +)$ em conjunto com uma operação*

$$A \times M \to M, \quad (a, v) \mapsto av,$$

a qual para todos $a, b \in A$, e todos $x, x_1, x_2 \in M$, satisfaz as seguintes propriedades:

(1) $a(x_1 + x_2) = ax_1 + ax_2$;

(2) $(a + b)x = ax + bx$;

(3) $a(bx) = (ab)x$;

(4) $1x = x$.

Além disso, precisamos definir e estabelecer algumas condições para os módulos que trabalharemos. Sendo assim, para qualquer M sendo um A-módulo à esquerda, M é dito *simples* se $M \neq \{0\}$ e não possui A-submódulos além de $\{0\}$ e M. Ademais, definimos também uma *série de composições* de M como uma cadeia de A-submódulos à esquerda $\{0\} = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_{t-1} \subseteq L_t = M$, em que $t \in \mathbb{N}$ e L_i/L_{i-1} é um A-módulo à esquerda simples, para todo $i \in [1, t]$. Observemos pois, que todas as definições acima, também são válidas para B-módulos à direita. A propósito, denotaremos por $\mathcal{P}(M)$, o conjunto de todos os A-submódulos à esquerda de M e consideraremos Ω como uma coleção não vazia de A-módulos simples.

Definiremos, agora, uma função p_Ω, que será de grande importância para nossa definição de um conjunto abundante. Desse modo, para qualquer A-módulo à esquerda M com série de composições $\{0\} = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_{t-1} \subseteq L_t = M$, definamos uma função p_Ω, de modo que,

$$p_\Omega(M) = |\{i \in [0, t] \text{ tal que } \exists\, W \in \Omega \text{ tal que } L_i/L_{i-1} \cong W\}|. \tag{4.1}$$

Pelo Teorema de Jordan-Hölder, todas as séries de composições de M são equivalentes [5], ou seja, $p_\Omega(M)$ independe da escolha da série de composições, logo, está bem definida. Por sua vez, também consideraremos, nesta seção, uma noção de um conjunto abundante, porém no contexto de p_Ω, o que nos leva à seguinte definição:

Definição 4.2.2. *Sejam M um A-módulo à esquerda com uma série de composições e $\Phi \subseteq \mathcal{P}(M)$. Então, (M, Φ, p_Ω) é dito abundante se as seguintes condições são satisfeitas:*

(1) $\{0\}, M \in \Phi$;

(2) *Para qualquer $C \in \Phi$ com $p_\Omega(C) \leq p_\Omega(M) - 1$, existe $D \in \Phi$ tal que $C \subseteq D$ e $p_\Omega(D) = p_\Omega(C) + 1$;*

(3) *Para qualquer $D \in \Phi$ com $p_\Omega(D) \geq 1$, existe $C \in \Phi$ tal que $C \subseteq D$ e $p_\Omega(C) = p_\Omega(D) - 1$.*

A função p_Ω preserva algumas propriedades de dimensão de espaços vetoriais, como mostra o Lema seguinte.

Lema 4.2.1. *Seja M um A-módulo à esquerda com uma série de composições. Então:*

(1) *$(M, \mathcal{P}(M), p_\Omega)$ é abundante;*

(2) *Para quaisquer $U, V \in \mathcal{P}(M)$ com $U \subseteq V$, $p_\Omega(V) = p_\Omega(U) + p_\Omega(V/U)$;*

(3) *Para quaisquer $X, Y \in \mathcal{P}(M)$, $p_\Omega(X + Y) + p_\Omega(X \cap Y) = p_\Omega(X) + p_\Omega(Y)$.*

Demonstração. A demonstração deste Lema está fora do escopo desta dissertação e pode ser encontrada em [20]. □

Agora, tendo em vista a definição de um conjunto abundante no contexto de p_Ω, podemos seguir para a definição de pesos generalizados e perfis de dimensão/comprimento para o contexto de w-demi polimatroide sobre módulos com série de composições. Primeiramente, definiremos w-demi polimatroide e, logo após, pesos generalizados e perfis de dimensão/comprimento.

