UNIVERSIDADE FEDERAL DO PARANÁ
Maycow Gonçalves Carneiro

Identidades de MacWilliams para Códigos Poset

Curitiba, 2013.

UNIVERSIDADE FEDERAL DO PARANÁ
Maycow Gonçalves Carneiro

Identidades de MacWilliams para Códigos Poset

Dissertação apresentada ao Programa de Pós-Graduação em Matemática Aplicada da Universidade Federal do Paraná, como requisito parcial à obtenção do grau de Mestre em Matemática.

Orientador: Prof. Dr. Marcelo Muniz S. Alves.

Curitiba, 2013.

TERMO DE APROVAÇÃO

"IDENTIDADES DE MACWILLIAMS PARA CÓDIGOS POSET"

por

MAYCOW GONÇALVES CARNEIRO

Dissertação aprovada como requisito parcial para obtenção do grau de Mestre no Programa de Pós-Graduação em Matemática Aplicada, pela Comissão Examinadora composta por:

Orientador: _____
Prof. Dr. Marcelo Muniz Silva Alves
Dep. de Matemática – UFPR

_____
Prof. Dr. Luciano Panek
Unioeste

_____
Prof. Dr. Giuliano Gadioli La Guardia
UEPG

Curitiba, 31 de janeiro de 2014.

Ministério da Educação
Universidade Federal do Paraná
Setor de Ciências Exatas/Departamento de Matemática
Programa de Pós-Graduação em Matemática Aplicada - PPGMA

ATA DA 55ª DEFESA DE DISSERTAÇÃO DE MESTRADO

Aos trinta e um dias do mês de janeiro de 2014, no Anfiteatro A, Prédio das PCs, da Universidade Federal do Paraná, foi instalada pelo Professor Marcelo Muniz Silva Alves, a Banca Examinadora para a quinquagésima quinta Defesa de Dissertação de Mestrado em Matemática Aplicada. Estiveram presentes ao Ato, professores, alunos e visitantes.

A banca examinadora, homologada pelo Colegiado do Programa de Pós-Graduação em Matemática Aplicada, ficou constituída pelos professores: Prof. Dr. Luciano Panek, da Universidade Estadual do Oeste do Paraná, Prof. Dr. Giuliano Gadioli La Guardia, da Universidade Estadual de Ponta Grossa, e o Prof. Dr. Marcelo Muniz Silva Alves, orientador da dissertação, a quem coube a presidência dos trabalhos.

Às dez horas, a banca iniciou seus trabalhos, convidando o candidato **MAYCOW GONÇALVES CARNEIRO** a fazer a apresentação do tema da dissertação intitulada "IDENTIDADES DE MACWILLIAMS PARA CÓDIGOS POSET". Encerrada a apresentação, iniciou-se a fase de argüição pelos membros participantes. Após a argüição, a banca com pelo menos 03 (três) membros, reuniu-se para apreciação do desempenho do pós-graduando.

A banca considerou que o pós-graduando fez uma apresentação com a necessária concisão. A Dissertação apresenta contribuição à área de estudos e não foram registrados problemas fundamentais de estrutura e redação, resultando em plena e satisfatória compreensão dos objetivos pretendidos.

Tendo em vista a dissertação e a argüição, os membros presentes da banca decidiram pela sua aprovação.

Curitiba, 31 de janeiro de 2014.

Prof. Dr. Marcelo Muniz Silva Alves
Presidente

Prof. Dr. Luciano Panek
Titular

Prof. Dr. Giuliano Gadioli La Guardia
Titular

Ministério da Educação
Universidade Federal do Paraná
Setor de Ciências Exatas/Departamento de Matemática
Programa de Pós-Graduação em Matemática Aplicada - PPGMA

PARECER DA BANCA EXAMINADORA

Após a apresentação, a banca deliberou pela aprovação da dissertação do candidato **MAYCOW GONÇALVES CARNEIRO** devendo, para tanto, incorporar as sugestões feitas pelos membros da banca, no prazo estabelecido pelo regimento correspondente.

Curitiba, 31 de janeiro de 2014.

Prof. Dr. Marcelo Muniz Silva Alves
Presidente

Prof. Dr. Luciano Panek
Titular

Prof. Dr. Giuliano Gadioli La Guardia
Titular

À minha mãe, irmão e irmãs.

Agradecimentos

Agradeço primeiramente a Deus pela sabedoria concedida e pela força em tantos momentos da minha vida.

Uma pessoa muito especial e que sempre me apoiou, que me criou, educou e fez de tudo para que eu pudesse crescer e alcançar meus objetivos, minha mãe! Como costumo brincar, Dona Dalila, à ti devo meus maiores agradecimentos! Obrigado mâezinha, por tudo que fez e continua fazendo! Te amo!

Agradeço também aos meus irmãos, Adriel, Kelly e Fabieli, pelo apoio e ajuda quando precisei, por passarem por tantas coisas ao meu lado! Amo-os também! Obrigado!

Agradeço ainda à minha namorada, Analice, por me apoiar e aguentar, dois anos longe não é fácil, mas ela sempre esteve ao meu lado! Te amo! Obrigado!

Outra pessoa muito importante para que tudo isso se tornasse possível foi meu orientador, Marcelo Muniz, quanto te incomodar, nos meus horários, nos horários dos outros, não tinha muito horário na verdade, mas você sempre estava ali para me ajudar com as dúvidas que surgiam, algumas triviais, outras nem tanto, mas sempre me ajudava! Obrigado.

Agradeço ao professor Marcelo Firer pela sugestão do artigo sobre relações de equivalência de tipo MacWilliams, sem o qual não teria obtido os resultados aqui apresentados.

Não posso deixar de agradecer a todos os meus professores da graduação, em especial ao Carlos, que sempre me incentivou a fazer o mestrado, continuar estudando e buscando sempre mais.

Agradeço à Coordenação de Aperfeiçoamento de Pessoal de Nível Superior pelo apoio financeiro e por fim, mas não menos importante, agradeço aos meus colegas do PPGMA que de uma forma ou outra contribuíram para esta conquista.

“O único lugar onde o sucesso vem antes do trabalho é no dicionário.”

Albert Einstein

“Se A é o sucesso, então A é igual a X mais Y mais Z.
O trabalho é X; Y é o lazer; e Z é manter a boca fechada.”

Albert Einstein

“Quanto mais aumenta nosso conhecimento, mais evidente fica nossa ignorância”

John F. Kennedy

“Talvez não tenha conseguido fazer o melhor, mas lutei para que o melhor fosse feito.
Não sou o que deveria ser, mas Graças a Deus, não sou o que era antes”

Marthin Luther King

Resumo

A classe de códigos mais estudada é a dos códigos lineares. Utilizando a métrica de Hamming conseguimos relacionar o polinômio enumerador de peso de um código $\mathscr{C}$ com o do seu código dual ($\mathscr{C}^{\perp}$) através das identidade de MacWilliams. Busca-se então, derivar tais identidades para códigos lineares utilizando uma métrica não Hamming. Assim, sendo P um poset em $[n]$, apresentamos os resultados que mostram que P admite identidades de MacWilliams se, e somente se, o poset é hierárquico. Além disso, se $I(P)$ é o conjunto de ideais de ordem de P e E é uma relação de equivalência em $I(P)$, introduzimos os conceitos de relação dual (E^*) de uma relação de equivalência E, distribuição de E-peso (resp. E^*-peso) de um P-código linear (resp. seu P-código dual ou P^*-código) e o conceito de relação de equivalência de tipo MacWilliams. Três tipos de relações de equivalência em $I(P)$ são apresentadas, as quais são definidas respectivamente pela cardinalidade dos ideais do poset, pela ação dos automorfismos do poset no conjunto de seus ideais, e pela existência de um isomorfismo entre dois ideais e mostramos sob que condições tais relações são de tipo MacWilliams. Além disso, mostramos que quando a relação de equivalência referente aos isomorfismos é de tipo MacWilliams, a mesma coincide com a relação referente aos automorfismos de P. Apresentamos ainda o conceito de ρ-métrica no espaço das matrizes $n \times s$ com entradas em $\mathbb{F}_q$ e os conceitos de T e H-enumeradores de pesos para tal caso, relacionando a ρ-métrica, com a P-métrica e os conceitos de relações de equivalência para um poset P, o qual é uma união disjunta de n cadeias de comprimento s cada uma. Conseguimos assim relacionar os T e H-enumeradores de códigos mutuamente duais utilizando os conceitos de relações de equivalência de tipo MacWilliams. Com isso, mostramos que as matrizes utilizadas para relacionar as distribuições de E-peso e E^*-peso são, neste caso, inteiramente determinadas pelos ideais referentes à primeira cadeia do poset P.

Palavras-chave: *Códigos Lineares; Identidades de MacWilliams; Poset; Distribuição de Pesos; Relações de Equivalência de tipo MacWilliams.*

Abstract

The most studied class of codes is that of Linear Codes. Using the Hamming metric we are able to relate the weight enumerator polynomial of a code $\mathscr{C}$ with its dual code ($\mathscr{C}^{\perp}$) via the MacWilliams identities. Then, we seek to derive such identities for linear codes using a non Hamming metric. Thus, with P being a poset in $[n]$, we present results showing that P admits MacWilliams identities if, and only if, it is a hierarchical poset. Furthermore, if $I(P)$ is the set of ordered ideals of P and E is a equivalence relation on $I(P)$, we introduce the concepts of the dual relation (E^*) of a equivalence relation E, E-weigth distribution (resp. E^*-weight) of a linear P-code (resp. its dual P-code or P^*-code) and the concept of MacWilliams type equivalence relation. Three types of equivalence relations in $I(P)$ are presented, which are respectively defined by the cardinality of the ideals of the poset, by the action of automorphisms of the poset on the set of ideals, and the existence of an isomorphism between two ideals and we show the conditions under which such relations are of MacWilliams type. Furthermore, we show that when the equivalence relation associated to the isomorphisms is of MacWilliams type, it coincides with the one regarding the automorphisms of P. We also present the concept of ρ-metric in the space of matrices $n \times s$ with entries in $\mathbb{F}_q$ and the concepts of T and H-weight enumerators for this case, relating the ρ-metric with the P-metric and the concepts of equivalence relation for the poset P which is the disjoint union of n chains each of length s. Thus we are able to relate the T and H-enumerators of mutually dual codes using the concepts of MacWilliams type equivalence relations. Thus, we show that the matrices used to relate the E-weight and E^*-weight are, in this case, entirely determined by the ideals of the first chain of the poset P.

Keywords: *Linear Codes; MacWilliams Identities; Poset; Weight Distribuition; MacWilliams type Equivalence Relations.*

Sumário

Introdução

A Teoria de Códigos Corretores de Erros se iniciou em 1948 com o trabalho de C. E. Shannon intitulado *A Mathematical Theory of Communication* [14] e desde então tem sido estudada por matemáticos e engenheiros. Os códigos corretores de erros estão presentes em nosso cotidiano sempre que fazemos uso de informações digitalizadas.

Um código corretor de erros é, em essência, um modo organizado de se introduzir dados a uma informação que se queira transmitir ou armazenar, de forma que ao se recuperar tal informação se consiga detectar e corrigir possíveis erros.

Primeiramente tomamos um conjunto A chamado alfabeto, com q símbolos e em seguida tomamos o conjunto A^k, onde k é um número natural, e identificamos cada mensagem com um elemento de A^k. Tal conjunto é chamado código da fonte. O que se faz então é recodificar os elementos do código da fonte, de modo a introduzir redundâncias que permitam detectar e corrigir erros. O novo código introduzido na recodificação é então um subconjunto próprio de A^n, com n natural e $n > k$, chamado código de canal. O canal é o meio físico pelo qual se transmitirá a mensagem.

O estudo consiste em transformar o código da fonte em código de canal, em detectar e corrigir erros na recepção e em decodificar o código de canal em código da fonte. Um esquema deste processo pode ser visto na figura abaixo.

Na prática, a classe de códigos mais utilizada é a dos códigos lineares. Tomamos o conjunto A como sendo um corpo finito com q elementos, que denotaremos por $\mathbb{F}_q$ e o código de canal como sendo um subespaço vetorial de $\mathbb{F}_q^n$.

Assim, ao recebermos uma palavra, tomamos esta como sendo a mais próxima das palavras do código de canal. Para isto, necessitamos de uma forma de identificar a proximidade

entre elementos de $\mathbb{F}_q^n$. Na teoria clássica de códigos corretores de erros, utiliza-se a métrica de Hamming, apresentada em [4] por R. Hamming: tomamos a palavra recebida como sendo a palavra do código de canal que difere em um número mínimo de coordenadas da palavra recebida.

A partir de 1990, outras métricas tem sido utilizadas no estudo dos códigos corretores de erros, entre elas a P-métrica, onde P é um conjunto parcialmente ordenado, abreviado, do inglês, poset [1], e a métrica Rosenbloom-Tsfasman ou ρ-métrica introduzida por Rosenbloom e Tsfasman [12], as quais serão utilizadas no decorrer deste trabalho.

Quando tomamos um código linear com dimensão alta, seu código dual consequentemente possuirá uma dimensão baixa, assim se torna de suma importância obter informações do código mediante seu dual.

Em [10] F. J. MacWilliams apresenta resultados que relacionam a distribuição de pesos do código com seu dual em espaços com a métrica de Hamming. Tais relações recebem o nome de identidades de MacWilliams. Assim, tentamos derivar tais identidades para espaços com outras métricas.

Em [7] Kim e Oh classificam todas as estruturas de poset que admitem as identidades de MacWilliams e derivam tais identidades para estes posets. Porém, em [2], Choi et al. introduzem listas de pesos baseadas em classes de equivalência de ideais do poset; o coeficiente associado a uma classe é o número de elementos do código cujo suporte gera um ideal que está nesta classe. Cada relação de equivalência fornece uma lista; o polinômio enumerador coincide com a relação onde dois ideais são equivalentes se, e somente se, tem o mesmo número de elementos. Em [2] os autores caracterizam relações de equivalência em termos das identidades de tipo MacWilliams para P-códigos lineares.

A ρ-métrica introduzida por Rosenbloom e Tsfasman é definida no espaço linear das matrizes $m \times n$ com entradas no corpo $\mathbb{F}_q$. Assim, considerando órbitas de grupos lineares preservando a ρ-métrica, Dougherthy e Skriganov [3] mostram que o enumerador de pesos associado a tais órbitas satisfaz identidades de tipo MacWilliams para códigos mutuamente duais. Além disso, mostram que os correspondentes espectros de peso de tais códigos são relacionados por transformações as quais envolvem generalizações multi-dimensionais dos conhecidos polinômios de Krawtchouk, os quais foram uma das motivações para [2].

Neste trabalho mostraremos que os resultados obtidos em [3] por Dougherthy e Skriganov podem ser provados utilizando-se os conceitos e resultados obtidos em [2] por Choi et al.. Além disso, conseguimos resultados interessantes sobre os conceitos apresentados nos respectivos trabalhos, como o fato de que se uma relação de equivalência é de tipo MacWilliams, então todo isomorfismo entre ideais do poset é, na verdade, uma extensão de um automor-

fismo e que no caso do poset ser uma união disjunta de cadeias de mesmo comprimento, então as matrizes apresentadas por Choi et al. podem ser obtidas analisando-se apenas a primeira cadeia do poset.

A organização do trabalho é esquematizada da seguinte maneira: No Capítulo 1 apresentamos os conceitos básicos para códigos lineares em espaços de Hamming e para códigos Poset ou P-códigos lineares. Além disso, caracterizamos o enumerador de pesos para ambos os casos bem como apresentamos os conceitos de Caracteres, os quais serão utilizados no decorrer do trabalho. No Capítulo 2 apresentamos as identidades de MacWilliams em espaços de Hamming e mostramos que uma condição necessária e suficiente para um poset admitir identidades de MacWilliams é que este seja hierárquico. No Capítulo 3 apresentamos as definições de relações de equivalência em posets e relações equivalentes para uma Relação de Equivalência de tipo MacWilliams. Apresentamos então três relações de equivalência de tipo MacWilliams, as quais são definidas respectivamente pela cardinalidade dos ideais do poset, pela ação dos automorfismos do poset no conjunto de seus ideais, e pela existência de um isomorfismo entre dois ideais; em seguida mostramos que quando a relação de equivalência determinada por isomorfismos é uma relação de tipo MacWilliams então esta relação coincide com a relação definida pela ação dos automorfismos de P. No Capítulo 4 apresentamos as definições e conceitos envolvendo a métrica R-T ou ρ-métrica e "traduzimos" tais conceitos para a P-métrica, provando assim os resultados obtidos em [3] utilizando-se os conceitos e resultados obtidos nos capítulos anteriores.

Afim de deixar o texto menos carregado, alguns conceitos sobre ações de grupos, como o Teorema da Órbita e Estabilizador e também sobre a fórmula de inversão de Mobius utilizados nos Capítulos 3 e 4, são apresentados no apêndice A.

Capítulo 1

Códigos Lineares com Métrica de Hamming e Poset

Este capítulo, subdividido nas seções *Códigos Lineares*, *Códigos Poset* e *caracterees*, tem por objetivo, apresentar os conceitos básicos sobre códigos corretores de erros e conjuntos parcialmente ordenados, bem como os conceitos de polinômios enumeradores de peso e caracterees, os quais serão necessários para a leitura do restante do trabalho . Uma abordagem mais detalhada sobre os conceitos apresentados neste capítulo podem ser encontrados em [5], [6], [10], [1] e [9].

1.1 Códigos com a Métrica de Hamming

Afim de construirmos um código corretor de erros, precisamos primeiramente de um conjunto finito A com q elementos, chamado de alfabeto. Denotaremos o número de elementos de A por $|A|$.

Um código corretor de erros é um subconjunto próprio de $A^n = \underbrace{A \times \cdots \times A}_{n}$, para algum número natural n.

1.1.1 Métrica de Hamming

Dada uma palavra de A^n, precisamos de uma forma de identificar a proximidade entre esta e outras palavras de A^n. Para isso introduzimos o conceito de Métrica de Hamming.

Definição 1.1. *Uma métrica em um conjunto X é uma função*

$$d : X \times X \longrightarrow \mathbb{R}$$

satisfazendo as seguintes propriedades:

(i) *(Positividade)* $d(x,y) \geq 0$ *para todo* $x, y \in X$*; a igualdade vale* $\Leftrightarrow x = y$.

(ii) *(Simetria)* $d(x,y) = d(y,x)$ *para todo* $x, y \in X$.

(iii) *(Desigualdade Triangular)* $d(x,y) \leq d(x,z) + d(z,y)$ *para todo* $x, y, z \in X$

Definição 1.2. *Dados dois elementos* $\boldsymbol{u}, \boldsymbol{v} \in A^n$*, a distância de Hamming entre* $\boldsymbol{u}$ *e* $\boldsymbol{v}$ *é definida como*

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

Proposição 1.1. *A distância de Hamming* $d_H(\cdot,\cdot)$ *definida acima é uma métrica.*

Demonstração: Precisamos mostrar que a distância de Hamming satisfaz as três propriedades da definição 1.1. De fato:

(i) Temos por definição $d_H(\mathbf{u},\mathbf{v}) = |\{i : u_i \neq v_i, 1 \leq i \leq n\}| \geq 0$. Caso $d_H(\mathbf{u},\mathbf{v}) = 0$ teremos $u_i = v_i$ para $i = 1, ..., n$ logo $\mathbf{u} = \mathbf{v}$. Por outro lado, se $\mathbf{u} = \mathbf{v}$ então $u_j = v_j$ para $j = 1, ..., n$ portanto $d_H(\mathbf{u},\mathbf{v}) = 0$.

(ii) Pela definição temos $d_H(\mathbf{u},\mathbf{v}) = |\{i : u_i \neq v_i, 1 \leq i \leq n\}| = |\{i : v_i \neq u_i, 1 \leq i \leq n\}| = d_H(\mathbf{v},\mathbf{u})$

(iii) Para demonstrar esta propriedade podemos analisar apenas a i-ésima coordenada de $\mathbf{u}$, $\mathbf{v}$ e $\mathbf{w}$. Temos dois casos para analisar, se a contribuição de u_i e v_i para $d_H(\mathbf{u},\mathbf{v})$ é zero ou um. Caso a contribuição seja zero, então a contribuição das i-ésimas coordenadas de $d_H(\mathbf{u},\mathbf{w}) + d_H(\mathbf{w},\mathbf{v})$ certamente será maior ou igual à contribuição da i-ésima coordenada de $d_H(\mathbf{u},\mathbf{v})$. Por outro lado, se a contribuição é igual a 1 então $u_i \neq v_i$, logo, se $w_i = u_i$, teremos $w_i \neq v_i$, da mesma forma, se $w_i = v_i$, teremos $w_i \neq u_i$, portanto a contribuição da i-ésima coordenada de $d_H(\mathbf{u},\mathbf{w}) + d_H(\mathbf{w},\mathbf{v})$ certamente será maior ou igual a 1 e temos o resultado.

■

Assim a distância de Hamming entre elementos de A^n é uma métrica, também chamada de *métrica de Hamming*.

Definição 1.3. *Dados um elemento $\boldsymbol{c} \in A^n$ e um número real $r > 0$ definimos a bola e a esfera de centro $\boldsymbol{c}$ e raio r como sendo, respectivamente, os conjuntos:*

$$B(\boldsymbol{c}, r) = \{\boldsymbol{u} \in A^n : d_H(\boldsymbol{u}, \boldsymbol{c}) \leq r\}$$
$$S(\boldsymbol{c}, r) = \{\boldsymbol{u} \in A^n : d_H(\boldsymbol{u}, \boldsymbol{c}) = r\}$$

Definição 1.4. *Dado um código $\mathscr{C}$, definimos a distância mínima de $\mathscr{C}$ por*

$$d_H = min\{d_H(\boldsymbol{u}, \boldsymbol{v}) : \boldsymbol{u}, \boldsymbol{v} \in \mathscr{C} \text{ e } \boldsymbol{u} \neq \boldsymbol{v}\}$$

Um código $\mathscr{C}$ sobre um alfabeto A, possui três parâmetros fundamentais $[n, M, d_H]$, os quais se referem respectivamente, ao seu comprimento n, ou seja, o ambiente A^n onde está o código $\mathscr{C}$, o seu número de palavras M e a sua distância mínima d_H.

1.1.2 Códigos Lineares

A classe de códigos mais utilizada na prática é a dos códigos lineares. Denotaremos por $\mathbb{F}_q$ um corpo com q elementos, o qual será tomado como alfabeto. Temos assim que $\mathbb{F}_q^n$ é um $\mathbb{F}_q$-espaço vetorial de dimensão n com as operações de soma módulo q entre as entradas dos vetores e produto por escalar.

Definição 1.5. *Um código $\mathscr{C} \subset \mathbb{F}_q^n$ será chamado código linear se for um subespaço vetorial de $\mathbb{F}_q^n$.*

Como $\mathscr{C}$ é um subespaço vetorial de $\mathbb{F}_q^n$ de dimensão finita, podemos considerar a dimensão deste subespaço como sendo k, assim tomemos uma base para tal subespaço, formada pelos vetores $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k\}$, logo para cada $\mathbf{u} \in \mathscr{C}$ teremos $\mathbf{u} = \lambda_1\mathbf{v}_1 + \lambda_2\mathbf{v}_2 + \cdots + \lambda_k\mathbf{v}_k$, $\lambda_i \in \mathbb{F}, i = 1, \ldots, k$.

Assim, como para cada $\lambda_i \in \mathbb{F}_q$ temos q escolhas, teremos $M = |\mathscr{C}| = q^k$ e consequentemente $\dim_{\mathbb{F}_q} \mathscr{C} = k = \log_q q^k = \log_q M$.

Definição 1.6. *Dado $\boldsymbol{x} \in \mathbb{F}_q^n$, definimos o peso de $\boldsymbol{x}$ como sendo o número inteiro*

$$\omega_H(\boldsymbol{x}) := |\{i : x_i \neq 0\}|,$$

ou seja, $\omega_H(\boldsymbol{x}) = d_H(\boldsymbol{x}, 0)$, onde d_H representa a métrica de Hamming.

Definição 1.7. *O peso de um código linear $\mathscr{C}$ é o número inteiro*

$$\omega_H(\mathscr{C}) := min\{\omega_H(\boldsymbol{x}) : x \in \mathscr{C} \setminus \{0\}\}.$$

Para um código linear $\mathscr{C}$ o número de palavras depende da dimensão do mesmo, visto que $M = q^k$, assim podemos tomar os parâmetros desse código como sendo $[n,k,d_H]$ onde n é o comprimento do código, k é a dimensão e d_H é a distância mínima que, pela Definição 1.7 é o mesmo que o peso do código.

De fato, note que para todo par de elementos $\mathbf{x},\mathbf{y} \in \mathscr{C}$, com $\mathbf{x} \neq \mathbf{y}$, temos $\mathbf{z} = \mathbf{x} - \mathbf{y} \in \mathscr{C} \setminus \{0\}$ e $d(\mathbf{x},\mathbf{y}) = \omega_H(\mathbf{z})$. Logo, $d = \omega(\mathscr{C})$

Uma das formas de se descrever um subespaço vetorial em álgebra linear, é tomando o mesmo como imagem de uma transformação linear. Assim, consideremos uma base $\beta = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k\}$ de $\mathscr{C}$ e tomemos a matriz G cujas linhas são os vetores $\mathbf{v}_i = v_{i1}, \ldots, v_{in}$ para $i = 1, \ldots, k$, isto é

$$G = \begin{pmatrix} \mathbf{v}_1 \\ \vdots \\ \mathbf{v}_k \end{pmatrix} = \begin{pmatrix} v_{11} & v_{12} & \cdots & v_{1n} \\ \vdots & \vdots & & \vdots \\ v_{k1} & v_{k2} & \cdots & v_{kn} \end{pmatrix}.$$

A matriz G é chamada matriz geradora do código $\mathscr{C}$ referente à base β.

Consideremos a transformação linear definida por

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

Assim se $\mathbf{x} = (x_1, \ldots, x_k)$, teremos que $T(\mathbf{x}) = x_1\mathbf{v}_1 + \cdots + x_k\mathbf{v}_k$, ou seja, $T(\mathbb{F}_q^k) = \mathscr{C}$.

Lembrando que dada uma base de um espaço vetorial, podemos conseguir outra base para este espaço vetorial, efetuando operações elementares sobre os elementos da primeira base, dada uma matriz geradora G e acrescentando também as operações de permutação de colunas e multiplicação de uma coluna por um escalar não nulo, obtemos uma matriz G' geradora de um código $\mathscr{C}'$ equivalente ao código $\mathscr{C}$, ou seja, com os mesmos parâmetros e número de palavras, sendo que o número de palavras de peso i em $\mathscr{C}$ se mantém em $\mathscr{C}'$.

De fato, quando efetuamos as operações elementares juntamente com as duas operações descritas acima em uma base de $\mathscr{C}$, efetuamos em todas as palavras de $\mathscr{C}$.

Definição 1.8. *Dizemos que uma matriz geradora G de um código $\mathscr{C}$ está na forma padrão se tivermos*

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

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

Nem sempre conseguimos uma matriz geradora para um código $\mathscr{C}$ na forma padrão, porém, conseguimos um código equivalente $\mathscr{C}'$ com matriz geradora na forma padrão. Este re-

sultado é provado em [5], página 87.

1.1.3 Códigos Duais

Sejam $\mathbf{u} = (u_1, \ldots, u_n)$ e $\mathbf{v} = (v_1, \ldots, v_n)$ elementos de $\mathbb{F}_q^n$, define-se o produto interno de $\mathbf{u}$ e $\mathbf{v}$ por

$$\mathbf{u} \cdot \mathbf{v} = u_1 v_1 + \cdots u_n v_n.$$

Definição 1.9. *Seja $\mathscr{C} \subset \mathbb{F}_q^n$ um código linear, definimos o código dual $\mathscr{C}^\perp$, como sendo*

$$\mathscr{C}^\perp = \{\boldsymbol{v} \in \mathbb{F}_q^n : \boldsymbol{v} \cdot \boldsymbol{u} = 0, \forall \boldsymbol{u} \in \mathscr{C}\}.$$

Note que $\mathscr{C}^\perp$ é um subespaço vetorial de $\mathbb{F}_q^n$, logo é também um código linear.

Proposição 1.2. *Seja $\mathscr{C} \subset \mathbb{F}_q^n$ um código de dimensão k com matriz geradora $G = (Id_k|A)$, na forma padrão. Então*

(i) $dim\mathscr{C}^\perp = n - k$

(ii) $H = (-A^t|Id_{n-k})$ *é a matriz geradora de* $\mathscr{C}^\perp$

Demonstração: Ver [5] pág 89. ∎

Lema 1.3. *Suponha que $\mathscr{C}$ seja um código linear de dimensão k em $\mathbb{F}_q^n$ com matriz geradora G. Uma matriz H de ordem $(n-k) \times n$, com coeficiente em $\mathbb{F}_q$ e com linhas linearmente independentes, é uma matriz geradora de $\mathscr{C}^\perp$ se, e somente se, $G \cdot H^t = 0$.*

Demonstração: Ver [5] pág 91. ∎

Note que para verificarmos se um determinado vetor $\mathbf{v}$ pertence a $\mathscr{C}$, basta checarmos se é nulo o vetor $H\mathbf{v}^t$. A matriz geradora H de $\mathscr{C}^\perp$ é chamada de *matriz teste de paridade* de $\mathscr{C}$.

Dados um código $\mathscr{C}$ com matriz teste de paridade H e um vetor $v \in \mathbb{F}_q^n$, chamamos o vetor $H\mathbf{v}^T$ de *síndrome* de $\mathbf{v}$.

A matriz teste de paridade de um código $\mathscr{C}$ contém informações importantes sobre o valor do peso d_H do código.

Teorema 1.4. *Seja H a matriz teste de paridade de um código $\mathscr{C}$. Temos que o peso de $\mathscr{C}$ é igual a s se, e somente se, quaisquer $s-1$ colunas de H são linearmente independentes e existem s colunas de H linearmente dependentes.*

Demonstração: Ver [5] pág 93. ∎

Corolário 1.5 (Limitante de Singleton)**.** *Os parâmetros* $[n,k,d_H]$ *de um código linear satisfazem à desigualdade*

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

Demonstração: De fato, sendo H a matriz teste de paridade, esta tem posto $n-k$, como pelo teorema anterior d_H-1 é menor ou igual ao posto de H, temos a desigualdade. ∎

Vejamos alguns exemplos clássicos de códigos.

Exemplo 1.1 (Códigos de Hamming)**.** Um *código de Hamming* de ordem m sobre $\mathbb{F}_2$ é um código com matriz teste de paridade H_m de ordem $m \times n$ cujas colunas são os elementos de $\mathbb{F}_2^m \backslash \{0\}$ numa ordem qualquer.

Assim temos que o comprimento de um código de Hamming de ordem m é $n = 2^m - 1$ e, portanto, a sua dimensão é $k = n-m = 2^m - m - 1$, além disso temos que $d_H = 3$, pois, em H_m é fácil achar três colunas linearmente dependentes.

Como exemplo numérico, considere a matriz

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

Exemplo 1.2 (Códigos de Reed-Solomon)**.** Seja $\mathbb{F}_q$ um corpo finito e considere o $\mathbb{F}_q$-espaço vetorial $\mathbb{F}_q[X]_{k-1}$ dos polinômios em $\mathbb{F}_q[X]$ de grau menor ou igual a $k-1$, incluindo o polinômio nulo, isto é,

$$\mathbb{F}_q[X]_{k-1} = \{P \in \mathbb{F}_q[X] : gr(P) \leq k-1\} \cup \{0\}.$$

Este é um espaço vetorial de dimensão k, com uma base dada por $\beta = \{1, X, X^2, \ldots, X^{k-1}\}$.

Sejam n um inteiro, tal que $k < n \leq q = |\mathbb{F}_q|$ e $\alpha_1, \ldots, \alpha_n$ elementos distintos de $\mathbb{F}_q$ e considere a função definida por

$$\begin{array}{rccc} T: & \mathbb{F}_q[X]_{k-1} & \longrightarrow & \mathbb{F}_q^n \\ & P & \mapsto & (P(\alpha_1), \ldots, P(\alpha_n)) \end{array}.$$

É fácil verificar que T é uma transformação linear injetora.

De fato, $\ker T = \{P \in \mathbb{F}_q[X]_{k-1} : P(\alpha_1) = \cdots P(\alpha_n) = 0\} = \{0\}$, pois um polinômio não nulo de grau menor do que k não pode ter n raízes distintas.

Portanto a imagem $\mathscr{C}$ de T é um código linear de comprimento n e dimensão k. Além disso, note que se $\mathbf{c}$ é uma palavra não nula de $\mathscr{C}$ então, existe um $P \in \mathbb{F}_q[X]_{k-1}$ tal que $\mathbf{c} = (P(\alpha_1), \ldots, P(\alpha_n))$.

Logo teremos,

$$\omega_H(\mathbf{c}) = |\{i \in \{1,\ldots,n\} : P(\alpha_i) \neq 0\}| = n - |\{i \in \{1,\ldots,n\} : P(\alpha_i) = 0\}| \geq n - gr(P) \geq n - k + 1$$

Segue daí que $d_H \geq n-k+1$, mas pela Cota de Singleton temos que $d_H \leq n-k+1$. Portanto teremos $d_H = n-k+1$.

Dizemos que um código que satisfaz $d_H = n-k+1$ é um código MDS (*Maximum Distance Separable*).

Este código será chamado de *Código de Reed-Solomon* de comprimento n e dimensão k definido por $\alpha_1, \ldots, \alpha_n$.

1.1.4 Decodificação

Após codificarmos uma mensagem, precisaremos, ao recebermos a mensagem codificada, decodificá-la. Assim, definimos o vetor erro $\mathbf{e}$ como sendo a diferença entre o vetor recebido $\mathbf{r}$ e o vetor enviado $\mathbf{c}$, ou seja, $\mathbf{e} = \mathbf{r}$ - $\mathbf{c}$. Note então que o peso do vetor erro será igual ao número de erros cometidos durante a transmissão, ou seja, $\omega_H(\mathbf{e}) = d(\mathbf{r}, \mathbf{c})$.

Seja H a matriz teste de paridade do código $\mathscr{C}$. Como $H\mathbf{c}^T = 0$, temos que

$$H\mathbf{e}^T = H(\mathbf{r}^T - \mathbf{c}^T) = H\mathbf{r}^T - H\mathbf{c}^T = H\mathbf{r}^T.$$

Logo, a palavra recebida e o vetor erro tem mesma síndrome.

Assim, sejam d_H a distância mínima de $\mathscr{C}$ e $\kappa = \left[\frac{d_H-1}{2}\right]$, ou seja, a parte inteira de $\frac{d_H-1}{2}$, a capacidade de correção do código. Se $\omega_H(\mathbf{e}) = d(\mathbf{r}, \mathbf{c}) < \kappa$, então $\mathbf{e}$ é univocamente determinado por $\mathbf{r}$ (ver [5] pág. 101) e tomamos $\mathbf{c} = \mathbf{r} - \mathbf{e}$.

Seja $\mathbf{v} \in \mathbb{F}_q^n$. Defina $v + \mathscr{C} = \{v + c : c \in \mathscr{C}\}$. Assim, temos que os vetores $v, u \in \mathbb{F}_q$ tem a mesma síndrome se, e somente se, $u \in v + \mathscr{C}$.

De fato, temos $Hu^T = Hv^T \Leftrightarrow H(u-v)^T = 0 \Leftrightarrow u - v \in \mathscr{C} \Leftrightarrow u \in v + \mathscr{C}$.

Chamamos cada conjunto da forma $v + \mathscr{C}$ de classe lateral de $\mathbf{v}$ segundo $\mathscr{C}$. Note que $v + \mathscr{C} = \mathscr{C} \Leftrightarrow v \in C$.

Definimos ainda o elemento líder de uma classe lateral como sendo o vetor com peso mínimo na classe lateral. Temos assim a seguinte proposição:

Proposição 1.6. *Seja $\mathscr{C}$ um código linear em $\mathbb{F}_q^n$ com distância mínima d_H. Se $u \in \mathbb{F}_q^n$ é tal que $\omega_H(u) \leq \left[\frac{d_H-1}{2}\right] = \kappa$, então u é o único elemento líder de sua classe.*

Demonstração: Suponhamos que $u, v \in \mathbb{F}_q^n$ com $\omega_H(u) \leq \left[\frac{d_H-1}{2}\right]$ e $\omega_H(v) \leq \left[\frac{d_H-1}{2}\right]$. Se $u-v \in \mathscr{C}$, então

$$\omega_H(u-v) \leq \omega_H(u)+\omega_H(v) \leq \left[\frac{d_H-1}{2}\right]+\left[\frac{d_H-1}{2}\right] \leq d_h-1;$$

logo, $u-v=0$ e, portanto $u=v$. ■

Assim conseguimos um algoritmo de correção de mensagens que tenham sofrido um número de erros menor ou igual à capacidade de correção do código, que é $\kappa = \left[\frac{d_H-1}{2}\right]$.

Primeiramente determine todos os elementos $u \in \mathbb{F}_q^n$, tais que $\omega_H(u) \leq \kappa$. Em seguida, calcule as síndromes desses elementos e coloque esses dados em uma tabela. Seja **r** uma palavra recebida.

(1) Calcule a síndrome $s^T = H r^T$.

(2) Se s está na tabela, seja l o elemento líder da classe determinada por s; troque r por $r-l$.

(3) Se s não está na tabela, então na mensagem recebida foram cometidos mais do que κ erros.

Exemplo 1.3. Considere o [6,3,3] código linear definido sobre $\mathbb{F}_2$ com matriz teste de paridade dada por

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

Nesse caso temos $d_H = 3$, logo $\kappa = 1$. Assim, os vetores de peso ≤ 1 com suas respectivas síndromes são

$(0,0,0,0,0,0)$ com síndrome $(0,0,0)$

$(0,0,0,0,0,1)$ com síndrome $(1,0,1)$

$(0,0,0,0,1,0)$ com síndrome $(0,1,1)$

$(0,0,0,1,0,0)$ com síndrome $(1,1,0)$

$(0,0,1,0,0,0)$ com síndrome $(0,0,1)$

$(0,1,0,0,0,0)$ com síndrome $(0,1,0)$

$(1,0,0,0,0,0)$ com síndrome $(1,0,0)$

Suponhamos agora que a palavra recebida seja $r = (1,0,0,0,1,1)$. Logo, $H r^T = (0,1,0)^T$ e, portanto, $e = (0,1,0,0,0,0)$. Consequentemente, $c = r-e = (1,0,0,0,1,1)$

1.2 Códigos Poset

Nesta seção veremos os conceitos fundamentais sobre conjuntos parcialmente ordenados, abreviado poset (*Partially Ordered set*), bem como a definição de códigos poset os quais serão de suma importância no decorrer do trabalho.

Um dos problemas fundamentais da teoria de códigos, sendo $\mathbb{F}_q$ um corpo finito e $\mathbb{F}_q^m$ o conjunto das m-uplas sobre $\mathbb{F}_q$, é encontrar o maior inteiro d tal que existem n vetores $\mathbf{h}_1,\ldots,\mathbf{h}_n \in \mathbb{F}_q^m$ tal que quaisquer $d-1$ sejam linearmente independentes. Assim, tomando a matriz H cujas colunas são os vetores $\mathbf{h}_1,\ldots,\mathbf{h}_n$, teremos uma matriz teste de paridade para algum código $\mathscr{C}$ de comprimento n, dimensão $n-m$ e distância mínima d.

O problema de determinar d foi generalizado por Niederreiter.

Sejam $n_1, n_2, \ldots, n_s$ inteiros positivos e $H = \{h_{(i,j)} : 1 \leq i \leq s, 1 \leq j \leq n_i\}$ o sistema de $n_1+n_2+\cdots+n_s$ vetores em $\mathbb{F}_q^m$ particionado em s conjuntos ordenados de cardinalidades $n_1, n_2, \ldots, n_s$ respectivamente, ou seja,

$$H = \{h_{11},\ldots,h_{1n_1}, h_{21},\ldots,h_{2n_2},\ldots,h_{s1},\ldots,h_{sn_s} \in \mathbb{F}_q^m\}. \tag{1.1}$$

Defina $d(H) = \min \sum_{i=1}^{s} d_i$, onde este mínimo é extendido sobre todos os inteiros $d_1,\ldots,d_s$ tal que $0 \leq d_i \leq n_i$ $(1 \leq i \leq s)$ e $\sum_{i=1}^{s} d_i$ é positivo e para o qual o conjunto de vetores $h_{(i,j)} : 1 \leq i \leq s, 1 \leq j \leq d_i$ é linearmente dependente.

Se não existem tais inteiros $d_1,\ldots,d_s$, ou seja, os vetores $h_{(i,j)}$ são linearmente independentes e $n_1+n_2+\cdots+n_s \leq m$, então definimos $d(H)$ como sendo $n_1+n_2+\cdots+n_s+1$.