Definição 4.2.3. *Seja M um A-módulo à esquerda com uma série de composições. Para quaisquer $f : \mathcal{P}(M) \to \mathbb{Z}$ e $w \in \mathbb{Z}^+$, (M, f, Ω) é dito um w-demi polimatroide se*

(1) $f(\{0\}) = 0$

(2) *Para quaisquer $X, Y \in \mathcal{P}(M)$ com $X \subseteq Y$, temos $0 \leq f(Y) - f(X) \leq w(p_\Omega(Y) - p_\Omega(X))$.*

Definição 4.2.4. *Sejam M um A-módulo à esquerda com uma série de composições, uma função $f : \mathcal{P}(M) \to \mathbb{Z}$ e $w \in \mathbb{Z}^+$, tais que (M, f, Ω) seja um w-demi polimatroide com $f(M) = k$, e consideremos $\Phi \subseteq \mathcal{P}(M)$, tal que (M, Φ, p_Ω) seja abundante. Para qualquer $a \in [0, k]$, o a-ésimo peso generalizado de $((M, f, \Omega), \Phi)$, é definido como*

$$d_a((M, f, \Omega), \Phi) = \min\{p_\Omega(W) \ \ tal\ que\ \ W \in \Phi,\ a \leq f(W)\},$$

e para qualquer $b \in [0, p_\Omega(M)]$, o b-ésimo perfil de comprimento de $((M, f, \Omega), \Phi)$, é definido como

$$K_b((M, f, \Omega), \Phi) = \max\{f(W) \ \ tal\ que\ \ W \in \Phi,\ p_\Omega(W) = b\}.$$

Outra vez, é importante mencionarmos que todas as definições acima também são aplicadas à B-módulos à direita. Essencialmente, consideremos Δ uma coleção não vazia de B-módulos à direita simples. Para qualquer B-módulo à direita N com uma série de composições $\{0\} = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_{s-1} \subseteq H_s = M$, de modo semelhante à p_Ω, definamos uma função λ_Δ, tal que

$$\lambda_\Delta(N) = |\{i \in [0, s] \ \text{ tal que } \ \exists\, Z \in \Delta \ \text{ tal que } \ H_i/H_{i-1} \cong Z\}|. \tag{4.2}$$

Neste momento, apresentaremos algumas definições para estendermos a noção de espaços duais.

Definição 4.2.5. *Sejam M um A-módulo à esquerda, N um B-módulo à direita e U um A-B-bimódulo. Fixemos $\beta : M \times N \to U$. Então, β é dito uma função bilinear se para quaisquer $a, b \in M$, $c, d \in N$, $r \in A$ e $s \in B$, as seguintes condições são satisfeitas:*

(1) $\beta(a + b, c) = \beta(a, c) + \beta(b, c)$;

(2) $\beta(a, c + d) = \beta(a, c) + \beta(a, d)$;

(3) $\beta(ra, cs) = r\beta(a, c)s$.

Definição 4.2.6. *Sejam $C \subseteq M$ e β uma função bilinear. O conjunto $C^\perp = \{y \ \ tal\ que \ \ y \in N,\ \beta(x, y) = 0$ para todo $x \in C\}$ é chamado anulador à esquerda de C com respeito à β.*

Definição 4.2.7. *Sejam $D \subseteq N$ e β uma função bilinear. O conjunto ${}^\perp D = \{x \ \ tal\ que \ \ x \in M,\ \beta(x, y) = 0$ para todo $y \in D\}$ é chamado anulador à direita de D com respeito à β.*

Observação 4.2.1. *Dizemos que β é uma função bilinear não-degenerada se $M^\perp = \{0\}$ e ${}^\perp N = \{0\}$.*

A fim de simplificarmos os próximos passos, ponderemos o seguinte: M é um A-módulo à esquerda e N é um B-módulo à direita, ambos admitindo séries de composições; U é um A-B-bimódulo, em que para qualquer A-módulo à esquerda X, temos $\mathrm{Hom}_A(X, U)$

como um B-módulo à direita simples e para qualquer B-módulo à direita Y, temos $\mathrm{Hom}_A(Y,U)$ como um A-módulo à esquerda simples; $\beta : M \times N \to U$ é uma função bilinear não-degenerada; Ω é uma coleção não vazia de A-módulos simples; e $\Delta = \{\mathrm{Hom}_A(X,U) \text{ tal que } X \in \Omega\}$, uma coleção não vazia de B-módulos simples.

Em [1], vemos que, considerando o A-B-bimódulo U e a função bilinear não-degenerada β, como M e N possuem série de composições, temos

$$^{\perp}(C^{\perp}) = C \text{ e } (^{\perp}D)^{\perp} = D \text{ para todo } C \in \mathcal{P}(M) \text{ e } D \in \mathcal{P}(N). \tag{4.3}$$

Além disso, conseguimos a seguinte relação:

$$\lambda_{\Delta}(D) = p_{\Omega}(M) - p_{\Omega}(^{\perp}D), \text{ para todo } D \in \mathcal{P}(N). \tag{4.4}$$

A equação acima é uma fórmula bem conhecida em Teoria dos Módulos e uma demonstração para a mesma, pode ser encontrada em [17]. Neste momento, fixemos $f : \mathcal{P}(M) \to \mathbb{Z}$ e $w \in \mathbb{Z}^+$ tais que (M, f, Ω) seja um w-demi polimatroide com $f(M) = k$ e definamos uma função $h : \mathcal{P}(N) \to \mathbb{Z}$ como

$$h(D) = f(^{\perp}D) + w \cdot \lambda_{\Delta}(D) - k.$$

Observemos que, por 4.3, como β é não degenerada, obtemos

$$M^{\perp} = \{0\} \Longrightarrow ^{\perp}(M^{\perp}) = ^{\perp}\{0\} \Longrightarrow M = ^{\perp}\{0\}.$$

Com isso, conseguimos $h(\{0\}) = 0$. Além disso, consideremos $X, Y \in \mathcal{P}(N)$, com $X \subseteq Y$. Assim, observemos o seguinte:

$$\begin{aligned} h(Y) - h(X) &= f(^{\perp}Y) + w \cdot \lambda_{\Delta}(Y) - k - (f(^{\perp}X) + w \cdot \lambda_{\Delta}(X) - k) \\ &= f(^{\perp}Y) - f(^{\perp}X) + w(\lambda_{\Delta}(Y) - \lambda_{\Delta}(X)). \end{aligned}$$

Como $X \subseteq Y$, temos $^{\perp}Y \subseteq ^{\perp}X$. Sendo assim, sabendo que (M, f, Ω) é um w-demi polimatroide, temos $f(^{\perp}X) - f(^{\perp}Y) \geq 0 \Longrightarrow f(^{\perp}Y) - f(^{\perp}X) \leq 0$. Logo, $h(Y) - h(X) \leq w(\lambda_{\Delta}(Y) - \lambda_{\Delta}(X))$. Por outro lado, por 4.4,

$$\begin{aligned} f(^{\perp}X) - f(^{\perp}Y) &\leq w(p_{\Omega}(^{\perp}X) - p_{\Omega}(^{\perp}Y)) \\ &= w(-\lambda_{\Delta}(X) + p_{\Omega}(M) + \lambda_{\Delta}(Y) - p_{\Omega}(M)) \\ &= w(\lambda_{\Delta}(Y) - \lambda_{\Delta}(X)), \end{aligned}$$

que implica $f(^{\perp}Y) - f(^{\perp}X) \geq w(\lambda_{\Delta}(X) - \lambda_{\Delta}(Y))$. Logo, $h(Y) - h(X) \geq 0$. Portanto, (N, h, Δ) é um w-demi polimatroide com $h(N) = w \cdot p_{\Omega}(M) - k$.

Agora, fixemos também $\Phi \subseteq \mathcal{P}(M)$, de maneira que, (M, Φ, p_{Ω}) seja abundante. Definamos $\Theta \subseteq \mathcal{P}(N)$, em que $\Theta = \{X^{\perp} \text{ tal que } X \in \Phi\}$. Por 4.3 e 4.4, chegamos a $(N, \Theta, \lambda_{\Delta})$ como um abundante. Em vista disso, conseguimos uma dualidade, no contexto de w-demi polimatroides, para $((M, f, \Omega), \Phi)$ e $((N, h, \Delta), \Theta)$.

Teorema 4.2.1. *1. Para qualquer* $l \in [0, p_\Omega(M)]$,

$$K_l((N,h,\Delta),\Theta) = K_{p_\Omega(M)-l}((M,f,\Omega),\Phi) + wl - k.$$

2. Para qualquer $\gamma \in \mathbb{Z}$, *definimos os conjuntos* $\mathcal{A}_\gamma$ *e* $\mathcal{B}_\gamma$ *como*

$$\begin{aligned}\mathcal{A}_\gamma &= \{d_a((M,f,\Omega),\Phi) \ \textit{tal que} \ a \in [1,k],\ a \equiv \gamma + k \mod w\},\\ \mathcal{B}_\gamma &= \{p_\Omega(M) + 1 - d_c((N,h,\Delta),\Theta) \ \textit{tal que} \ c \in [1, w\cdot p_\Omega(M) - k],\ c \equiv \gamma \mod w\}.\end{aligned}$$

Então, para qualquer $\gamma \in \mathbb{Z}$, *temos* $\mathcal{A}_\gamma \cap \mathcal{B}_\gamma = \emptyset$, $\mathcal{A}_\gamma \cup \mathcal{B}_\gamma = [1, p_\Omega(M)]$.