Exemplo 1.4. Consideremos o espaço vetorial $\mathbb{F}_2^3$ e tomemos $n_1 = 1$, $n_2 = 3$ e $n_3 = 3$. Seja

$$H = \{h_{11}, h_{21}, h_{22}, h_{23}, h_{31}, h_{32}, h_{33}\} = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

Como devemos ter $0 \leq d_i \leq n_i$, ao analisarmos o número $d(H) = \min \sum_{i=1}^{3} d_i$ tal que o conjunto de vetores $\{h_{(i,j)} : 1 \leq i \leq 3, 1 \leq j \leq d_i\}$ é linearmente dependente, encontramos que $d(H) = 3$ pois caso contrário, pelas opções dos valores de d_i teríamos um ou dois vetores que claramente são linearmente independentes, e tomando $d_1 = 0$, $d_2 = 3$ e $d_3 = 0$ teremos o conjunto $\{h_{21}, h_{22}, h_{23}\}$ que é linearmente dependente, logo $d(H) = 3$. Note ainda que esta matriz H é

a matriz teste de paridade do código de Hamming de ordem 3, o qual tem distância mínima $d = 3$.

O problema levantado por Niederreiter é estudar o número $d_q(n_1, \ldots, n_s, m) = \max d(H)$ e se possível encontrá-lo, onde o máximo é tomado sobre todos os sistemas da forma (1.1). Se $n_1 = \ldots, n_s = 1$, então teremos o problema fundamental da teoria de códigos.

O problema de Niederreiter também pode ser visto no cenário de conjuntos parcialmente ordenados.

Definição 1.10. *Uma relação de ordem parcial em um conjunto X é uma relação binária $\preceq$ satisfazendo, para todo $x, y, z \in X$*

(i) $x \preceq x$ *(reflexiva)*

(ii) $x \preceq y$ *e* $y \preceq x \Rightarrow x = y$ *(anti-simétrica)*

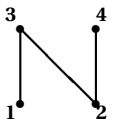
(iii) $x \preceq y$ *e* $y \preceq z \Rightarrow x \preceq z$ *(transitiva)*

Diremos que a relação de ordem é total se quaisquer dois elementos do conjunto forem comparáveis, isto é, $x \preceq y$ ou $y \preceq x \forall\, x, y \in X$.

Definição 1.11. *Se $\preceq$ é uma relação de ordem parcial em X, chamaremos o par ordenado $P = (X, \preceq)$ de poset.*

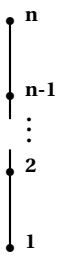
No decorrer do trabalho iremos nos referir ao poset P com elementos $\{1, 2, \ldots, n\}$, como sendo o poset P em $[n]$ e a relação de ordem referente ao poset P por $\preceq_P$. Também podemos representar o poset geometricamente através do seu diagrama de Hasse.

Exemplo 1.5. Tomemos o poset P em $[4]$ com relação de ordem $1 \preceq_P 3$, $2 \preceq_P 3$ e $2 \preceq_P 4$. Assim teremos o diagrama de Hasse

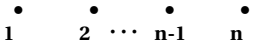


Alguns exemplos de poset utilizados no decorrer do trabalho são dados a seguir.

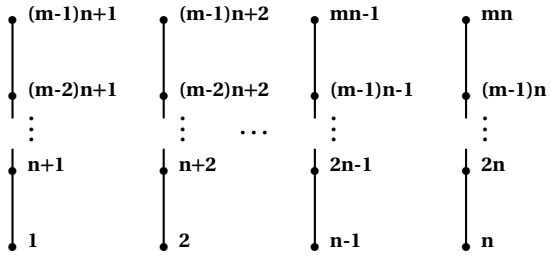
Exemplo 1.6 (Poset Cadeia)**.** Um poset P é dito um poset cadeia se tivermos uma relação de ordem total, ou seja, quaisquer dois elementos do poset são comparáveis. Assim, se tomarmos o poset P em $[n]$ teremos que $1 \preceq_P 2 \preceq_P \cdots \preceq_P n-1 \preceq_P n$, é uma cadeia para este poset. Tal poset tem diagrama de Hasse dado por



Exemplo 1.7 (Poset Anti-cadeia)**.** Um poset P é dito uma anticadeia se quaisquer dois elementos do poset forem não comparáveis. Assim, se tomarmos o poset P em $[n]$, teremos o seguinte diagrama de Hasse

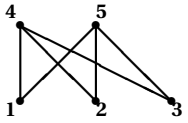


Exemplo 1.8 (Niederreiter-Rosembloom-Tsfasman NRT)**.** O poset NRT é uma união disjunta de cadeias de mesmo comprimento, ou seja, tomamos união de cadeias C_i de comprimento m em $\{i, n+i, 2n+i, \ldots, (m-1)n+i\}$ para $1 \leq i \leq n$, logo teremos um poset P em $[nm]$ com diagrama de Hasse como segue



Exemplo 1.9 (Poset Hierárquico)**.** Sejam $n_1, n_2, \ldots, n_t$ inteiros positivos com $n_1 + n_2 + \cdots + n_t = n$. Definimos o poset $\mathbb{H}(n; n_1, n_2, \ldots, n_t)$ no conjunto $\{(i, j) | 1 \leq i \leq t, 1 \leq j \leq n_i\}$ cuja relação de ordem é dada por $(i, j) \prec (l, m) \Leftrightarrow i < l$. O poset $\mathbb{H}(n; n_1, n_2, \ldots, n_t)$ é chamado poset hierárquico com t-níveis e n-elementos, assim teremos que os níveis são anticadeias e cada elemento de um nível se relaciona com todos os elementos do nível anterior.

Para representarmos pelo diagrama de Hasse tomemos o poset $\mathbb{H}(5; 3, 2)$ logo teremos



Definição 1.12. *Um subconjunto I de um poset P é dito um ideal se $x \in I$ e $y \preceq_P x$ implica que $y \in I$.*

Definição 1.13. *Seja I um ideal de um poset P. Um elemento $x \in I$ é dito elemento maximal no ideal I se, para todo elemento $y \in I$ tal que $x \preceq_P y$ tivermos $x = y$. Analogamente, um elemento $x \in I$ é dito elemento minimal no ideal I se, para todo elemento $y \in I$ tal que $y \preceq_P x$ tivermos $y = x$. Denotaremos o conjunto dos elementos maximais do ideal I por $M(I)$, o conjunto dos elementos minimais do ideal I por $Min(I)$ e o conjunto dos elementos que não são maximais por I_M. Note que $Min(I) \subset I_M$.*

Como mencionado no início da seção, o problema de Niederreiter pode ser visto no cenário dos conjuntos parcialmente ordenados, da seguinte maneira.

Tomamos um poset $P(n_1, \ldots, n_s) = \{(i, j) : 1 \leq i \leq s, 1 \leq j \leq n_i\}$, consistindo de s cadeias $N_1, \ldots, N_s$ disjuntas, de tamanho $n_1, \ldots, n_s$ respectivamente. Assim podemos obter um ideal de $P(n_1, \ldots, n_s)$ tomando, para cada $i = 1, \ldots, s$ um elemento $x_i \in N_i$ e todos os elementos abaixo deste em N_i. Logo, os ideais de tamanho t de $P(n_1, \ldots, n_s)$ estão em correspondência biunívoca com as partições $t_1, \ldots, t_s$ de t para os quais $0 \leq t_i \leq n_i$ para cada $i = 1, 2, \ldots, s$.

Assim buscamos vetores em $\mathbb{F}_q^m$ para os elementos do poset $P(n_1, \ldots, n_s)$ tal que estes vetores, para cada ideal de tamanho t, formem um conjunto linearmente independente e t seja máximo (o número $d_q(n_1, \ldots, n_s; m)$ é então um a mais que esse máximo).

Como mencionado anteriormente, se tomarmos $n_i = 1, \forall\, i = 1, \ldots, s$, teremos o problema fundamental da teoria de códigos. Assim podemos pensar em estender o problema de Niederreiter para um poset (finito) abitrário. Para isso, introduzamos o conceito de métrica poset.

1.2.1 Métrica Poset

Seja P um poset arbitrário com cardinalidade n e relação de ordem $\preceq_P$. Se $X \subset P$, então denotamos por $\langle X \rangle_P$ o menor ideal de P contendo X.

Considere o espaço vetorial $\mathbb{F}_q^n$ sobre $\mathbb{F}_q$. Podemos assumir sem perda de generalidade que o poset está definido em $[n]$, assim teremos uma correspondência biunívoca entre as posições coordenadas dos elementos de $\mathbb{F}_q^n$ e os elementos do poset P.

Definição 1.14. *Seja $x = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$. Definimos o P-peso de x como sendo*

$$\omega_P(x) = |\langle \mathrm{supp}(x) \rangle_P|,$$

onde $\mathrm{supp}(x) = \{i : x_i \neq 0\}$

Note que se mudarmos uma ou mais coordenadas não nulas de x para zero, é possível que obtenhamos um elemento x' com $\omega_P(x) = \omega_P(x')$.

Definição 1.15. *Sejam $x, y \in \mathbb{F}_q^n$. Definimos a P-distância entre x e y por*

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

Note que se P é uma anticadeia, então o P-peso e a P-distância são respectivamente o peso e a distância de Hamming.

Lema 1.7. *Seja P um poset com n elementos. Então a P-distância $d_P(\cdot,\cdot)$ é uma métrica em $\mathbb{F}_q^n$.*

Demonstração: De fato, sejam $x, y, z \in \mathbb{F}_q^n$. É trivial verificar que $d_P(x,y) \geq 0$ e $d_P(x,y) = d_P(y,x)$. Mostremos a desigualdade triangular, isto é, $d_P(x,y) \leq d_P(x,z) + d_P(z,y)$.

Note que $\text{supp}(a+b) \subset \text{supp}(a) \cup \text{supp}(b)$, logo segue da definição que

$d_P(x,y) = \omega_P(x-y) = |\langle \text{supp}(x-y)\rangle_P| = |\langle \text{supp}(x-z+z-y)\rangle_P| \leq$

$\leq |\langle \text{supp}(x-z)\rangle_P \cup \langle \text{supp}(z-y)\rangle_P| \leq |\langle \text{supp}(x-z)\rangle_P| + |\langle \text{supp}(z-y)\rangle_P| =$ ■

$= \omega_P(x-z) + \omega_P(z-y) = d_P(x,z) + d_P(z,y)$

Chamamos a métrica $d_P(\cdot,\cdot)$ em $\mathbb{F}_q^n$ de métrica poset.

Definição 1.16. *Definimos a P-bola e a P-esfera, com centro x e raio r como sendo, respectivamente, o conjunto*

$$B_P(x;r) = \{y \in \mathbb{F}_q^n : d_P(x,y) \leq r\}$$

$$S_P(x;r) = \{y \in \mathbb{F}_q^n : d_P(x,y) = r\}$$

Pela definição de P-bola, vemos que este é o conjunto de todos os vetores em $\mathbb{F}_q^n$ cuja P-distância para x é no máximo igual a r.

Proposição 1.8. *O número de vetores em $\mathbb{F}_q^n$ cuja distância para o vetor nulo é exatamente i é igual a*

$$\begin{cases} 1 & se \quad i = 0 \\ \displaystyle\sum_{j=1}^{i} (q-1)^j q^{i-j} \Omega_j(i) & se \quad i > 0 \end{cases},$$

onde $\Omega_j(i)$ é o número de ideais de P com cardinalidade i tendo exatamente j elementos maximais.

Demonstração: De fato, se $i = 0$ então $S_P(0,0)$ contém apenas o vetor nulo, logo $|S_P(0,0)| = 1$. Suponha que $i \geq 1$, se $x \in S_P(0,i)$ então $\omega_P(x) = i$, ou seja, o ideal gerado pelo suporte de x possui i elementos. Portanto, sendo I um ideal de P tal que $|I| = i$, devemos encontrar quantos vetores $y \in \mathbb{F}_q^n$ satisfazem $\langle \text{supp}(y)\rangle_P = I$. Suponha que $|M(I)| = j$, temos que $1 \leq j \leq i$. Como

$y=(y_1,\ldots,y_n)$, se y_s é tal que $s\in M(I)$, segue que $y_s\neq 0$, logo existem $q-1$ escolhas para y_s e portanto temos $(q-1)^j$ escolhas para as posições coordenadas de $y\in\mathbb{F}_q^n$ indexadas pelos elementos maximais de I. Para as posições coordenadas de $y\in\mathbb{F}_q^n$ indexadas pelos elementos do conjunto $I\backslash M(I)$, temos q^{i-j} escolhas. Como as demais coordenadas são nulas, temos $(q-1)^j q^{i-j}$ vetores em $y\in\mathbb{F}_q^n$ tal que $\langle \mathrm{supp}(y)\rangle_P = I$. Ainda, como temos $\Omega_j(i)$ ideais de P com cardinalidade i tendo j elementos maximais e $1\leq j\leq i$, teremos $S_P(0,i)=\sum_{j=1}^{i}(q-1)^j q^{i-j}\Omega_j(i)$ se $i\geq 1$. ■

Note que, como $d_P(x,y)=d_P(0,x-y)$, segue que o número de vetores em uma P-bola de raio r não depende do centro e será $|B_P(x,r)|=|\bigcup_{i=1}^{r}S_P(0,i)|=1+\sum_{i=1}^{r}\sum_{j=1}^{i}(q-1)^j q^{i-j}\Omega_j(i)$.

1.2.2 Códigos Posets

Se $\mathbb{F}_q^n$ está munido de uma métrica poset dizemos que $\mathbb{F}_q^n$ é um P-espaço. Um subconjunto $\mathscr{C}$ de $\mathbb{F}_q^n$ será dito um P-código ou código poset.

Assim como na teoria clássica de códigos, se $\mathscr{C}$ é um subespaço vetorial de um P-espaço $\mathbb{F}_q^n$ com dimensão k, então $\mathscr{C}$ é um P-código linear. Além disso, se d_P é a P-distância mínima entre duas palavras quaisquer de $\mathscr{C}$, então $\mathscr{C}$ é um $[n,k,d_P]$ P-código linear.

Definição 1.17. *Seja P um poset em $[n]$. Definimos o poset dual P^* em $[n]$, como sendo o poset com relação de ordem $\preceq_{P^*}$ dada por*

$$x\preceq_{P^*} y \Leftrightarrow y\preceq_P x.$$

Definição 1.18. *Seja $\mathscr{C}$ um $[n,k,d_P]$ P-código linear. Definimos o P^*-código dual $\mathscr{C}^\perp$ como sendo*

$$\mathscr{C}^\perp=\{v\in\mathbb{F}_q^n : v\cdot u=0, \forall\, u\in\mathscr{C}\}.$$

Claramente $\mathscr{C}^\perp$ é um subespaço vetorial de $\mathbb{F}_q^n$ de dimensão $n-k$, logo teremos que $\mathscr{C}^\perp$ é um P^*-código linear com parâmetros $[n,n-k,d_{P^*}]$.

Exemplo 1.10. Seja P um poset em $[3]$ com relação de ordem dada por $1\preceq_P 2\preceq_P 3$ e P^* o poset dual, ou seja, o poset em $[3]$ com relação de ordem $3\preceq_{P^*} 2\preceq_{P^*} 1$. Considere o seguinte P-código linear em $\mathbb{F}_2^3$:

$$\mathscr{C}=\{(0,0,0),(0,0,1)\}.$$

É fácil verificar que o código dual de $\mathscr{C}$ é o [3,2,2] P^*-código linear dado por

$$\mathscr{C}^{\perp} = \{(0,0,0),(1,0,0),(0,1,0),(1,1,0)\}.$$

Agora podemos generalizar o problema de Niederreiter.

Seja P um poset em [n]. Considere o sistema de vetores em $\mathbb{F}_q^m$ dado por $H = \{h_i : 1 \leq i \leq n\}$, indexado pelos elementos de P e defina $d_P(H)$ como o menor inteiro d tal que existe um ideal I de P de tamanho d com os vetores $\{h_i : i \in I\}$ linearmente dependentes. Se não há tal ideal, ou seja, $n \leq m$, então $d_P(H)$ é definido como sendo $n+1$. Como todo conjunto de $m+1$ vetores em $\mathbb{F}_q^m$ é linearmente dependente, temos que $d_P(H) \leq m+1$.

Olhando H como uma matriz teste de paridade de um P-código linear $\mathscr{C}$, vemos que $d_P(H)$ é o P-peso mínimo de uma palavra não nula de $\mathscr{C}$. Além disso, temos que $d_P(H) \geq d(H)$.

De fato, se o poset P é uma anticadeia temos a igualdade, pois neste caso a P-métrica se torna a métrica de Hamming. Suponha que P não é uma anticadeia, logo existe ao menos uma relação entre elementos de P. Suponha ainda que $d(H) = d$, logo dada qualquer palavra do código, temos que pelo menos d coordenadas são não nulas. Seja $x \in \mathscr{C}$ tal que x possui exatamente d coordenadas não nulas, se nenhuma dessas d coordenadas está relacionada com uma coordenada nula da palavra x então temos que $d_P(H) = d(H)$, porém se alguma das d coordenadas está relacionada com pelo menos uma coordenada nula de x então teremos $d_P(H) \geq d(H)+1$.

Seja $d_q(P;m) = \max d_P(H)$, onde o máximo é tomado sobre todos os sistemas H da forma descrita acima. Assim $d_P(P;m)$ é a maior P-distância mínima atingível por um $[n, n-m]$ P-código linear sobre $\mathbb{F}_q$. Claramente, $d_q(P;m) \leq m+1$, além disso, escolhendo um sistema H de vetores não nulos, temos que $d_q(P;m) \geq d_P(H) \geq 2$. Logo $2 \leq d_q(P;m) \leq m+1$.

1.3 Enumerador de Pesos e caracteres

Nesta seção daremos a definição de *distribuição de pesos* de um código bem como a de *polinômio enumerador de pesos*, os quais tem um papel de grande importância no estudo de códigos corretores de erros pelas informações que os mesmos contêm sobre o código. Outro tema abordado na seção são os *caracteres*, os quais utilizaremos nas demonstrações de vários teoremas ao longo do trabalho.

1.3.1 Enumerador de Pesos

Sejam $\mathbb{F}_q^n$ um P-espaço e $\mathscr{C}$ um P-código em $\mathbb{F}_q^n$. Denotaremos por $A_{i,P}(\mathscr{C})$ o número de palavras do código $\mathscr{C}$ com P-peso i, ou seja

$$A_{i,P}(\mathscr{C}) = |\{u \in \mathscr{C} : \omega_P(u) = i\}|.$$

De forma análoga, se $\mathscr{C}^\perp$ é o código dual de $\mathscr{C}$, denotamos por $A'_{i,P^*}(\mathscr{C}^\perp)$ o número de palavras de $\mathscr{C}^\perp$ com P^*-peso i.

Chamaremos os conjuntos $\{A_{i,P}(\mathscr{C})\}$ e $\{A'_{i,P^*}(\mathscr{C}^\perp)\}$ de distribuição de P-peso do código $\mathscr{C}$ e P^*-peso do código $\mathscr{C}^\perp$ respectivamente.

Quando não houver possibilidade de confusão, denotaremos de uma forma mais simplificada os elementos da distribuição de pesos: $A_{i,P}(\mathscr{C}) = A_i$ e $A'_{i,P^*}(\mathscr{C}^\perp) = A'_i$.

É fácil verificar que se P é um poset em $[n]$ e $\mathscr{C}$ é um $[n,k,d_P]$ P-código linear então $A_0 + A_1 + \cdots + A_n = q^k$ e além disso $A_0 = 1$ e $A_1 = \cdots = A_{d_P-1} = 0$.

Definição 1.19. *Seja $\mathscr{C}$ um P-código (linear) em $\mathbb{F}_q^n$. Definimos o enumerador de P-pesos do código $\mathscr{C}$ como sendo o polinômio*

$$W_{\mathscr{C},P}(x) = \sum_{u \in \mathscr{C}} x^{\omega_P(u)} = \sum_{i=0}^{n} A_i x^i. \tag{1.2}$$

Analogamente o enumerador de P^*-pesos de $\mathscr{C}^\perp$ será

$$W_{\mathscr{C}^\perp,P^*}(x) = \sum_{v \in \mathscr{C}^\perp} x^{\omega_{P^*}(v)} = \sum_{i=0}^{n} A'_i x^i. \tag{1.3}$$

Exemplo 1.11. Considere os posets P , P^* e os códigos $\mathscr{C}$ e $\mathscr{C}^\perp$ dados no Exemplo 1.10. Então os enumeradores de peso serão

$$W_{\mathscr{C},P}(x) = 1 + x^3 \qquad \text{e} \qquad W_{\mathscr{C}^\perp,P^*}(x) = 1 + x^2 + 2x^3.$$

Note que ao considerarmos o poset P como sendo uma anticadeia, temos $\omega_P(x) = \omega_H(x)$ e $d_P(x,y) = d_H(x,y)$, onde $\omega_H(\cdot)$ e $d_H(\cdot)$ são respectivamente o peso e a distância de Hamming, teremos também o enumerador de peso para códigos em espaços de Hamming.

Outro conceito que usaremos no decorrer do trabalho é o chamado Polinômio de Krawtchouk.

Definição 1.20. *Sejam q uma potência de primo e n um inteiro positivo. O polinômio de Krawt-*

chouk é definido por

$$P_k(x:n)=\sum_{j=0}^{k}(q-1)^{k-j}\binom{x}{j}\binom{n-x}{k-j}, k=0,\ldots,n.$$

Esses polinômios tem função geradora

$$(1+(q-1)x)^{n-y}(1-x)^{y}=\sum_{k=0}^{n}P_k(y;n)x^k. \tag{1.4}$$

De fato, chamemos $(q-1)=\gamma$. Sendo $a(x)=a_0+a_1x+\cdots+a_nx^n$ e $b(x)=b_0+b_1x+\cdots+b_mx^m$ dois polinômios, temos que o produto de $a(x)$ por $b(x)$ é dado por

$$a(x)b(x)=c_0+c_1x+\cdots+c_{n+m}x^{n+m} \quad \text{onde} \quad c_k=\sum_{j=0}^{k}a_jb_{k-j}.$$

Como podemos escrever

$$(1+\gamma x)^{n-y}=\sum_{m=0}^{n-y}\binom{n-y}{m}\gamma^m x^m \qquad \text{e} \qquad (1-x)^y=\sum_{j=0}^{y}\binom{y}{j}(-1)^j x^j,$$

teremos

$$\begin{aligned}(1-x)^y(1+\gamma x)^{n-y}&=\left(\sum_{j=0}^{y}\binom{y}{j}(-1)^j x^j\right)\left(\sum_{m=0}^{n-y}\binom{n-y}{m}\gamma^m x^m\right)\\&=\left(\sum_{j=0}^{y}a_jx^j\right)\left(\sum_{m=0}^{n-y}b_mx^m\right)=\sum_{k=0}^{y+n-y=n}c_kx^k\end{aligned}$$

onde $a_j=\binom{y}{j}(-1)^j$, $b_m=\binom{n-y}{m}\gamma^m$ e $c_k=\sum_{j=0}^{k}a_jb_{k-j}=\sum_{j=0}^{k}\binom{y}{j}(-1)^j\binom{n-y}{k-j}\gamma^{k-j}$.

Portanto $(1-x)^y(1+\gamma x)^{n-y}=\sum_{k=0}^{n}\sum_{j=0}^{k}(-1)^j\gamma^{k-j}\binom{y}{j}\binom{n-y}{k-j}x^k$, e da igualdade entre polinômios e de (1.4) temos $P_k(x:n)=\sum_{j=0}^{k}(q-1)^{k-j}\binom{x}{j}\binom{n-x}{k-j}$.

1.3.2 Caracteres

Nessa subseção consideraremos G um grupo abeliano finito de ordem $|G|$ com elemento identidade 1_G.

Definição 1.21. *Um caractere χ de G é um homomorfismo de G em $\mathbb{C}^* = \mathbb{C}\backslash\{0\}$.*

Como $\chi(1_G) = \chi(1_G)\chi(1_G)$ temos que $\chi(1_G) = 1$. Além disso, $(\chi(g))^{|G|} = \chi(g^{|G|}) = \chi(1_G) = 1$ para todo $g \in G$, logo os valores de χ são $|G|$-ésimas raízes da unidade.

Se $\chi(g) = 1$ para todo $g \in G$ chamamos este caractere de *caractere trivial* e denotamos por χ_0. Todos ou outros caracteres de G são chamados *não triviais*.

Definição 1.22. *Um caractere aditivo é um caractere de um grupo aditivo G. Um caractere aditivo de $\mathbb{F}_q^n$ é um caractere do grupo aditivo de $\mathbb{F}_q^n$.*

Assim, um caractere aditivo χ satisfaz $\chi(h+g) = \chi(h)\chi(g)$ para todo $g, h \in G$.

Lembremos ainda que um grupo multiplicativo G é dito cíclico se existe um elemento $a \in G$ tal que para qualquer $b \in G$, existe um inteiro j com $b = a^j$. O elemento a é chamado de gerador do grupo cíclico.

Para um corpo finito $\mathbb{F}_q$, denotamos por $\mathbb{F}_q^*$ o grupo multiplicativo de elementos não nulos de $\mathbb{F}_q$. Além disso, temos que $\mathbb{F}_q^*$ é um grupo cíclico, resultado que pode ser visto no Teorema 2.8 em [9] página 50.

Definição 1.23. *Um gerador do grupo cíclico $\mathbb{F}_q^*$ é chamado elemento primitivo de $\mathbb{F}_q$.*

Teorema 1.9. *Seja $\mathbb{F}_p$ um corpo finito com p primo e $\mathbb{F}_q$ uma extensão de $\mathbb{F}_p$, ou seja, $q = p^m$ para algum inteiro m. Então $\mathbb{F}_q = \mathbb{F}_p[\alpha]$, onde α é um elemento primitivo de $\mathbb{F}_p$.*

Demonstração: Ver [9] página 51. ∎

Tomemos o corpo $\mathbb{F}_q$ com q elementos e $q = p^m$ com p primo. Em relação a adição $\mathbb{F}_q$ é um grupo aditivo e pelo teorema acima temos que qualquer elemento $\beta \in \mathbb{F}_q$ pode ser escrito na forma $\beta = \beta_0 + \beta_1\alpha + \beta_2\alpha^2 + \cdots + \beta_{m-1}\alpha^{m-1}$, ou como uma m-upla $\beta = (\beta_0, \beta_1, \ldots, \beta_{m-1})$, onde α é um elemento primitivo de $\mathbb{F}_q$ e $0 \leq \beta_i \leq p-1$.

Seja ζ o número complexo $e^{\frac{2\pi i}{p}}$. Este é uma p-ésima raiz primitiva da unidade.

Exemplo 1.12. Para cada $\beta = (\beta_0, \beta_1, \ldots, \beta_{m-1}) \in \mathbb{F}_q$ defina χ_β como sendo a função de valor complexa definida em $\mathbb{F}_q$ por

$$\chi_\beta(\gamma) = \zeta^{\beta_0\gamma_0 + \cdots + \beta_{m-1}\gamma_{m-1}}, \quad \text{para todo} \quad \gamma = (\gamma_0, \ldots, \gamma_{m-1}) \in \mathbb{F}_q.$$

Então χ_β é um caractere aditivo.

De fato, temos que

$$\chi_\beta(\gamma + \gamma') = \zeta^{\beta_0(\gamma_0+\gamma_0') + \cdots + \beta_{m-1}(\gamma_{m-1}+\gamma_{m-1}')} = \zeta^{\beta_0\gamma_0 + \cdots + \beta_{m-1}\gamma_{m-1}} \zeta^{\beta_0\gamma_0' + \cdots + \beta_{m-1}\gamma_{m-1}'} = \chi_\beta(\gamma)\chi_\beta(\gamma')$$

Se colocarmos $\beta = 0$ obtemos o *caractere aditivo trivial* χ_0, onde $\chi_0(\gamma) = 1$ para todo $\gamma \in \mathbb{F}_q$.

Teorema 1.10. *Se χ é um caractere não trivial de um grupo abeliano finito G, então*

$$\sum_{g \in G} \chi(g) = 0$$

Demonstração: De fato, como χ é não trivial, existe $h \in G$ tal que $\chi(h) \neq 1$ assim teremos

$$\chi(h) \sum_{g \in G} \chi(g) = \sum_{g \in G} \chi(hg) = \sum_{g \in G} \chi(g)$$

pois, como g percorre todo G teremos que hg também percorrerá, logo teremos

$$(\chi(h) - 1) \sum_{g \in G} \chi(g) = 0$$

e como $\chi(h) \neq 1$ teremos a igualdade desejada. ■

Um resultado que utilizaremos ao longo do trabalho será colocado como um lema e segue abaixo.

Lema 1.11. *Sejam X um conjunto finito não vazio, n um inteiro positivo e R um anel. Considere a sequência $(y_{j,x})_{\substack{j \in \{1,\ldots,n\} \\ x \in X}}$ com elementos no anel R. Então*

$$\sum_{(x_1,\ldots,x_n) \in X^n} \left(\prod_{j=1}^{n} y_{(j,x_j)} \right) = \prod_{j=1}^{n} \left(\sum_{x \in X} y_{(j,x)} \right)$$

Demonstração: De fato, mostremos por indução em n. Se $n = 1$ é válido. Suponha que vale para $n-1$. Logo teremos

$$\sum_{(x_1,\ldots,x_n) \in X^n} \left(\prod_{j=1}^{n} y_{(j,x_j)} \right) = \sum_{x_n \in X} \left(\sum_{(x_1,\ldots,x_{n-1}) \in X^{n-1}} \left(\prod_{j=1}^{n-1} y_{(j,x_j)} y_{(n,x_n)} \right) \right) =$$
$$\sum_{x_n \in X} y_{(n,x_n)} \left(\sum_{(x_1,\ldots,x_{n-1}) \in X^{n-1}} \left(\prod_{j=1}^{n-1} y_{(j,x_j)} \right) \right) = \left(\sum_{x \in X} y_{(n,x)} \right) \prod_{j=1}^{n-1} \left(\sum_{x \in X} y_{(j,x)} \right) = \prod_{j=1}^{n} \sum_{x \in X} y_{(j,x)}.$$

■

Lema 1.12. *Seja χ um caractere aditivo não trivial, $x \in \mathbb{F}_q^n$ fixado e $x \cdot y$ o produto escalar de x*

e y. Então

$$\sum_{y\in\mathbb{F}_q^n}\chi(x\cdot y)=\begin{cases}0 & se \quad x\neq 0\\ q^n & se \quad x=0\end{cases}$$

Demonstração: De fato, temos que, se $x=0$ então $x_i=0$ para $i=1,\dots n$ logo para todo $i=1,\dots,n$ e teremos $\sum_{y_i\in\mathbb{F}_q}\chi(x_iy_i)=q$, assim, pelo Lema 1.11 teremos $\sum_{y\in\mathbb{F}_q^n}\chi(x\cdot y)=\prod_{i=1}^{n}\sum_{y_i\in\mathbb{F}_q}\chi(x_iy_i)=\prod_{i-1}^{n}q=q^n$. Por outro lado, se $x\neq 0$ então $x_i\neq 0$ para algum $1\leq i\leq n$, digamos $i=r$ e teremos pelo Teorema 1.10 que $\sum_{y_r\in\mathbb{F}_q}\chi(x_ry_r)=0$, portanto $\sum_{y\in\mathbb{F}_q^n}\chi(x\cdot y)=\prod_{i=1}^{n}\sum_{y_i\in\mathbb{F}_q}\chi(x_iy_i)=0$. ■

Lema 1.13. *Seja χ um caractere aditivo não trivial de $\mathbb{F}_q$. Então, para qualquer código linear $\mathscr{C}$ sobre $\mathbb{F}_q$*

$$\sum_{v\in\mathscr{C}}\chi(v\cdot u)=\begin{cases}0 & se \quad u\notin\mathscr{C}^\perp\\ |\mathscr{C}| & se \quad u\in\mathscr{C}^\perp\end{cases}$$

Demonstração: De fato, se $u\in\mathscr{C}^\perp$ então $v\cdot u=0$ logo teremos $\chi(v\cdot u)=\chi(0)=1$ donde $\sum_{v\in\mathscr{C}}\chi(v\cdot u)=\sum_{v\in\mathscr{C}}1=|\mathscr{C}|$. Suponha agora que $u\notin\mathscr{C}^\perp$, logo temos a igualdade $\sum_{v\in\mathscr{C}}\chi(v\cdot u)=\sum_{a\in\mathbb{F}_q}\sum_{v\in\mathscr{C},v\cdot u=a}\chi(a)$.

Note que para todo $a\in\mathbb{F}_q$ existe $v\in\mathscr{C}$ tal que $v\cdot u=a$, pois, como $u\notin\mathscr{C}^\perp$ temos que $v\cdot u=k\neq 0$ logo teremos $(\alpha v)\cdot u=\alpha k$ e fazendo α percorrer $\mathbb{F}_q$ conseguiremos todos os elementos de $\mathbb{F}_q$. Além disso, para cada $a\in\mathbb{F}_q$ o número de vetores $v\in\mathscr{C}$ tal que $v\cdot u=a$ é o mesmo. Para mostrarmos esta afirmação, tomemos $a=0$ e um $0\neq k\in\mathbb{F}_q$ arbitrário e consideremos os conjuntos $A=\{v\in\mathscr{C}:v\cdot u=0\}$ e $B=\{v\in\mathscr{C}:v\cdot u=k\}$, mostremos que $|A|=|B|$. De fato, seja $w\in\mathscr{C}$ tal que $w\cdot u=k$, que existe pois $u\notin\mathscr{C}^\perp$. Considere o quociente $\mathscr{C}/A$. Temos que $w+A\in\mathscr{C}/A$ e portanto $|w+A|=|A|$. Além disso temos que $w+A=B$. De fato, se $w_1\in w+A$ então $w_1=w+x$ logo, $w_1\cdot u=(w+x)\cdot u=w\cdot u=k$ portanto $w_1\in B$. Reciprocamente, se $w_1\in B$ então podemos escrever $w_1=w+(w_1-w)$, pois $w_1-w\in A$. Portanto temos que $|\{v\in\mathscr{C}:v\cdot u=k_1\}|=|\{v\in\mathscr{C}:v\cdot u=k_2\}|$ para todo $k_1,k_2\in\mathbb{F}_q$. Logo teremos, para $u\notin\mathscr{C}^\perp$ que $\sum_{v\in\mathscr{C}}\chi(v\cdot u)=\sum_{a\in\mathbb{F}_q}\left(\sum_{v\in\mathscr{C},v\cdot u=a}\chi(a)\right)=\sum_{v\in\mathscr{C},v\cdot u=a}\left(\sum_{a\in\mathbb{F}_q}\chi(a)\right)=\frac{|\mathscr{C}|}{|A|}\sum_{a\in\mathbb{F}_q}\chi(a)$.

Pelo Teorema 1.10 temos que $\sum_{a\in\mathbb{F}_q}\chi(a)=0$, logo temos o resultado desejado. ■

Definição 1.24 (Transformada de Hadamard)**.** *Seja f uma função definida de $\mathbb{F}_q^n$ em uma $\mathbb{C}$-Álgebra e χ um caractere aditivo não trivial em $\mathbb{F}_q^n$. A transformada de Hadamard $\hat{f}$ de f é*

definida por

$$\hat{f}(u)=\sum_{v\in\mathbb{F}_q^n}\chi(u\cdot v)f(v).$$

Lema 1.14 (Fórmula da soma discreta de Poisson)**.** *Seja $\mathscr{C}$ um [n,k] código linear sobre $\mathbb{F}_q$ e f uma função em $\mathbb{F}_q^n$. Então*

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

Demonstração: De fato, pelo Lema 1.13 temos que $\sum_{u\in\mathscr{C}}\chi(u\cdot v)=0$ se $v\notin\mathscr{C}^\perp$ e $\sum_{u\in\mathscr{C}}\chi(u\cdot v)=|C|$ se $v\in\mathscr{C}^\perp$. Agora pela definição 1.24 temos que

$$\sum_{u\in\mathscr{C}}\hat{f}(u)=\sum_{u\in\mathscr{C}}\sum_{v\in\mathbb{F}_q^n}\chi(u\cdot v)f(v)=\sum_{v\in\mathbb{F}_q^n}f(v)\sum_{u\in\mathscr{C}}\chi(u\cdot v)=|\mathscr{C}|\sum_{u\in\mathscr{C}^\perp}f(u)$$

e temos o resultado desejado. ■

Lema 1.15. *Seja $f:\mathbb{F}_q^n\longrightarrow\mathbb{C}[x]$ dada por $f(u)=x^{\omega_H(u)}$, então sua transformada de Hadamard $\hat{f}$ de f é dada por*

$$\hat{f}(u)=\sum_{v\in\mathbb{F}_q^n}\chi(u\cdot v)f(v)=(1+(q-1)x)^{n-\omega_H(u)}(1-x)^{\omega_H(u)}.$$

Demonstração: De fato, se $\alpha\neq 0$ então $\sum_{\beta\in\mathbb{F}_q}\chi(\alpha\beta)=0$ logo

$$0=\chi(0)+\sum_{0\neq\beta\in\mathbb{F}_q}\chi(\alpha\beta)=1+\sum_{0\neq\beta\in\mathbb{F}_q}\chi(\alpha\beta),$$

assim temos $\sum_{0\neq\beta\in\mathbb{F}_q}\chi(\alpha\beta)=-1$.

Denotemos os elementos de $\mathbb{F}_q$ por $w_0=0,w_1,\ldots,w_{q-1}$ e definamos a função $\phi(v_i)=\phi(w_s)=\begin{cases}1 & se \quad w_s\neq 0\\ 0 & se \quad w_s=0\end{cases}$, então teremos

$$\hat{f}(u)=\sum_{v\in\mathbb{F}_q^n}\chi(u\cdot v)f(v)=\sum_{v\in\mathbb{F}_q^n}\chi(u\cdot v)x^{\omega_H(v)}=\sum_{v\in\mathbb{F}_q^n}\left(\prod_{i=1}^{n}\chi(u_iv_i)x^{\phi(v_i)}\right)=$$
$$=\prod_{i=1}^{n}\left(\sum_{s=0}^{q-1}\chi(u_iw_s)x^{\phi(w_s)}\right)=\prod_{i=1}^{n}\left(\chi(0)x^{\phi(0)}+\sum_{s=1}^{q-1}\chi(u_iw_s)x^{\phi(w_s)}\right)=$$
$$=\prod_{i=1}^{n}\left(1+\sum_{s=1}^{q-1}\chi(u_iw_s)x\right)=\prod_{u_i=0}\left(1+\sum_{s=1}^{q-1}\chi(u_iw_s)x\right)\prod_{u_i\neq 0}\left(1+\sum_{s=1}^{q-1}\chi(u_iw_s)x\right)=$$
$$=(1+(q-1)x)^{n-\omega_H(u)}(1-x)^{\omega_H(u)}$$

■

Capítulo 2

Identidades de MacWilliams em posets

Um tema muito estudado na teoria dos códigos são os polinômios enumeradores de peso, vistos no final do capítulo anterior. Tais polinômios fornecem informações importantes sobre os códigos, tais como número de palavras, distância mínima entre outras, [10]. Neste capítulo veremos as identidades de MacWilliams, que nos mostram que o polinômio enumerador do código dual pode ser obtido através do polinômio enumerador do código e vice-versa. O capítulo é divido em duas seções. Na primeira seção do capítulo veremos o resultado clássico das identidades de MacWilliams para espaços de Hamming. Já na segunda seção determinaremos condições sobre um poset para que o mesmo admita as identidades de MacWilliams. Uma abordagem mais detalhada sobre esses assuntos podem ser obtidas em [10] e [7].

2.1 Identidades de MacWilliams em espaços de Hamming

Uma das mais importantes identidades na teoria de códigos é a identidade de MacWilliams para códigos lineares em um espaço de Hamming $\mathbb{F}_q^n$, a qual expressa o polinômio enumerador de um código $\mathscr{C}$ em termos do enumerador de peso do seu código dual $\mathscr{C}^\perp$ e vice-versa, visto que $\mathscr{C} = (\mathscr{C}^\perp)^\perp$.

Teorema 2.1 (Identidade de MacWilliams em espaços de Hamming)**.** *Seja $\mathbb{F}_q^n$ um espaço de Hamming. Se $\mathscr{C}$ é um $[n,k,d_H]$ código linear sobre $\mathbb{F}_q$ então*

$$W_{\mathscr{C}^\perp}(x) = \frac{1}{|\mathscr{C}|}(1+(q-1)x)^n W_{\mathscr{C}}\left(\frac{1-x}{1+(q-1)x}\right)$$

Demonstração: De fato, temos por (1.3) que $W_{\mathscr{C}^\perp}(x) = \sum_{u\in\mathscr{C}^\perp} x^{\omega_H(u)}$ e tomando $f(u) = x^{\omega_H(u)}$ e

aplicando a fórmula da soma discreta de Poisson teremos $W_{\mathscr{C}^\perp}(x) = \sum_{u\in\mathscr{C}^\perp} f(u) = \frac{1}{|\mathscr{C}|}\sum_{u\in\mathscr{C}} \hat{f}(u)$. Agora, aplicando o Lema 1.15 teremos

$$W_{\mathscr{C}^\perp}(x) = \frac{1}{|\mathscr{C}|}\sum_{u\in\mathscr{C}}(1+(q-1)x)^{n-\omega_H(u)}(1-x)^{\omega_H(u)} = \frac{1}{|\mathscr{C}|}(1+(q-1)x)^n \sum_{u\in\mathscr{C}}\left(\frac{1-x}{1+(q-1)x}\right)^{\omega_H(u)} =$$
$$= \frac{1}{|\mathscr{C}|}(1+(q-1)x)^n W_{\mathscr{C}}\left(\frac{1-x}{1+(q-1)x}\right)$$

■

Exemplo 2.1. Considere o código linear $\mathscr{C} = \{000, 011, 101, 110\}$ de comprimento 3 sobre $\mathbb{F}_2$. Assim temos que $\mathscr{C}^\perp = \{000, 111\}$, logo $W_{\mathscr{C}}(x) = 1+3x^2$ e $W_{\mathscr{C}^\perp}(x) = 1+x^3$.