Demonstração. Utilizando que (M,Φ,p_Ω) é abundante e (M,f,Ω) é um w-demi polimatroide com $f(E) = k$, definamos uma função $g : \Phi \to [0, p_\Omega(M)]$, em que $g(A) = p_\Omega(A)$. Como (M,Φ,p_Ω) é abundante, então g é uma função sobrejetiva. Além disso, como (M,f,Ω) é um w-demi polimatroide com $f(E) = k$, a função f restrita à Φ, $f|_\Phi$, é uma função de Φ à $[0,k]$, em que $k \in \mathbb{N}$. Dessa forma, considerando as funções g e $f|_\Phi$, as condições 3.2 à 3.5 são válidas. Agora, definamos uma função $\sigma : \Theta \to \Phi$, em que $\sigma(D) =^\perp D$. Pela definição do conjunto Θ, temos, de imediato, σ como uma função bijetiva. Além disso, definamos também uma função $\mu : \Theta \to [0, p_\Omega(M)]$, em que $\mu(D) = p_\Omega(M) - g(\sigma(D))$ e consideremos $h|_\Theta : \Theta \to \mathbb{Z}$. Desse modo, $\mu(D) = p_\Omega(M) - g(^\perp D) = p_\Omega(M) - p_\Omega(^\perp D)$, que por 4.4, nos dá $\mu(D) = \lambda_\Delta(D)$ e com isso, temos

$$h|_\Theta(D) = f|_\Phi(\sigma(D)) + w\cdot\mu(D) - k.$$

Nestas circunstâncias, definamos, por fim, as funções T, S, τ e η, tais como nas condições de 3.8 à 3.11, desta vez considerando $(g, f|_\Phi)$ e $(\mu, h|_\Theta)$, respectivamente. Logo, pela Definição 4.2.4, $T(a) = \mathrm{d}_a((M,f,\Omega),\Phi)$, para $a \in [0,k]$ e $S(b) = \mathrm{K}_b((M,f,\Omega),\Phi)$, para $b \in [0, p_\Omega(M)]$. E ainda, $\tau(c) = \mathrm{d}_c((N,h,\Delta),\Theta)$, para $c \in [0, w\cdot p_\Omega(M) - k]$ e $\eta(b) = \mathrm{K}_b((N,h,\Delta),\Theta)$, para $b \in [0, p_\Omega(M)]$. Portanto, aplicando o Teorema da Ponte (3.2.1), temos exatamente o que queríamos. □

5 Considerações finais

Neste trabalho, estudamos e apresentamos resultados sobre a dualidade de Wei, a partir de conexões de Galois entre subconjuntos finitos de $\mathbb{Z}$ para pesos generalizados e perfis de dimensão/comprimento de um código C. Ademais, vimos aplicações desses resultados em estruturas como w-demi matroides e w-demi polimatroides. Para isso, foi necessário recorrer a diversas literaturas para que desenvolvêssemos uma base do estudo de matroides e demi-matroides e a dualidade de Wei para estas estruturas.

A dualidade de Wei tem sido estendida em várias direções. Teoremas de dualidade do tipo Wei provados para códigos lineares sobre anéis de Galois ([2]), para códigos lineares sobre anéis de cadeia finitos ([10]), para códigos com a métrica poset ([3] e [6]) e com a métrica posto ([16], [7] e [11]), além de provados também para noções de combinatória como demi-matroides, matroides, grafos e transversais ([4]) são exemplos de extensões deste estudo.

Por fim, este trabalho possibilitou uma maior compreensão da dualidade de Wei em códigos lineares, assunto que possui um campo vasto na pesquisa em Códigos Corretores de Erros. Procuramos compor um trabalho, o mais autossuficiente possível, que fosse de grande auxílio para futuras leituras. Desse modo, esperamos que todo o estudo feito para este trabalho, assim como o conteúdo que desenvolvemos, contribua para o avanço das pesquisas relacionadas a este tema.

Referências

[1] ANDERSON, Frank W.; FULLER, Kent R. **Rings and categories of modules**. Springer Science & Business Media, 2012. Citado na página 50.

[2] ASHIKHMIN, Alexei. On generalized Hamming weights for Galois ring linear codes. **Designs, Codes and Cryptography**, v. 14, n. 2, p. 107-126, 1998. Citado na página 52.

[3] BARG, Alexander; PURKAYASTHA, Punarbasu. Near MDS poset codes and distributions. In: **2010 IEEE International Symposium on Information Theory**. IEEE, 2010. p. 1310-1314. Citado na página 52.

[4] BRITZ, Thomas et al. Wei-type duality theorems for matroids. **Designs, Codes and Cryptography**, v. 62, n. 3, p. 331-341, 2012. Citado 2 vezes nas páginas 11 e 52.

[5] CURTIS, Charles W.; REINER, Irving. **Representation theory of finite groups and associative algebras**. American Mathematical Soc., 1966. Citado 2 vezes nas páginas 44 e 48.

[6] DE OLIVEIRA MOURA, Allan; FIRER, Marcelo. Duality for poset codes. **IEEE Transactions on Information Theory**, v. 56, n. 7, p. 3180-3186, 2010. Citado na página 52.

[7] DUCOAT, Jérôme. Generalized rank weights: a duality statement. **arXiv preprint arXiv:1306.3899**, 2013. Citado na página 52.

[8] FORNEY, G. David. Dimension/length profiles and trellis complexity of linear block codes. **IEEE Transactions on information theory**, v. 40, n. 6, p. 1741-1752, 2002. Citado na página 16.

[9] HEFEZ, Abramo; VILLELA, Maria Lúcia T. **Códigos corretores de erros**. Instituto de Matematica Pura e Aplicada, 2008. Citado na página 11.

[10] HORIMOTO, Hiroshi; SHIROMOTO, Keisuke. On generalized Hamming weights for codes over finite chain rings. In: **International Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes**. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001. p. 141-150. Citado na página 52.

[11] MARTÍNEZ-PEÑAS, Umberto; MATSUMOTO, Ryutaroh. Relative generalized matrix weights of matrix codes for universal security on wire-tap networks. **IEEE**

Transactions on Information Theory, v. 64, n. 4, p. 2529-2549, 2017. Citado na página 52.

[12] MUKHOPADHYAY, Malhar M.; VASSILIEV, Evgueni. On the Vamos matroid, homogeneous pregeometries and dense pairs. **Australas. J Comb.**, v. 75, p. 158-170, 2019. Citado na página 11.

[13] OXLEY, James G. **Matroid theory**. Oxford University Press, USA, 2006. Citado 2 vezes nas páginas 11 e 23.

[14] OZAROW, Lawrence H.; WYNER, Aaron D. Wire-tap channel II. **AT&T Bell Laboratories technical journal**, v. 63, n. 10, p. 2135-2157, 1984. Citado na página 9.

[15] POLCINO MILIES, Francisco César. Anéis e módulos. 1972. Citado na página 44.

[16] RAVAGNANI, Alberto. Generalized weights: an anticode approach. **Journal of Pure and Applied Algebra**, v. 220, n. 5, p. 1946-1962, 2016. Citado na página 52.

[17] VERTIGAN, Dirk. Latroids and their representation by codes over modules. **Transactions of the American Mathematical Society**, v. 356, n. 10, p. 3841-3868, 2004. Citado na página 50.

[18] WILSON, Robin J. An introduction to matroid theory. **The American Mathematical Monthly**, v. 80, n. 5, p. 500-525, 1973. Citado 2 vezes nas páginas 11 e 20.

[19] WEI, Victor K. Generalized Hamming weights for linear codes. **IEEE Transactions on information theory**, v. 37, n. 5, p. 1412-1418, 2002. Citado 4 vezes nas páginas 9, 11, 15 e 18.

[20] XU, Yang; KAN, Haibin; HAN, Guangyue. A Galois connection approach to Wei-type duality theorems. **IEEE Transactions on Information Theory**, v. 68, n. 8, p. 5133-5144, 2022. Citado 5 vezes nas páginas 11, 15, 33, 44 e 48.