Aplicando o Teorema 2.1 temos

$$W_{\mathscr{C}^\perp}(x) = \frac{1}{|\mathscr{C}|}(1+(q-1)x)^n W_{\mathscr{C}}\left(\frac{1-x}{1+(q-1)x}\right) = \frac{1}{4}(1+(2-1)x)^3\left(1+3\left(\frac{1-x}{1+(2-1)x}\right)^2\right) =$$
$$= \frac{1}{4}(1+x)^3\left(1+3\left(\frac{1-x}{1+x}\right)^2\right) = \frac{1}{4}\left((1+x)^3+3(1+x)(1-x)^2\right) = \frac{1}{4}(4+4x^3) = 1+x^3,$$

como esperado.

Exemplo 2.2. Consideremos o código de Hamming [7,4,3] dado no Exemplo 1.1. Sabemos que a distribuição de peso do código de Hamming é dada por $A_0(\mathscr{C}) = A_7(\mathscr{C}) = 1$ e $A_3(\mathscr{C}) = A_4(\mathscr{C}) = 7$. Logo temos que o polinômio enumerador de um código de Hamming [7,4,3] é dado por $W_{\mathscr{C}}(x) = 1+7x^3+7x^4+x^7$. Sabemos também que o código dual de um código de Hamming [7,4,3] tem uma palavra nula e as outras 7 com peso 4, logo temos que o polinômio enumerador do código dual será $W_{\mathscr{C}^\perp}(x) = 1+7x^4$, e assim vemos que, realmente temos $W_{\mathscr{C}^\perp}(x) = \frac{1}{|\mathscr{C}|}(1+(q-1)x)^n W_{\mathscr{C}}\left(\frac{1-x}{1+(q-1)x}\right)$.

Corolário 2.2. *Seja $\mathbb{F}_q^n$ um espaço de Hamming. Se $\mathscr{C}$ é um $[n,k,d_H]$ código linear sobre $\mathbb{F}_q$ então*

$$A_i^\perp = \frac{1}{|\mathscr{C}|}\sum_{j=0}^{n} A_j P_i(j;n).$$

Demonstração: De fato, tomando $\gamma = q-1$, temos por 1.4 que $(1+\gamma x)^{n-\omega_H(u)}(1-x)^{\omega_H(u)} = \sum_{i=0}^{n} P_i(\omega_H(u);n)x^i$. Logo teremos

$$W_{\mathscr{C}^\perp}(x) = \sum_{i=0}^{n} A_i^\perp x^i = \frac{1}{|\mathscr{C}|}\sum_{u\in\mathscr{C}}\sum_{i=0}^{n} P_i(\omega_H(u);n)x^i = \sum_{i=0}^{n}\sum_{u\in\mathscr{C}}\frac{1}{|\mathscr{C}|}P_i(\omega_H(u);n)x^i.$$

Note agora que $\sum_{u\in\mathscr{C}}\frac{1}{|\mathscr{C}|}P_i(\omega_H(u);n)x^i = \sum_{j=0}^{n}\sum_{u\in\mathscr{C},\omega_H(u)=j}\frac{1}{|\mathscr{C}|}P_i(j;n) = \sum_{j=0}^{n}\frac{A_j}{|\mathscr{C}|}P_i(j;n)$. Logo pela igualdade de polinômios temos que $A_i^\perp = \frac{1}{|\mathscr{C}|}\sum_{j=0}^{n} A_j P_i(j;n)$ ■

Isto nos mostra que o polinômio enumerador de peso do código $\mathscr{C}$ e consequentemente sua distribuição de peso é unicamente determinado pelo polinômio enumerador de peso do código dual $\mathscr{C}^\perp$ e consequentemente sua distribuição de peso. Um exemplo sobre isto pode ser visto considerando-se os códigos de Hamming.

Exemplo 2.3. O código dual de um código de Hamming é chamado de código simplex. Seja $n = \frac{(q^r-1)}{(q-1)}$, então todas as palavras do $[n,r]$-código simplex $\mathscr{C}$ tem peso q^{r-1}.

De fato, como $G = H_r$ é a matriz geradora do código simplex r-dimensional $\mathscr{C}$ sobre $\mathbb{F}_q$, temos que $\mathscr{C} = \{xG | x \in \mathbb{F}_q^r\}$, se $x \neq 0$, e assim $\omega_H(xG) = n - s$, onde s é o número de colunas y de G tal que $x \cdot y^T = 0$. Note que o conjunto de vetores de $\mathbb{F}_q^r$ ortogonal a x é um subespaço $(r-1)$-dimensional de $\mathbb{F}_q^r$ e assim exatamente $\frac{(q^{r-1}-1)}{(q-1)}$ colunas y de G satisfazem $x \cdot y^T = 0$. Então $\omega_H(xG) = \frac{q^r-1}{q-1} - \frac{q^{r-1}-1}{q-1} = q^{r-1}$.

Assim, a distribuição de peso de $\mathscr{C}$ é $A_0 = 1, A_{q^{r-1}} = q^r - 1$, e $A_i = 0$ para qualquer outro i. Logo pelo Corolário 2.2 teremos

$$A_i^\perp = q^{-r}\left(\sum_{j=0}^{n} A_j P_i(j:n)\right) = q^{-r}\left(A_0 P_i(0:n) + A_{q^{r-1}} P_i(q^{r-1}:n)\right) =$$
$$= q^{-r}\left(1.P_i(0:n) + (q^r-1)P_i(q^{r-1}:n)\right) = q^{-r}\left((q-1)^i\binom{n}{i} + (q^r-1)P_i(q^{r-1}:n)\right).$$

Logo conseguimos facilmente a distribuição de pesos do código dual $\mathscr{C}^\perp$ o qual é um $[n, n-r, 3]$-código de Hamming.

Como podemos considerar um código em um espaço de Hamming como sendo um P-código, onde o poset é uma anticadeia, nos vem a pergunta se conseguimos o mesmo resultado para posets em geral. O próximo exemplo nos mostra que nem sempre é possível. Porém na próxima seção estudaremos condições suficientes e necessárias para que um poset P admita as identidades de MacWilliams.

Exemplo 2.4. Sejam P um poset em $[3]$ com relação de ordem $1 \preceq 3$, sendo esta a única relação entre elementos de P e o poset dual P^*, ou seja, o poset em $[3]$ com relação de ordem $3 \preceq 1$, sendo esta a única relação de ordem entre elementos de P^*. Considere os P-códigos lineares

sobre $\mathbb{F}_2$ de comprimento 3, dados por

$$\mathscr{C}_1 = \{(0,0,0),(0,0,1)\} \qquad \mathscr{C}_2 = \{(0,0,0),(1,1,0)\}.$$

É fácil verificar que os enumeradores de P-peso de $\mathscr{C}_1$ e $\mathscr{C}_2$ são

$$W_{\mathscr{C}_1,P}(x) = 1 + x^2 = W_{\mathscr{C}_2,P}(x).$$

Os códigos duais de $\mathscr{C}_1$ e $\mathscr{C}_2$ são, respectivamente, dados por

$$\mathscr{C}_1^{\perp} = \{(0,0,0),(1,0,0),(0,1,0),(1,1,0)\} \qquad \text{e} \qquad \mathscr{C}_2^{\perp} = \{(0,0,0),(1,1,0),(0,0,1),(1,1,1)\}.$$

Temos que os enumeradores de P^*-peso de $\mathscr{C}_1^{\perp}$ e $\mathscr{C}_2^{\perp}$ são, respectivamente

$$W_{\mathscr{C}_1^{\perp},P^*}(x) = 1 + x + x^2 + x^3 \qquad \text{e} \qquad W_{\mathscr{C}_2^{\perp},P^*}(x) = 1 + x + 2x^3.$$

Vemos então que os polinômios enumeradores dos códigos duais não são unicamente determinados pelos polinômios enumeradores dos códigos, pois se fossem deveríamos ter $W_{\mathscr{C}_1^{\perp},P^*}(x) = W_{\mathscr{C}_2^{\perp},P^*}(x)$.

2.2 Posets admitindo identidades de MacWilliams

Como vimos no Exemplo 2.4, nem todos os posets admitem as identidades de MacWilliams. Nesta seção determinaremos condições para que um poset as admita. Primeiramente definamos quando um poset admite tais identidades e depois vejamos que posets satisfazem a definição.

Definição 2.1. *Seja P um poset em $[n]$. Dizemos que P admite identidade de MacWilliams se o enumerador de P^*-peso do código dual $\mathscr{C}^{\perp}$ de um P-código linear sobre $\mathbb{F}_q$ é unicamente determinado pelo enumerador de P-peso de $\mathscr{C}$ independentemente do P-código linear $\mathscr{C}$.*

A definição acima nos diz que um poset P admite identidade de MacWilliams se, e somente se, $\mathscr{C}_1$ e $\mathscr{C}_2$ são dois P-códigos lineares com $W_{\mathscr{C}_1,P}(x) = W_{\mathscr{C}_2,P}(x)$ então $W_{\mathscr{C}_1^{\perp},P^*}(x) = W_{\mathscr{C}_2^{\perp},P^*}(x)$.

2.2.1 Condição Necessária para admitir Identidade de MacWilliams

Vejamos uma condição necessária para um poset P admitir identidade de MacWilliams. Lembremos primeiramente do Exemplo 1.9, que um poset hierárquico é uma soma ordinal de

anticadeias, as quais formam os níveis do poset e onde cada elemento do j-ésimo nível está relacionado com todos os elementos dos níveis anteriores.

Seja $\mathbb{H}(n;n_1,n_2,\ldots,n_t)$ o poset hierárquico com t-níveis e n elementos. Para cada $1\leq i\leq t$ tomamos o conjunto $\{(i,j)|1\leq j\leq n_i\}$ de $\mathbb{H}(n;n_1,n_2,\ldots,n_t)$, o qual é chamado de conjunto de i-ésimo nível de $\mathbb{H}(n;n_1,n_2,\ldots,n_t)$ e denotado por $\Gamma^i(\mathbb{H})$, ou seja, $\Gamma^i(\mathbb{H})$ é uma anticadeia de cardinalidade n_i.

Relacionaremos as posições coordenadas de vetores em $\mathbb{F}_q^n$ com os elementos do poset $\mathbb{H}(n;n_1,n_2,\ldots,n_t)$, identificando o subconjunto $\{n_1+n_2+\cdots+n_{i-1}+1,\ldots,n_1+n_2+\cdots+n_{i-1}+n_i\}$ de $[n]$ com o conjunto de i-ésimo nível $\Gamma^i(\mathbb{H})$, colocando $n_0=0$.

Para um poset P, definimos $\min(P)=\{i\in P|i \text{ é um minimal em } P\}$ e também $\max(P)=\{i\in P|i \text{ é um maximal em } P\}$.

Vejamos agora 4 resultados, que nos auxiliarão a mostrar que uma condição necessária para que um poset P admita identidade de MacWilliams é que este deve ser um poset hierárquico.

Lema 2.3. *Seja P um poset em $[n]$ e P^* o poset dual de P. Para $x\in\mathbb{F}_q^n$, temos*

$$\omega_{P^*}(x)=n \Leftrightarrow supp(x)\supseteq min(P)$$

Demonstração: De fato, note primeiramente que $\min(P)=\max(P^*)$. Assim temos que $\min(P)\subseteq \operatorname{supp}(x)\Leftrightarrow \max(P^*)\subseteq\operatorname{supp}(x)\Leftrightarrow |\langle\operatorname{supp}(x)\rangle_{P^*}|=n\Leftrightarrow \omega_{P^*}(x)=n$. ∎

Para um poset P dado, colocamos $P'=P\backslash\min(P)$, o qual é um poset com relação de ordem induzida pela relação de ordem de P.

Lema 2.4. *Seja P um poset de cardinalidade n. Suponha que $|min(P)|=n_1$. Então, para cada vetor $x\in\mathbb{F}_q^n$ satisfazendo $supp(x)\subseteq min(P)$, temos q^{n-n_1} divide $|\{y\in\mathbb{F}_q^n : x\cdot y=0 \text{ e } \omega_{P^*}(y)=n\}|$.*

Demonstração: Sem perda de generalidade, podemos assumir que $\min(P)=\{1,2,\ldots,n_1\}$. Como $\operatorname{supp}(x)\subseteq\min(P)$, podemos escrever x na forma $x=(x_1,\ldots,x_i,0,\ldots,0)$, onde $0\neq x_j\in\mathbb{F}_q$ para todo $1\leq j\leq i$ e $i\leq n_1$. Denotemos por A o conjunto dos vetores sobre $\mathbb{F}_q$ de comprimento i definido por $A:=\{(y_1,\ldots,y_i)\in\mathbb{F}_q^i : x_1y_1+\cdots+x_iy_i=0 \text{ e } y_j\neq 0 \text{ para } 1\leq j\leq i\}$. Então temos $|\{y\in\mathbb{F}_q^n : x\cdot y=0,\ \omega_{P^*}(y)=n\}|=|A|q^{n-n_1}(q-1)^{n_1-i}$. ∎

Lema 2.5. *Suponha que P admite indentidade de MacWilliams. Então, para cada elemento minimal $i\in P'=P\backslash min(P)$ e $j\in min(P)$, temos $i\succeq_P j$.*

Demonstração: Sejam $|P| = n$ e $|\min(P)| = n_1$. Se $n = n_1$, o lema é verdadeiro. Suponhamos que $n > n_1$.

Afirmamos que $|\langle i \rangle_P| = 1 + |\min(P)|$ para cada $i \in \min(P')$.

De fato, suponha o contrário. Então podemos escolher $i \in \min P'$ tal que $|\langle i \rangle_P| < 1 + |\min(P)|$, logo podemos escolher dois vetores $x_1, x_2 \in \mathbb{F}_q^n$ tais que $\text{supp}(x_1) = \{i\}$, $\text{supp}(x_2) \subseteq \min(P)$ e $|\langle \text{supp}(x_1) \rangle_P| = |\langle \text{supp}(x_2) \rangle_P|$.

Consideremos agora dois P-códigos lineares $\mathscr{C}_1$ e $\mathscr{C}_2$ gerados por x_1 e x_2 respectivamente. Como $|\langle \text{supp}(x_1) \rangle_P| = |\langle \text{supp}(x_2) \rangle_P|$, $\mathscr{C}_1$ e $\mathscr{C}_2$ tem o mesmo enumerador de P-peso. Como por hipótese P admite MacWilliams, teremos que $\mathscr{C}_1^\perp$ e $\mathscr{C}_2^\perp$ tem mesmo enumerador de P^*-peso. Portanto, devemos ter $|\{v \in \mathscr{C}_1^\perp : \omega_{P^*}(v) = n\}| = |\{v \in \mathscr{C}_2^\perp : \omega_{P^*}(v) = n\}|$.

Temos que $|\{v \in \mathscr{C}_1^\perp : \omega_{P^*}(v) = n\}| = q^{n-(n_1+1)}(q-1)^{n_1}$ pois, uma vez que $\text{supp}(x_1) = \{i\}$, temos $x_1 = (0, \ldots, 0, x_i^1, 0, \ldots, 0)$ e como $\omega_{P^*}(v) = n$ devemos ter $v_j \neq 0$ para $1 \leq j \leq n_1$, $v_i = 0$ e as outras coordenadas de v podem assumir qualquer valor em $\mathbb{F}_q$.

Assim, segue do Lema 2.4 que $q^{n-n_1} \Big| |\{v \in \mathscr{C}_2^\perp : \omega_{P^*}(v) = n\}| = |\{v \in \mathscr{C}_1^\perp : \omega_{P^*}(v) = n\}| = q^{n-(n_1+1)}(q-1)^{n_1}$.

Entretanto, como q é uma potência de primo isto é impossível. Portanto temos que $|\langle i \rangle_P| = 1 + |\min(P)|$ para cada $i \in \min P'$ e assim $i \succeq_P j$. ∎

Observação 2.1. Se $i \in P'$, então $i \succeq_P k$ para algum $k \in \min(P')$. Entretanto, nós obtivemos o resultado que se P admite identidade de MacWilliams, então para $i \in P'$ e $j \in \min(P)$, temos $i \succeq_P j$.

Lema 2.6. *Se P é um poset que admite identidade de MacWilliams, então P' também admite identidade de MacWilliams.*

Demonstração: Sejam $|P| = n$ e $|\min(P)| = n_1$. Se $n = n_1$, o lema é verdadeiro. Assumamos que $n > n_1$.

Consideremos dois P'-códigos lineares $\mathscr{C}_1'$ e $\mathscr{C}_2'$ de comprimento $n - n_1$ sobre $\mathbb{F}_q$ com mesmo enumerador de P'-peso.

Tomemos dois P-códigos lineares de comprimento n definidos por

$$\mathscr{C}_1 = \mathbb{F}_q^{n_1} \oplus \mathscr{C}_1' = \{(u, v) : u \in F_q^{n_1}, v \in \mathscr{C}_1'\}$$

e

$$\mathscr{C}_2 = \mathbb{F}_q^{n_1} \oplus \mathscr{C}_2' = \{(u, v) : u \in F_q^{n_1}, v \in \mathscr{C}_2'\}$$

.

Segue da observação acima que $\mathscr{C}_1$ e $\mathscr{C}_2$ tem mesmo enumerador de P-peso.

De fato, se $(u,v) \in \mathscr{C}_i$ então $\text{supp}(u,0) \subseteq \min(P)$ e como se $i \in P'$ e $j \in \min(P)$ implica que $i \succeq_P j$, então segue do fato que $\mathscr{C}_1'$ e $\mathscr{C}_2'$ tem mesmo enumerador de P'-peso que $\mathscr{C}_1$ e $\mathscr{C}_2$ tem mesmo enumerador de P-peso. Logo, pela hipótese teremos que $\mathscr{C}_1^{\perp}$ e $\mathscr{C}_2^{\perp}$ tem mesmo enumerador de P^*-peso.

Como $\mathscr{C}_i^{\perp} = \{(0,v) : 0 \in \mathbb{F}_q^{n_1}, v \in \mathscr{C}_i'^{\perp}\}$ para $i = 1,2$ temos que $\mathscr{C}_1^{\perp}$ e $\mathscr{C}_2^{\perp}$ tem mesmo enumerador de $(P')^*$. Portanto P' também admite identidade de MacWilliams. ■

Teorema 2.7. *Se P admite identidade de MacWilliams, então P é um poset hierárquico.*

Demonstração: Seja P um poset que admite identidade de MacWilliams tal que $|P| = n$ e $|\min(P)| = n_1$. Mostremos por indução, ou seja, supondo que P' é um poset hierárquico mostremos que P também o é. Se $n = n_1$, então P é um poset hierárquico com apenas um nível. Suponha que $n > n_1$, então, pelo Lema 2.6 temos que $P' = P \backslash \min(P)$ é um poset que admite identidade de MacWilliams e pela hipótese indutiva P' é hierárquico. Logo temos P' definido no conjunto $\{(i,j) : 2 \leq i \leq t, 1 \leq j \leq n_i\}$ com relação de ordem dada por $(i,j) \preceq_{P'} (l,m) \Leftrightarrow i \preceq_{P'} l$.

Se tomarmos $\min(P)$ definido no conjunto $\{(1,j) : 1 \leq j \leq n_1\}$, então este conjunto é uma anticadeia e pelo Lema 2.5, para cada elemento minimal $j \in P'$ e $l \in \min(P)$ temos $j \succeq_P l$, então teremos $(2,j) \succ_P (1,l)$ para todo $1 \leq l \leq n_1$. Portanto P é um poset hierárquico. ■

2.2.2 Condição Suficiente para admitir Identidade de MacWilliams

Veremos nessa subseção que, a condição necessária vista na subseção anterior também é uma condição suficiente para que o poset admita identidade de MacWilliams. Para isso introduziremos a definição de polinômio enumerador da distribuição de P-peso por nível e de polinômio enumerador do i-ésimo nível.

A menos de mencionarmos o contrário, o poset P utilizado nessa subseção será o poset hierárquico $P = \mathbb{H}(n; n_1, \ldots, n_t)$ com n elementos e t níveis.

Utilizaremos as seguintes notações, para simplificar:

$$\widehat{n_i} = n - (n_1 + \cdots + n_i) = n_{i+1} + \cdots + n_t$$

e

$$\widetilde{u_{i+1}} = (u_{i+1}, \ldots, u_t) \in \mathbb{F}_q^{\widehat{n_i}}, \text{ onde } u_j \in \mathbb{F}_q^{n_j}.$$

Como vimos anteriormente, podemos relacionar as posições coordenadas dos vetores de $\mathbb{F}_q^n$ com os conjuntos subjacentes de P. Como $n = n_1 + \cdots + n_t$ e $\mathbb{F}_q^n = \mathbb{F}_q^{n_1} \oplus \mathbb{F}_q^{n_2} \oplus \cdots \oplus \mathbb{F}_q^{n_t}$, para $u \in \mathbb{F}_q^n$ podemos escrever $u = (u_1, \ldots, u_t)$ com $u_i \in \mathbb{F}_q^{n_i}$.

Definiremos ainda para um P-código linear $\mathscr{C}$:

$$\mathscr{C}_i = \{u \in \mathscr{C} : \widehat{u_{i+1}} = 0\} \qquad \text{e} \qquad \mathscr{C}_i^1 = \{u \in \mathscr{C}_i : u_i \neq 0\}.$$

Introduzamos agora o polinômio enumerador da distribuição de P-peso por nível. Seja $\mathscr{C}$ um P-código linear de comprimento n sobre $\mathbb{F}_q$. O polinômio enumerador da distribuição de P-peso por nível é dado por

$$W_{\mathscr{C},P}(x : y_0, y_1, \ldots, y_t) = \sum_{u \in \mathscr{C}} x^{\omega_P(u)} y_{s(u)} = A_{0,P}\, y_0 + (A_{1,P}\, x + \cdots + A_{n_1,P}\, x^{n_1}) y_1 +$$
$$(A_{n_1+1,P}\, x^{n_1+1} + \cdots + A_{n_1+n_2,P}\, x^{n_1+n_2}) y_2 + \cdots + (A_{n_1+\cdots+n_{t-1},P}\, x^{n_1+\cdots+n_{t-1}+1} + \cdots + A_{n_1+\cdots+n_t,P}\, x^{n_1+\cdots+n_t}) y_t,$$

onde $s(u) = \max\{i : u_i \neq 0\}$ com $u = (u_1, \ldots, u_t)$ e $A_{i,P} = |\{u \in \mathscr{C} : \omega_P(u) = i\}|$.

Para simplificar, utilizando o fato que $n - \widehat{n_i} = (n_1 + \cdots + n_i)$, $n_0 = 0$, podemos escrever

$$W_{\mathscr{C},P}(x : y_0, y_1, \ldots, y_t) = \sum_{u \in \mathscr{C}} x^{\omega_P(u)} y_{s(u)} = A_{0,P}\, y_0 + (A_{n-\widehat{n_0}+1,P}\, x^{n-\widehat{n_0}+1} + \cdots + A_{n-\widehat{n_1},P}\, x^{n-\widehat{n_1}}) y_1 +$$
$$+ (A_{n-\widehat{n_1}+1,P}\, x^{n-\widehat{n_1}+1} + \cdots + A_{n-\widehat{n_2},P}\, x^{n-\widehat{n_2}}) y_2 + \cdots + (A_{n-\widehat{n_{t-1}}+1,P}\, x^{n-\widehat{n_{t-1}}+1} + \cdots + A_{n-\widehat{n_t},P}\, x^{n-\widehat{n_t}}) y_t =$$
$$= A_{0,P}\, y_0 + \sum_{j=1}^{t} (A_{n-\widehat{n_{j-1}+1},P}\, x^{n-\widehat{n_{j-1}}} + \cdots + A_{n-\widehat{n_j},P}\, x^{n-\widehat{n_j}}) y_j) =$$
$$= A_{0,P}\, y_0 + \sum_{j=1}^{t} \left(\sum_{i=1}^{n_j} A_{n-\widehat{n_{j-1}}+i,P}\, x^{n-\widehat{n_{j-1}}+i} \right) y_j.$$

Ou seja, temos que

$$W_{\mathscr{C},P}(x : y_0, y_1, \ldots, y_t) = A_{0,P}\, y_0 + \sum_{i=1}^{t} \left(\sum_{j=1}^{n_i} A_{n-\widehat{n_{i-1}}+j,P}\, x^{n-\widehat{n_{i-1}}+j} \right) y_i. \tag{2.1}$$

Note que se colocarmos $y_i = 1$ para todo $0 \leq i \leq t$ teremos $W_{\mathscr{C},P}(x : y_0, y_1, \ldots, y_t) = W_{\mathscr{C},P}(x)$. Aqui utilizaremos a mesma notação que utilizamos em espaços de Hamming.

Outro polinômio enumerador que introduziremos é o polinômio enumerador do i-ésimo nível, no qual os coeficientes são o número de palavras do código do i-ésimo nível do poset

P. Tal polinômio é dado por

$$LW^{(i)}_{\mathscr{C},P}(x)=\sum_{j=1}^{n_i}A_{n-\widehat{n_{i-1}}+j,P}\,x^{n-\widehat{n_{i-1}}+j}=\left(\sum_{j=1}^{n_i}A_{n-\widehat{n_{i-1}}+j,P}\,x^{j}\right)x^{n-\widehat{n_{i-1}}}=W_{\mathscr{C}_i,P}(x)-W_{\mathscr{C}_{i-1},P}(x). \quad (2.2)$$

Colocamos ainda $LW^{(0)}_{\mathscr{C},P}(x)=A_{0,P}$. Note que o polinômio $LW^{(i)}_{\mathscr{C},P}(x)$ nada mais é que o coeficiente de y_i no polinômio dado em (2.1).

Com as notações estabelecidas acima, mostremos que é suficiente um poset ser hierárquico para que este admita identidade de MacWilliams.

Para este fim, lembrando que $W_{\mathscr{C}^\perp,P^*}(x:z_0,z_1\ldots,z_t)=\sum_{u\in\mathscr{C}^\perp}x^{\omega_{P^*}(u)}z_{s_{p^*(u)}}$, apliquemos a fórmula da soma discreta de Poisson definida no Lema 1.14 na função $f(u)=x^{\omega_{P^*}(u)}z_{s^*(u)}$, onde $s^*(u)=\min\{i:u_i\neq 0\}$.

Coloquemos $s^*(0)=t+1$ e consideremos o conjunto $D_i=\{u=(u_1,\ldots,u_t)\in\mathbb{F}_q^n:u_1=\cdots=u_i=0 \text{ e } u_{i+1}\neq 0\}$ para $0\leq i\leq t$. Note que $D_t=\{0\in\mathbb{F}_q^n\}$ e $\mathbb{F}_q^n=\bigcup_{i=0}^{t}D_i$ onde a união é disjunta.

Encontremos a transformada de Hadammard, $\hat{f}(u)$. Pela definição 1.24 e das considerações acima, temos que

$$\hat{f}(u)=\sum_{v\in\mathbb{F}_q^n}\chi(u\cdot v)f(v)=\sum_{i=0}^{t}\sum_{v\in D_i}\chi(u\cdot v)x^{\omega_{P^*}(v)}z_{s^*(v)}. \quad (2.3)$$

Vamos denotar a soma interna em 2.3 por $S_i(u)$ para $0\leq i\leq t$ e consideremos $i<t$ logo, para $v\in D_i$ temos que

$$\omega_{P^*}(v)=n_{i+2}+\cdots+n_t+\omega_H(v_{i+1})=\widehat{n_{i+1}}+\omega_H(v_{i+1}) \qquad \text{e} \qquad s^*(v)=i+1.$$

Assim teremos, para $i<t$, tomando $Q(x)=\dfrac{1-x}{1+(q-1)x}$ e aplicando o Lema 1.15 que

$$S_i(u)=\sum_{v\in D_i}\chi(u\cdot v)x^{\widehat{n_{i+1}}+\omega_H(v_{i+1})}z_{i+1}=x^{\widehat{n_{i+1}}}z_{i+1}\sum_{v\in D_i}\chi(u\cdot v)x^{\omega_H(v_{i+1})}=$$

$$=x^{\widehat{n_{i+1}}}z_{i+1}\left(\sum_{\widetilde{v_{i+2}}\in\mathbb{F}_q^{\widehat{n_{i+1}}}}\chi(\widetilde{u_{i+2}}\cdot\widetilde{v_{i+2}})\right)\left(\sum_{0\neq v_{i+1}\in\mathbb{F}_q^{n_{i+1}}}\chi(u_{i+1}\cdot v_{i+1})x^{\omega_H(v_{i+1})}\right)=$$

$$=x^{\widehat{n_{i+1}}}z_{i+1}\left(\sum_{\widetilde{v_{i+2}}\in\mathbb{F}_q^{\widehat{n_{i+1}}}}\chi(\widetilde{u_{i+2}}\cdot\widetilde{v_{i+2}})\right)\Big((1+(q-1)x)^{n_{i+1}-\omega_H(u_{i+1})}(1-x)^{\omega_H(u_{i+1})}-1\Big)=$$

$$=x^{\widehat{n_{i+1}}}z_{i+1}\left(\left(\frac{1-x}{Q(x)}\right)^{n_{i+1}}Q(x)^{\omega_H(u_{i+1})}-1\right)\left(\sum_{\widetilde{v_{i+2}}\in\mathbb{F}_q^{\widehat{n_{i+1}}}}\chi(\widetilde{u_{i+2}}\cdot\widetilde{v_{i+2}})\right).$$

Segue do Lema 1.12 que

$$S_i(u)=\begin{cases}0 & se\quad \widetilde{u_{i+2}}\neq 0\in\mathbb{F}_q^{\widehat{n_{i+1}}}\\ (qx)^{\widehat{n_{i+1}}}z_{i+1}\left(\left(\frac{1-x}{Q(x)}\right)^{n_{i+1}}Q(x)^{\omega_H(u_{i+1})}-1\right) & se\quad \widetilde{u_{i+2}}=0\end{cases}\tag{2.4}$$

Agora, se $i=t$ teremos $\sum_{v\in D_t}\chi(u\cdot v)x^{\widehat{n_{t+1}}+\omega_H(v_{t+1})}z_{t+1}=z_{t+1}$ pois $v=0$, logo em (2.3) teremos

$$\hat{f}(u)=z_{t+1}+\sum_{i=0}^{t-1}S_i(u)$$

onde $S_i(u)$ é dado em (2.4).

Consideremos agora o P-código linear $\mathscr{C}$ de comprimento n sobre $\mathbb{F}_q$ e o subespaço $\mathscr{C}_i$ de $\mathscr{C}$ dado por $\mathscr{C}_i=\{u\in\mathscr{C}:\widetilde{u_{i+1}}=0\}$. Assim, segue de (2.4) que

$$\sum_{u\in\mathscr{C}}S_i(u)=\sum_{u\in\mathscr{C}_{i+1}}S_i(u)=(qx)^{\widehat{n_{i+1}}}z_{i+1}\sum_{u\in\mathscr{C}_{i+1}}\left(\left(\frac{1-x}{Q(x)}\right)^{n_{i+1}}Q(x)^{\omega_H(u_{i+1})}-1\right)\tag{2.5}$$

Lembrando que $Q(x)=\dfrac{1-x}{1+(q-1)x}$, a soma do lado direito da igualdade em (2.5) fica

$$\sum_{u\in\mathscr{C}_{i+1}}\left(\left(\frac{1-x}{Q(x)}\right)^{n_{i+1}}Q(x)^{\omega_H(u_{i+1})}-1\right)=(1+(q-1)x)^{n_{i+1}}\sum_{u\in\mathscr{C}_{i+1}}Q(x)^{\omega_H(u_{i+1})}-|\mathscr{C}_{i+1}|\tag{2.6}$$

Note ainda que $\mathscr{C}_{i+1}=\mathscr{C}_{i+1}^0\oplus\mathscr{C}_{i+1}^1$, onde $\mathscr{C}_{i+1}^0=\{u\in\mathscr{C}_{i+1}:u_{i+1}=0\}$ e $\mathscr{C}_{i+1}^1=\{u\in\mathscr{C}_{i+1}:$

$u_{i+1} \neq 0\}$, e para cada $u \in \mathscr{C}_{i+1}^1$ temos $\omega_P(u) = \omega_H(u_{i+1}) + (n - \widehat{n_i})$. Logo teremos

$$\begin{aligned}&\sum_{u\in\mathscr{C}_{i+1}} Q(x)^{\omega_H(u_{i+1})} = \sum_{u\in\mathscr{C}_{i+1}^0} Q(x)^{\omega_H(u_{i+1})} + \sum_{u\in\mathscr{C}_{i+1}^1} Q(x)^{\omega_H(u_{i+1})} = |\mathscr{C}_i| + \sum_{u\in\mathscr{C}_{i+1}^1} Q(x)^{\omega_P(u)-(n-\widehat{n_i})} = \\ &= |\mathscr{C}_i| + \left(\tfrac{1}{Q(x)}\right)^{n-\widehat{n_i}} \sum_{u\in\mathscr{C}_{i+1}^1} Q(x)^{\omega_P(u)}\end{aligned} \tag{2.7}$$

Portanto observando que por (2.2) temos $LW_{\mathscr{C},P}^{(i)}(x) = \sum_{u\in\mathscr{C}_{i+1}^1} Q(x)^{\omega_P(u)}$, segue de (2.5), (2.6) e (2.7) que:

$$\begin{aligned}&\sum_{u\in\mathscr{C}} S_i(u) = \sum_{u\in\mathscr{C}_{i+1}} S_i(u) = \\ &= (qx)^{\widehat{n_{i+1}}} z_{i+1}[(1+(q-1)x)^{n_{i+1}} \left(\left(\tfrac{1}{Q(x)}\right)^{n-\widehat{n_i}} \sum_{u\in\mathscr{C}_{i+1}^1} Q(x)^{\omega_P(u)} + |\mathscr{C}_i| \right) - |\mathscr{C}_{i+1}|] = \\ &= (qx)^{\widehat{n_{i+1}}}(1+(q-1)x)^{n_{i+1}} \left(\tfrac{1}{Q(x)}\right)^{n-\widehat{n_i}} z_{i+1} \sum_{u\in\mathscr{C}_{i+1}^1} Q(x)^{\omega_P(u)} + \\ &+ (qx)^{\widehat{n_{i+1}}} z_{i+1} \left(|\mathscr{C}_i|(1+(q-1)x)^{n_{i+1}} - |\mathscr{C}_{i+1}| \right) = \\ &= (qx)^{\widehat{n_{i+1}}}(1+(q-1)x)^{n_{i+1}} \left(\tfrac{1}{Q(x)}\right)^{n-\widehat{n_i}} z_{i+1} LW_{\mathscr{C},P}^{(i+1)}(Q(x)) + \\ &+ (qx)^{\widehat{n_{i+1}}} z_{i+1} \left(|\mathscr{C}_i|(1+(q-1)x)^{n_{i+1}} - |\mathscr{C}_{i+1}| \right) = \\ &= (qx)^{\widehat{n_{i+1}}}(1+(q-1)x)^{n_{i+1}}(1+(q-1)x)^{n-\widehat{n_i}}(1-x)^{-(n-\widehat{n_i})} z_{i+1} LW_{\mathscr{C},P}^{(i+1)}(Q(x)) + \\ &+ (qx)^{\widehat{n_{i+1}}} z_{i+1} \left(|\mathscr{C}_i|(1+(q-1)x)^{n_{i+1}} - |\mathscr{C}_{i+1}| \right) = \\ &= \frac{(qx)^n}{(qx)^{n-\widehat{n_{i+1}}}}(1+(q-1)x)^{n-\widehat{n_{i+1}}} \frac{(1-x)^{\widehat{n_i}}}{(1-x)^n} z_{i+1} LW_{\mathscr{C},P}^{(i+1)}(Q(x)) + \\ &+ (qx)^{\widehat{n_{i+1}}} z_{i+1} \left(|\mathscr{C}_i|(1+(q-1)x)^{n_{i+1}} - |\mathscr{C}_{i+1}| \right) = \\ &= \left(\tfrac{qx}{1-x}\right)^n \left(\tfrac{1+(q-1)x}{qx}\right)^{n-\widehat{n_{i+1}}} (1-x)^{\widehat{n_i}} z_{i+1} LW_{\mathscr{C},P}^{(i+1)}(Q(x)) + \\ &+ (qx)^{\widehat{n_{i+1}}} z_{i+1} \left(|\mathscr{C}_i|(1+(q-1)x)^{n_{i+1}} - |\mathscr{C}_{i+1}| \right).\end{aligned} \tag{2.8}$$

Lembrando que para $f(u) = x^{\omega_{P^*}(u)} z_{s^*(u)}$ temos $\hat{f}(u) = z_{t+1} + \sum_{i=0}^{t-1} S_i(u)$ e para simplificar,

denotando $a_i(x)=\left(\frac{1+(q-1)x}{qx}\right)^{n-\widehat{n_{i+1}}}$ e $b_i(x)=(1+(q-1)x)^{n_{i+1}}(qx)^{\widehat{n_{i+1}}}$ então por (2.8), teremos

$$\sum_{u\in\mathscr{C}}\hat{f}(u)=|\mathscr{C}|z_{t+1}+\sum_{u\in\mathscr{C}}\sum_{i=0}^{t-1}S_i(u)=|\mathscr{C}|z_{t+1}+\sum_{i=0}^{t-1}\sum_{u\in\mathscr{C}}S_i(u)=$$
$$=|\mathscr{C}|z_{t+1}+\sum_{i=0}^{t-1}\left(\left(\frac{qx}{1-x}\right)^n\left(\frac{1+(q-1)x}{qx}\right)^{n-\widehat{n_{i+1}}}(1-x)^{\widehat{n_i}}z_{i+1}LW^{(i+1)}_{\mathscr{C},P}(Q(x))+\right.$$
$$\left.+(qx)^{\widehat{n_{i+1}}}z_{i+1}\left(|\mathscr{C}_i|(1+(q-1)x)^{n_{i+1}}-|\mathscr{C}_{i+1}|\right)\right)=$$
$$=|\mathscr{C}|z_{t+1}+\left(\tfrac{qx}{1-x}\right)^n\sum_{i=0}^{t-1}a_i(x)(1-x)^{\widehat{n_i}}z_{i+1}LW^{(i+1)}_{\mathscr{C},P}(Q(x))+\sum_{i=0}^{t-1}b_i(x)z_{i+1}|\mathscr{C}_i|-\sum_{i=0}^{t-1}(qx)^{\widehat{n_{i+1}}}z_{i+1}|\mathscr{C}_{i+1}|. \tag{2.9}$$

Assim, como $W_{\mathscr{C},P}(x:y_0,\ldots,y_t)=\sum_{i=0}^{t}LW^{(i)}_{\mathscr{C},P}(x)y_i$, temos

$$\begin{aligned}&\left(\frac{qx}{1-x}\right)^n\sum_{i=0}^{t-1}a_i(x)z_{i+1}LW^{(i+1)}_{\mathscr{C},P}(Q(x))=\\&=\left(\frac{qx}{1-x}\right)^n\sum_{i=0}^{t}LW^{(i)}_{\mathscr{C},P}(Q(x))f_i=\left(\frac{qx}{1-x}\right)^n W_{\mathscr{C},P}(Q(x):f_0,\ldots,f_t)\end{aligned} \tag{2.10}$$

onde

$$f_i=\begin{cases}0 & se\quad i=0\\ \left(\frac{1+(q-1)x}{qx}\right)^{n-\widehat{n_i}}(1-x)^{\widehat{n_{i-1}}}z_i & se\quad i\geq 1.\end{cases} \tag{2.11}$$

Como $LW^{(i)}_{\mathscr{C},P}(1)=W_{\mathscr{C}_i,P}(1)-W_{\mathscr{C}_{i-1},P}(1)=|\mathscr{C}_i|-|\mathscr{C}_{i-1}|=A_{n_1+\cdots+n_{i-1},P}+\cdots+A_{n_1+\cdots+n_i,P}$ e além disso, $W_{\mathscr{C},P}(1:y_0,\ldots,y_t)=\sum_{i=0}^{t}LW^{(i)}_{\mathscr{C},P}(1)y_i$ teremos

$$\sum_{i=0}^{t-1}b_i(x)|\mathscr{C}_i|z_{i+1}=\sum_{i=0}^{t}LW^{(i)}_{\mathscr{C},P}(1)g_i=W_{\mathscr{C},P}(1:g_0,\ldots,g_t) \tag{2.12}$$

onde

$$g_j=\begin{cases}\sum_{i=j}^{t-1}(qx)^{\widehat{n_{i+1}}}(1+(q-1)x)^{n_{i+1}}z_{i+1} & se\quad 0\leq j\leq t-1\\ 0 & se\quad j=t\end{cases}. \tag{2.13}$$

Da mesma forma conseguimos escrever

$$\sum_{i=0}^{t-1}(qx)^{\widehat{n_{i+1}}}z_{i+1}|\mathscr{C}_{i+1}|=\sum_{i=0}^{t}LW^{(i)}_{\mathscr{C},P}(1)h_i=W_{\mathscr{C},P}(1:h_0,\ldots,h_t) \tag{2.14}$$

onde

$$h_j = \begin{cases} \sum_{i=1}^{t} \widehat{(qx)^{n_i}} z_i & se \quad j = 0 \\ \sum_{i=j}^{t} \widehat{(qx)^{n_i}} z_i & se \quad 1 \leq j \leq t-1 \end{cases} . \tag{2.15}$$

Assim, conseguimos o seguinte teorema:

Teorema 2.8. *Seja P um poset hierárquico com t-níveis e n elementos. Se $\mathscr{C}$ é um P-código linear de comprimento n sobre $\mathbb{F}_q$ então*

$$W_{\mathscr{C}^\perp,P^*}(x : z_{t+1},\ldots,z_1) = \tfrac{1}{|\mathscr{C}|} \sum_{u\in\mathscr{C}} \hat{f}(u) =$$
$$= z_{t+1} + \tfrac{1}{|\mathscr{C}|}\left(\left(\tfrac{qx}{1-x}\right)^n W_{\mathscr{C},P}(Q(x) : f_0,\ldots,f_t) + W_{\mathscr{C},P}(1 : g_0,\ldots,g_t) - W_{\mathscr{C},P}(1 : h_0,\ldots,h_t)\right)$$

onde $Q(x) = \dfrac{1-x}{1+(q-1)x}$, *e* f_i, g_i *e* h_i *são dados em (2.11), (2.13) e (2.15).*

Demonstração: De fato, de (2.9), (2.10), (2.12) e (2.14) temos que

$$\sum_{u\in\mathscr{C}} \hat{f}(u) = |\mathscr{C}| z_{t+1} + \left(\frac{qx}{1-x}\right)^n W_{\mathscr{C},P}(Q(x) : f_0,\ldots,f_t) + W_{\mathscr{C},P}(1 : g_0,\ldots,g_t) - W_{\mathscr{C},P}(1 : h_0,\ldots,h_t).$$

Agora, aplicando a fórmula da soma discreta de Poisson com $f(u) = x^{\omega_{P^*}(u)} z_{s^*(u)}$ teremos

$$W_{\mathscr{C}^\perp,P^*}(x : z_{t+1,\ldots,z_1}) = \sum_{u\in\mathscr{C}^\perp} f(u) = \frac{1}{|\mathscr{C}|} \sum_{u\in\mathscr{C}} \hat{f}(u) =$$
$$= \tfrac{1}{|\mathscr{C}|}\left(|\mathscr{C}| z_{t+1} + \left(\tfrac{qx}{1-x}\right)^n W_{\mathscr{C},P}(Q(x) : f_0,\ldots,f_t) + W_{\mathscr{C},P}(1 : g_0,\ldots,g_t) - W_{\mathscr{C},P}(1 : h_0,\ldots,h_t)\right).$$

E temos assim o resultado desejado. ∎

Com o resultado do teorema acima e do Teorema 2.7 conseguimos o seguinte teorema:

Teorema 2.9. *Um poset P admite identidade de MacWilliams se, e somente se, o poset P é hierárquico.*

Demonstração:

(⇒) Segue do Teorema 2.7.

(⇐) Se colocarmos $z_1 = \cdots = z_{t+1} = 1$ no Teorema 2.8, teremos que $W_{\mathscr{C}^\perp,P^*}(x : 1\ldots,1)$ se torna o enumerador de P^*-peso $W_{\mathscr{C}^\perp,P^*}(x)$ usual do código dual $\mathscr{C}^\perp$ no poset P^*. Portanto, o

enumerador de P^*-peso do código dual é unicamente determinado pelo enumerador de P-peso de $\mathscr{C}$. E temos o resultado.

■

Como ilustração para o teorema acima, lembrando que o caso de Hamming é um caso especial de poset quando o mesmo é uma anticadeia, vejamos que o teorema acima pode ser aplicado para este caso especial e obtemos o resultado encontrado no Teorema 2.1.

Corolário 2.10. *Seja P uma anticadeia de n elementos e $\mathscr{C}$ um P-código linear de comprimento n sobre $\mathbb{F}_q$. Então*

$$W_{\mathscr{C}^\perp}(x) = W_{\mathscr{C}^\perp,P^*}(x:1,1) = \frac{1}{|\mathscr{C}|}\left((1+(q-1)x)^n W_{\mathscr{C}}\left(\frac{1-x}{1+(q-1)x}\right)\right).$$

Demonstração: De fato, note primeiramente que P é um poset hierárquico com apenas um nível e colocando $z_1 = z_2 = 1$ as equações (2.11), (2.13) e (2.15) podem ser escritas como

$$f_0 = 0, \quad f_1 = \left(\frac{1+(q-1)x}{qx}\right)^n (1-x)^n \tag{2.16}$$

$$g_0 = (1+(q-1)x)^n, \quad g_1 = 0 \tag{2.17}$$

$$h_0 = h_1 = 1. \tag{2.18}$$

Logo, do Teorema 2.8 teremos

$$\begin{aligned}
&W_{\mathscr{C}^\perp}(x) = W_{\mathscr{C}^\perp,P^*}(x:1,1) = \\
&= 1 + \tfrac{1}{|\mathscr{C}|}\left(\left(\tfrac{qx}{1-x}\right)^n W_{\mathscr{C},P}(Q(x):f_0,f_1) + W_{\mathscr{C},P}(1:g_0,g_1) - W_{\mathscr{C},P}(1:h_0,h_1)\right) = \\
&= 1 + \tfrac{1}{|\mathscr{C}|}\left(\tfrac{qx}{1-x}\right)^n (A_{0,P}f_0 + (A_{1,P}Q(x) + \cdots + A_{n,P}Q(x)^n)f_1) + \tfrac{1}{|\mathscr{C}|}(A_{0,P}g_0 + (A_{1,P} + \cdots + A_{n,P})g_1) - \\
&- \tfrac{1}{|\mathscr{C}|}(A_{0,P}h_0 + (A_{1,P} + \cdots + A_{n,P})h_1)) = \\
&= 1 + \tfrac{1}{|\mathscr{C}|}\left(\tfrac{qx}{1-x}\right)^n ((A_{1,P}Q(x) + \cdots + A_{n,P}Q(x)^n)\left(\tfrac{1+(q-1)x}{qx}\right)^n (1-x)^n) + \tfrac{1}{|\mathscr{C}|}(A_{0,P}(1+(q-1)x)^n) - \\
&- \tfrac{1}{|\mathscr{C}|}(A_{0,P} + A_{1,P} + \cdots + A_{n,P}) = \\
&= 1 + \tfrac{1}{|\mathscr{C}|}(1+(q-1)x)^n (A_{0,P} + A_{1,P}Q(x) + \cdots + A_{n,P}Q(x)^n) - \tfrac{1}{|\mathscr{C}|}|\mathscr{C}| = \\
&= \tfrac{1}{|\mathscr{C}|}(1+(q-1)x)^n W_{\mathscr{C},P}(Q(x):1,1) = \tfrac{1}{|\mathscr{C}|}(1+(q-1)x)^n W_{\mathscr{C},P}\left(\tfrac{1-x}{1+(q-1)x}\right).
\end{aligned}$$

■

2.2.3 Relação entre Distribuições de Peso

Seja P um poset hierárquico com t-níveis e n elementos e $\mathscr{C}$ um P-código linear de comprimento n sobre $\mathbb{F}_q$. Assim como no caso clássico, também conseguimos relações entre as distribuições de P-pesos, $\{A_{i,P}\}_{i=0,\ldots,n}$ e as distribuições de P^*-pesos, $\{A'_{i,P^*}\}_{i=0,\ldots,n}$ de $\mathscr{C}$ e seu dual $\mathscr{C}^\perp$ respectivamente.

Analisemos o termo $\frac{1}{|\mathscr{C}|}\left(\frac{qx}{1-x}\right)^n W_{\mathscr{C},P}(Q(x):f_0,\ldots,f_t)$ no Teorema 2.8. Multipliquemos por $|\mathscr{C}|$ para simplificar e coloquemos $z_1=z_2=\cdots=z_{t+1}=1$ e $\gamma=q-1$. Utilizando (2.1) e (2.11), temos que

$$\begin{aligned}
&\left(\frac{qx}{1-x}\right)^n W_{\mathscr{C},P}(Q(x):f_0,\ldots,f_t)=\left(\frac{qx}{1-x}\right)^n\left[A_{0,P}f_0+\sum_{j=1}^{t}\left(\sum_{i=1}^{n_j}A_{n-\widehat{n_{j-1}}+i,P}Q(x)^{n-\widehat{n_{j-1}}+i}\right)f_j\right]=\\
&=\left(\frac{qx}{1-x}\right)^n\left[\sum_{j=1}^{t}\left(\sum_{i=1}^{n_j}A_{n-\widehat{n_{j-1}}+i,P}\left(\frac{1-x}{1+\gamma x}\right)^{n-\widehat{n_{j-1}}+i}\right)\left(\frac{1+\gamma x}{qx}\right)^{n-\widehat{n_j}}(1-x)^{\widehat{n_{j-1}}}\right]=\\
&=\left(\frac{qx}{1-x}\right)^n\sum_{j=1}^{t}\left(\sum_{i=1}^{n_j}A_{n-\widehat{n_{j-1}}+i,P}(1+\gamma x)^{n_j-i}(1-x)^{n+i}(qx)^{\widehat{n_j}-n}\right)=\\
&=\left(\frac{qx}{1-x}\right)^n\sum_{j=0}^{t-1}\left(\sum_{i=1}^{n_{j+1}}A_{n-\widehat{n_j}+i,P}(1+\gamma x)^{n_{j+1}-i}(1-x)^{n+i}(qx)^{\widehat{n_{j+1}}-n}\right)=\\
&=\sum_{j=0}^{t-1}\left(\sum_{i=1}^{n_{j+1}}A_{n-\widehat{n_j}+i,P}(1+\gamma x)^{n_{j+1}-i}(1-x)^{i}(qx)^{\widehat{n_{j+1}}}\right)=\\
&=\sum_{j=0}^{t-1}\frac{(qx)^{\widehat{n_{j+1}}}}{(1-x)^{n-\widehat{n_j}}}\left(\sum_{i=1}^{n_{j+1}}A_{n-\widehat{n_j}+i,P}(1+\gamma x)^{n_{j+1}-i}(1-x)^{n-\widehat{n_j}+i}\right).
\end{aligned}$$

Definamos $LW^{(i)}_{\mathscr{C},P}(x,y)$ como segue:

$$LW^{(i)}_{\mathscr{C},P}(x,y):=\sum_{j=1}^{n_i}A_{n-\widehat{n_{i-1}}+j,P}\,x^{n_i-j}\,y^{n-\widehat{n_{i-1}}+j} \tag{2.19}$$

Logo obtemos

$$\left(\frac{qx}{1-x}\right)^n W_{\mathscr{C},P}(Q(x):f_0,\ldots,f_t)=\sum_{i=0}^{t-1}\frac{(qx)^{\widehat{n_{i+1}}}}{(1-x)^{n-\widehat{n_i}}}LW^{(i+1)}_{\mathscr{C},P}(1+\gamma x,1-x). \tag{2.20}$$

Assim, conseguimos o seguinte teorema:

Teorema 2.11. *Seja P um poset hierárquico com t-níveis e n elementos. Se $\mathscr{C}$ é um P-código*

linear de comprimento n sobre $\mathbb{F}_q$ *então*

$$W_{\mathscr{C}^\perp,P^*}(x)=1+\frac{1}{|\mathscr{C}|}\sum_{i=0}^{t-1}\frac{(qx)^{\widehat{n_{i+1}}}}{(1-x)^{n-\widehat{n_i}}}LW_{\mathscr{C},P}^{(i+1)}(1+\gamma x,1-x)+\frac{1}{|\mathscr{C}|}\sum_{i=0}^{t-1}(qx)^{\widehat{n_{i+1}}}((1+\gamma x)^{n_{i+1}}|\mathscr{C}_i|-|\mathscr{C}_{i+1}|) \tag{2.21}$$

Demonstração: De fato, tomemos $z_1=\cdots=z_{t+1}=1$ no Teorema 2.8 e lembrando que $b_i(x)=(1+(q-1)x)^{n_{i+1}}(qx)^{\widehat{n_{i+1}}}$ segue de (2.20), (2.12) e (2.14) que

$$\begin{aligned}
&|\mathscr{C}|W_{\mathscr{C}^\perp,P^*}(x)=|\mathscr{C}|W_{\mathscr{C}^\perp,P^*}(x:1,\ldots,1)=\\
&=|\mathscr{C}|+\left(\left(\tfrac{qx}{1-x}\right)^n W_{\mathscr{C},P}(Q(x):f_0,\ldots,f_t)+W_{\mathscr{C},P}(1:g_0,\ldots,g_t)-W_{\mathscr{C},P}(1:h_0,\ldots,h_t)\right)=\\
&=|\mathscr{C}|+\sum_{i=0}^{t-1}\frac{(qx)^{\widehat{n_{i+1}}}}{(1-x)^{n-\widehat{n_i}}}LW_{\mathscr{C},P}^{(i+1)}(1+\gamma x,1-x)+\sum_{i=0}^{t-1}(qx)^{\widehat{n_{i+1}}}(1+\gamma x)^{n_{i+1}}|\mathscr{C}_i|-\sum_{i=0}^{t-1}(qx)^{\widehat{n_{i+1}}}|\mathscr{C}_{i+1}|=\\
&=|\mathscr{C}|+\sum_{i=0}^{t-1}\frac{(qx)^{\widehat{n_{i+1}}}}{(1-x)^{n-\widehat{n_i}}}LW_{\mathscr{C},P}^{(i+1)}(1+\gamma x,1-x)+\sum_{i=0}^{t-1}(qx)^{\widehat{n_{i+1}}}((1+\gamma x)^{n_{i+1}}|\mathscr{C}_i|-|\mathscr{C}_{i+1}|).
\end{aligned}$$

E temos o resultado desejado. ∎

Segue de (1.4) e (2.19) que

$$\begin{aligned}
&\frac{(qx)^{\widehat{n_{i+1}}}}{(1-x)^{n-\widehat{n_i}}}LW_{\mathscr{C},P}^{(i+1)}(1+\gamma x,1-x)=\frac{(qx)^{\widehat{n_{i+1}}}}{(1-x)^{n-\widehat{n_i}}}\left(\sum_{j=1}^{n_{i+1}}A_{n-\widehat{n_i}+j,P}(1+\gamma x)^{n_{i+1}+j}(1-x)^{n-\widehat{n_i}+j}\right)=\\
&=(qx)^{\widehat{n_{i+1}}}\left(\sum_{j=1}^{n_{i+1}}A_{n-\widehat{n_i}+j,P}(1+\gamma x)^{n_{i+1}+j}(1-x)^{j}\right)=(qx)^{\widehat{n_{i+1}}}\left(\sum_{j=1}^{n_{i+1}}A_{n-\widehat{n_i}+j,P}\sum_{k=0}^{n_{i+1}}P_k(j:n_{i+1})x^k\right)=\\
&=(qx)^{\widehat{n_{i+1}}}\sum_{k=0}^{n_{i+1}}\left(\sum_{j=1}^{n_{i+1}}A_{n-\widehat{n_i}+j,P}P_k(j:n_{i+1})x^k\right).
\end{aligned}$$

Denotemos $\sum_{j=1}^{n_{i+1}}A_{n-\widehat{n_i}+j,P}P_k(j:n_{i+1})$ por $a_k(j:n_{i+1})$, logo, como $P_0(j:n_{i+1})=1$, teremos

$$a_0(j:n_{i+1})=\sum_{j=1}^{n_{i+1}}A_{n-\widehat{n_i}+j,P}=|\mathscr{C}_{i+1}|-|\mathscr{C}_i| \tag{2.22}$$

Portanto substituindo no primeiro somatório do lado direito de (2.21), ficamos com

$$\sum_{i=0}^{t-1}\frac{(qx)^{\widehat{n_{i+1}}}}{(1-x)^{n-\widehat{n_i}}}LW_{\mathscr{C},P}^{(i+1)}(1+\gamma x,1-x)=\sum_{i=0}^{t-1}(qx)^{\widehat{n_{i+1}}}\left(\sum_{k=0}^{n_{i+1}}a_k(j:n_{i+1})x^k\right) \tag{2.23}$$

Temos também, da série binomial, que $(1+\gamma x)^{n_{i+1}} = \sum_{k=0}^{n_{i+1}} \binom{n_{i+1}}{k} \gamma^k x^k$. Logo o último somatório em (2.21) fica

$$\begin{aligned}
&\sum_{i=0}^{t-1} (qx)^{\widehat{n_{i+1}}}((1+\gamma x)^{n_{i+1}}|\mathscr{C}_i| - |\mathscr{C}_{i+1}| = \sum_{i=0}^{t-1} (qx)^{\widehat{n_{i+1}}} \left(\sum_{k=0}^{n_{i+1}} \binom{n_{i+1}}{k} \gamma^k x^k |\mathscr{C}_i| - |\mathscr{C}_{i+1}| \right) = \\
&= \sum_{i=0}^{t-1} (qx)^{\widehat{n_{i+1}}}(|\mathscr{C}_i| - |\mathscr{C}_{i+1}| + \sum_{k=1}^{n_{i+1}} \binom{n_{i+1}}{k} \gamma^k x^k |\mathscr{C}_i|)
\end{aligned} \tag{2.24}$$

Assim, de (2.22), (2.23) e (2.24) temos que o lado direto de (2.21) ficará

$$\begin{aligned}
&|\mathscr{C}| + \sum_{i=0}^{t-1} (qx)^{\widehat{n_{i+1}}} \left(\sum_{k=0}^{n_{i+1}} a_k(j:n_{i+1}) x^k \right) + \sum_{i=0}^{t-1} (qx)^{\widehat{n_{i+1}}}(|\mathscr{C}_i| - |\mathscr{C}_{i+1}| + \sum_{k=1}^{n_{i+1}} \binom{n_{i+1}}{k} \gamma^k x^k |\mathscr{C}_i|) = \\
&= |\mathscr{C}| + \sum_{i=0}^{t-1} (qx)^{\widehat{n_{i+1}}} \left(a_0(j:n_{i+1}) + \sum_{k=1}^{n_{i+1}} a_k(j:n_{i+1}) x^k + |\mathscr{C}_i| - |\mathscr{C}_{i+1}| + \sum_{k=1}^{n_{i+1}} \binom{n_{i+1}}{k} \gamma^k x^k |\mathscr{C}_i| \right) = \\
&= |\mathscr{C}| + \sum_{i=0}^{t-1} (qx)^{\widehat{n_{i+1}}} \sum_{k=1}^{n_{i+1}} (a_k(j:n_{i+1}) + \binom{n_{i+1}}{k} \gamma^k |\mathscr{C}_i|) x^k.
\end{aligned} \tag{2.25}$$

Por outro lado temos que o lado esquerdo de (2.21) pode ser escrito como

$$\begin{aligned}
&W_{\mathscr{C}^\perp, P^*}(x) = \sum_{u \in \mathscr{C}^\perp} x^{\omega_{P^*}(u)} = A'_{0,P^*} + A'_{\widehat{n_t}+1,P^*} x^{\widehat{n_t}+1} + \cdots + A'_{\widehat{n_t}+n_t,P^*} x^{\widehat{n_t}+n_t} + \\
&+ (A'_{\widehat{n_{t-1}}+1,P^*} x^{\widehat{n_{t-1}}+1} + \cdots + A'_{\widehat{n_{t-1}}+n_{t-1},P^*} x^{\widehat{n_{t-1}}+n_{t-1}}) + \cdots + A'_{\widehat{n_1}+1,P^*} x^{\widehat{n_1}+1} + \cdots + A'_{\widehat{n_1}+n_1,P^*} x^{\widehat{n_1}+n_1}) = \\
&= A'_{0,P^*} + \sum_{i=1}^{t} \left(A'_{\widehat{n_i}+1,P^*} x^{\widehat{n_i}+1} + \cdots + A'_{\widehat{n_i}+n_i,P^*} x^{\widehat{n_i}+n_i} \right) = \\
&1 + \sum_{i=1}^{t} \left(\sum_{k=1}^{n_i} (A'_{\widehat{n_i}+k,P^*} x^{\widehat{n_i}+k} \right) = 1 + \sum_{i=0}^{t-1} x^{\widehat{n_{i+1}}} \sum_{k=1}^{n_{i+1}} A'_{\widehat{n_{i+1}}+k,P^*} x^k.
\end{aligned} \tag{2.26}$$

Portanto conseguimos o seguinte teorema, que relaciona as distribuições de peso do P-código $\mathscr{C}$ com seu P^*- código dual $\mathscr{C}^\perp$.

Teorema 2.12. *Seja P um poset hierárquico com t-níveis e n elementos. Se $\mathscr{C}$ é um P-código linear de comprimento n sobre $\mathbb{F}_q$ então, para cada $0 \leq i \leq t-1$, $1 \leq k \leq n_{i+1}$*

$$A'_{\widehat{n_{i+1}}+k,P^*} = \frac{q^{\widehat{n_{i+1}}}}{|\mathscr{C}|} \sum_{j=1}^{n_{i+1}} P_k(j:n_{i+1}) A_{n-\widehat{n_i}+j,P} + \frac{q^{\widehat{n_{i+1}}}}{|\mathscr{C}|} \binom{n_{i+1}}{k} \gamma^k \sum_{j=0}^{n-\widehat{n_i}} A_{j,P}$$

.

Demonstração: De fato, segue de (2.26) e (2.25) que

$$1+\sum_{i=0}^{t-1} x^{\widehat{n_{i+1}}} \sum_{k=1}^{n_{i+1}} A'_{\widehat{n_{i+1}}+k,P^*} x^k = 1+\frac{1}{|\mathscr{C}|}\left(\sum_{i=0}^{t-1}(q\,x)^{\widehat{n_{i+1}}} \sum_{k=1}^{n_{i+1}}(a_k(j:n_{i+1})+\binom{n_{i+1}}{k}\gamma^k|\mathscr{C}_i|)x^k\right)$$

Logo da igualdade entre polinômios temos

$$\sum_{i=0}^{t-1} x^{\widehat{n_{i+1}}} A'_{\widehat{n_{i+1}}+k,P^*} = \frac{1}{|\mathscr{C}|}\left(\sum_{i=0}^{t-1}(q\,x)^{\widehat{n_{i+1}}}(a_k(j:n_{i+1})+\binom{n_{i+1}}{k}\gamma^k|\mathscr{C}_i|)\right)$$

Agora, lembrando que $|\mathscr{C}_i| = \sum_{j=0}^{n-\widehat{n_i}} A_{j,P}$ e $a_k(j:n_{i+1}) = \sum_{j=1}^{n_{i+1}} P_k(j:n_{i+1}) A_{n-\widehat{n_i}+j,P}$ e novamente da igualdade entre polinômios temos

$$A'_{\widehat{n_{i+1}}+k,P^*} = \frac{q^{\widehat{n_{i+1}}}}{|\mathscr{C}|}\sum_{j=1}^{n_{i+1}} P_k(j:n_{i+1}) A_{n-\widehat{n_i}+j,P} + \frac{q^{\widehat{n_{i+1}}}}{|\mathscr{C}|}\binom{n_{i+1}}{k}\gamma^k \sum_{j=0}^{n-\widehat{n_i}} A_{j,P}$$

■

Capítulo 3

Relações de Equivalência de tipo MacWilliams

Vimos no capítulo anterior que as identidades de MacWilliams são satisfeitas se, e somente se o poset é hierárquico. Neste capítulo veremos que se possuirmos mais informações sobre o código, podemos relacionar as distribuições de pesos através de relações de equivalências no conjunto dos ideais do poset.

3.1 Relações de equivalências em posets

Nesta seção definiremos algumas relações de equivalência em um poset, bem como alguns conceitos que utilizaremos ao longo do capítulo.

Seja P um poset em $[n]$ com relação de ordem $\preceq$ e P^* o poset dual. Denotemos por $I(P)$ ao conjunto de ideais de ordem de P.

Proposição 3.1. *Seja I um ideal de ordem em $I(P)$. Então o complemento I^c de I é um ideal de ordem de P^*.*

Demonstração: De fato, seja $x \in I^c$, logo, se $y \preceq x$ em P^* então $x \preceq y$ em P. Portanto $y \notin I$, caso contrário teríamos $x \in I$ o que é um absurdo. ■

Do mesmo modo, cada ideal J de P^* dá origem ao ideal J^c de $I((P^*)^*) = I(P)$. Logo temos uma correspondência biunívoca entre $I(P)$ e $I(P^*)$.

Denotaremos ainda por $\overline{I}$(respec. $\overline{I^c}$) a classe de equivalência de I (respec. I^c) com respeito a uma relação de equivalência E(respec. E^*) em $I(P)$(respec. $I(P^*)$). Lembremos ainda

da definição 1.13 que $M(I)$ denota o conjunto dos elementos maximais do ideal I e I_M denota o conjunto dos elementos não maximais de I.

Uma permutação σ de P é chamada um automorfismo se σ e σ^{-1} preservam relação de ordem de P, isto é, $x \preceq y \Leftrightarrow \sigma(x) \preceq \sigma(y)$ para todo $x, y \in P$. O conjunto Aut(P) dos automorfismos de P forma um grupo o qual é chamado de grupo de automorfismos de P.

Seja P um poset em $[n]$ e E uma relação de equivalência em $\mathcal{I}(P)$ definida pela propriedade (A), então conseguimos uma relação E' em $\mathcal{I}(P^*)$, também definida pela propriedade (A). Assim temos a definição de relação de equivalência dual.

Definição 3.1. *Seja P um poset em $[n]$ e E uma relação de equivalência em $\mathcal{I}(P)$. Dizemos que E' é a relação dual em $\mathcal{I}(P^*)$ de E, e denotamos por E^* se esta satisfaz a seguinte propriedade: $(I, J) \in E$ é definido pela propriedade (A) em $\mathcal{I}(P) \Leftrightarrow (I^c, J^c) \in E'$ é também definida pela propriedade (A) em $\mathcal{I}(P^*)$.*

Introduziremos agora três tipos de relações de equivalência no conjunto de ideais de um poset P.

Lema 3.2. *Seja P um poset em $[n]$ e $I, J \in \mathcal{I}(P)$.*

(i) *A relação E_C em $\mathcal{I}(P)$ é definida pela regra $(I, J) \in E_C \Leftrightarrow |I| = |J|$. Então E_C é uma relação de equivalência e a relação dual E_C^* em $\mathcal{I}(P^*)$ é naturalmente determinada por $|I^c| = |J^c|$.*

(ii) *Seja H um subgrupo de Aut(P). A relação E_H em $\mathcal{I}(P)$ é definida pela regra $(I, J) \in E_H \Leftrightarrow \sigma(I) = J$ para algum $\sigma \in H$. Então E_H é uma relação de equivalência e a relação dual E_H^* em $\mathcal{I}(P^*)$ é naturalmente determinada por $\sigma(I^c) = J^c$.*

(iii) *A relação E_S em $\mathcal{I}(P)$ é definida pela regra $(I, J) \in E_S \Leftrightarrow I \simeq J$, ou seja, I é isomorfo a J como um poset. Então E_S é uma relação de equivalência em $\mathcal{I}(P)$.*

Demonstração: Sejam $I, J, L \in \mathcal{I}(P)$.

(i) Mostremos que E_C é uma relação de equivalência:

reflexividade: claramente $|I| = |I|$, logo $I \in E_C$;

simetria: se $|I| = |J|$ então claramente $|J| = |I|$, logo $I, J \in E_C$;

transitividade: se $|I| = |J|$ e $|J| = |L|$ então $|I| = |L|$, logo $I, L \in E_C$.

Logo E_C é uma relação de equivalência em $\mathcal{I}(P)$ e além disso, temos que E_C^* é uma relação de equivalência em $\mathcal{I}(P^*)$:

reflexividade: como $|I| = |I|$ então $|I^c| = |I^c|$ logo $I^c \in E_C^*$;

simetria: como $|I| = |J|$ então $|I^c| = |J^c|$ donde segue que $|J^c| = |I^c|$, logo $I^c, J^c \in E_C^*$;

transitividade: como $|I| = |J|$ e $|J| = |L|$ então $|I^c| = |J^c|$ e $|J^c| = |L^c|$ logo $|I^c| = |L^c|$, assim $I^c, L^c \in E_C^*$.

(ii) Como H é um subgrupo de Aut(P), temos que o elemento neutro de Aut(P), que denotaremos por e, pertence a H, logo teremos

reflexividade: $e(I) = I$ logo $I \in E_H$;

simetria: como $\sigma \in H$ e H é um subgrupo temos que $\sigma^{-1} \in H$, logo se $(I, J) \in E_H$ existe $\sigma \in H$ tal que $\sigma(I) = J$, logo tomando σ^{-1} teremos $\sigma^{-1}(J) = I$ portanto $(J, I) \in E_H$;

transitividade: Sejam $(I, J) \in E_H$ e $(J, L) \in E_H$, logo existem σ_1 e σ_2 tais que $\sigma_1(I) = J$ e $\sigma_2(J) = L$, assim, do fato de H ser um subgrupo, temos que $\sigma_2\sigma_1 \in H$ logo teremos $\sigma_2\sigma_1(I) = \sigma_2(J) = L$, donde segue que $(I, L) \in E_H$.

Portanto E_H é uma relação de equivalência em P, além disso E_H^* é uma relação de equivalência em $I(P^*)$ e a prova é análoga à feita acima para mostrar que E_H é uma relação de equivalência.

(iii) Mostremos que E_S é uma relação de equivalência em P.

reflexividade: claramente temos $I \simeq I$ logo $I \in E_S$;

simetria: se $(I, J) \in E_S$ então $I \simeq J$ logo $J \simeq I$ donde segue que $(J, I) \in E_S$;

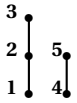
transitividade: sejam $(I, J) \in E_S$ e $(J, L) \in E_S$, logo $I \simeq J$ e $J \simeq L$ assim temos pela reflexividade $I \simeq J \simeq J \simeq L$ logo $I \simeq L$ donde segue que $(I, L) \in E_S$.

Portanto E_S é uma relação de equivalência em $I(P)$.

■

Vejamos agora um exemplo.

Exemplo 3.1. Seja P um poset em [5] com relação de ordem dada por: $1 \preceq 2 \preceq 3$ e $4 \preceq 5$, ou seja, com diagrama de Hasse dado por:



Temos que o conjunto dos ideais de P é dado por

$$\mathcal{I}(P) = \{\emptyset, \{1\}, \{4\}, \{1,2\}, \{1,4\}, \{4,5\}, \{1,2,3\}, \{1,2,4\}, \{1,4,5\}, \{1,2,3,4\}, \{1,2,4,5\}, P\}.$$

Assim, considerando a relação de equivalência E_C temos que

$$\mathcal{I}(P)/E_C = \{\overline{\emptyset}, \overline{\{1\}}, \overline{\{1,2\}}, \overline{\{1,2,3\}}, \overline{\{1,2,3,4\}}, \overline{P}\},$$

$$\mathcal{I}(P^*)/E_C^* = \{\overline{\emptyset^c}, \overline{\{1\}^c}, \overline{\{1,2\}^c}, \overline{\{1,2,3\}^c}, \overline{\{1,2,3,4\}^c}, \overline{P^c}\}.$$

Note que $\overline{\{1\}} = \{\{1\},\{4\}\}$, $\overline{\{1,2\}} = \{\{1,2\},\{1,4\},\{4,5\}\}$ e $\overline{\{1,2,3\}} = \{\{1,2,3\},\{1,2,4\},\{1,4,5\}\}$. Por outro lado, se considerarmos a relação de equivalência E_S teremos

$$\mathcal{I}(P)/E_S = \{\overline{\emptyset}, \overline{\{1\}}, \overline{\{1,2\}}, \overline{\{1,4\}}, \overline{\{1,2,3\}}, \overline{\{1,2,4\}}, \overline{\{1,2,3,4\}}, \overline{\{1,2,4,5\}\overline{P}}\},$$

onde $\overline{\{1\}} = \{\{1\},\{4\}\}$, $\overline{\{1,2\}} = \{\{1,2\},\{4,5\}\}$ e $\overline{\{1,2,4\}} = \{\{1,2,4\},\{1,4,5\}\}$. Além disso temos

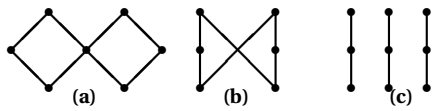
$$\mathcal{I}(P^*)/E_S' = \{\overline{\emptyset^c}, \overline{\{1\}^c}, \overline{\{1,2\}^c}, \overline{\{1,4\}^c}, \overline{\{1,2,3\}^c}, \overline{\{1,2,4\}^c}, \overline{\{1,2,3,4\}^c}, \overline{\{1,2,4,5\}^c}, \overline{P^c}\}.$$

Notamos porém que a relação dual E_S^* não existe em $\mathcal{I}(P^*)$ visto que a definição 3.1 não é satisfeita, pois $(\{1,2\},\{4,5\}) \in E_S$, ou seja, $\{1,2\} \simeq \{4,5\}$, mas $\{1,2\}^c = \{3,4,5\}$ e $\{4,5\}^c = \{1,2,3\}$ não são isomorfos como poset, ou seja, $(\{1,2\}^c, \{4,5\}^c) \notin E_S'$.

Motivados por esse exemplo, modificamos a relação E_S para dar a seguinte definição:

Definição 3.2. *Um poset P é um poset complemento de isomorfismo se satisfaz a seguinte condição: para qualquer I e J em $\mathcal{I}(P)$ temos que $I \simeq J \Leftrightarrow I^c \simeq J^c$.*

Exemplo 3.2. Alguns exemplos de posets que satisfazem a definição acima são dados pelos diagramas de Hasse abaixo.



Lema 3.3. *Sejam P um poset hierárquico em $[n]$ e $I, J \in I(P)$. Então existe $\sigma \in Aut(P)$ tal que $\sigma(I) = J$ se, e somente se, $|I| = |J|$.*

Demonstração: De fato, se existe $\sigma \in \mathrm{Aut}(P)$ tal que $\sigma(I) = J$ então claramente teremos $|I| = |J|$. Por outro lado, suponha que o poset P é hierárquico e sejam $(I, J) \in E_C$, ou seja, $|I| =$

$|J|$, consequentemente $|M(I)| = |M(J)|$. Temos ainda que se $x \preceq y$ então $\sigma(x) \preceq \sigma(y)$ para qualquer $\sigma \in \text{Aut}(P)$, logo sendo P um poset hieráquico, basta tomarmos $\sigma \in \text{Aut}(P)$ como sendo uma permutação nos elementos em $M(I)$ de forma que se consiga os elementos em $M(J)$ e mantendo os demais. Assim teremos $\sigma(I) = J$. Portanto $(I, J) \in Aut(P)$. ■

Com base nas definições de E_H, E_S e E_C apresentadas temos o seguinte resultado:

Proposição 3.4. *Seja $H = Aut(P)$. Então $E_{Aut(P)} \subseteq E_S \subseteq E_C$. Além disso, se o poset é hierárquico vale a igualdade.*

Demonstração: De fato, sejam $(I, J) \in E_{\text{Aut}(P)}$, logo $\sigma(I) = J$ para algum $\sigma \in \text{Aut(P)}$. Temos então, que se $x \preceq y$ em I, $\sigma(x) \preceq \sigma(y)$ em J, portanto $I \simeq J$, ou seja, $(I, J) \in E_S$, além disso, segue imediatamente que $(I, J) \in E_C$. Portanto $E_{\text{Aut}(P)} \subseteq E_S \subseteq E_C$. Por outro lado, se P é hierárquico, como $E_{\text{Aut}(P)} \subseteq E_S \subseteq E_C$ e pelo lema acima temos a igualdade $E_C = E_{\text{Aut}(P)}$ obtemos o resultado desejado. Um exemplo de que a igualdade não vale em geral pode ser vista no Exemplo 3.1. ■

Aqui também podemos definir esferas. Seja I um ideal de ordem do poset P em $[n]$. Definimos a I-esfera, denotada por $S_I(x)$ e a I^c-esfera, denotada por $S_{I^c}(x)$ de $\mathbb{F}_q^n$ centrada em $x \in \mathbb{F}_q^n$ como segue:

$$S_I(x) = \{y \in \mathbb{F}_q^n | \langle \text{supp}(x-y) \rangle_P = I\}$$

$$S_{I^c}(x) = \{y \in \mathbb{F}_q^n | \langle \text{supp}(x-y) \rangle_{P^*} = I^c\}.$$

Como temos relações de equivalência, também definimos a $\overline{I}$-esfera, $S_{\overline{I},E}(x)$ e a $\overline{I^c}$-esfera, $S_{\overline{I^c},E^*}(x)$, centrada em $x \in \mathbb{F}_q^n$, com respeito a E e E^*, respectivamente, como segue:

$$S_{\overline{I},E}(x) = \{y \in \mathbb{F}_q^n | (\langle \text{supp}(x-y) \rangle_P, I) \in E\}$$

$$S_{\overline{I^c},E^*}(x) = \{y \in \mathbb{F}_q^n | (\langle \text{supp}(x-y) \rangle_{P^*}, I^c) \in E^*\}.$$

Observação 3.1. Note que temos as seguintes igualdades:

(i) $S_{\overline{I},E}(x) = \bigcup_{J \in \overline{I}} S_J(x)$

(ii) $S_{\overline{I^c},E^*}(x) = \bigcup_{J^c \in \overline{I^c}} S_{J^c}(x)$

De fato, temos que

(i) Seja $y \in S_{\overline{I},E}(x)$, então $(\langle \text{supp}(x-y) \rangle_P, I) \in E$ logo $J = \langle \text{supp}(x-y) \rangle_P \in \overline{I}$ e assim $y \in S_J(x)$ para algum $J \in \overline{I}$. Portanto $S_{\overline{I},E}(x) \subseteq \bigcup_{J \in \overline{I}} S_J(x)$. Por outro lado, se $y \in \bigcup_{J \in \overline{I}} S_J(x)$ então $\exists J \in \overline{I}$

tal que $y \in S_J(x)$. Como $J \in \overline{I}$ então $(\langle \text{supp}(x-y)\rangle_P = J, I) \in E$ logo $y \in S_{\overline{I},E}(x)$. Portanto temos a igualdade $S_{\overline{I},E}(x) = \bigcup_{J\in\overline{I}} S_J(x)$.

(ii) Análogo ao item **(i)**.

Por simplicidade escreveremos S_I e S_{I^c} (respectivamente $S_{\overline{I},E}$ e $S_{\overline{I^c},E^*}$) quanto a esfera estiver centrada no vetor nulo.

Seja $\mathscr{C}$ um P-código em $\mathbb{F}_q^n$. Definimos

$$A_{\overline{I},E}(\mathscr{C}) := |S_{\overline{I},E} \cap \mathscr{C}|$$

e

$$W(\mathscr{C}, P, E) := \left[A_{\overline{I},E}(\mathscr{C})\right]_{\overline{I}\in I(P)/E} = \left[\begin{array}{ccc} A_{\overline{I_0},E}(\mathscr{C}) & \cdots & A_{\overline{I_n},E}(\mathscr{C}) \end{array}\right]_{1\times n} \text{ onde } I(P)/E = \{\overline{I_0},\ldots,\overline{I_n}\}.$$

Chamamos $W(\mathscr{C}, P, E)$ a distribuição de peso de $\mathscr{C}$ com respeito a E ou distribuição de E-peso de $\mathscr{C}$. Em particular, se o poset P é uma anticadeia em $[n]$ e a relação é dada por E_C, então $A_{\overline{I},E}(\mathscr{C})$ é o número de palavras do código com peso de Hamming igual a $|I|$ e a distribuição de E_C-peso é a distribuição de peso de Hamming de $\mathscr{C}$.

Definição 3.3. *Seja P um poset em $[n]$, E uma relação de equivalência em $I(P)$ que admite relação dual e E^* a relação dual em $I(P^*)$ de E. Uma relação de equivalência E em $I(P)$ é de tipo MacWilliams se, para quaisquer P-códigos $\mathscr{C}_1$ e $\mathscr{C}_2$ em $\mathbb{F}_q^n$, $W(\mathscr{C}_1, P, E) = W(\mathscr{C}_2, P, E)$ implica $W(\mathscr{C}_1^\perp, P^*, E^*) = W(\mathscr{C}_2^\perp, P^*, E^*)$, ou seja, a distribuição de E^*-peso do código dual $\mathscr{C}^\perp$, é unicamente determinada pela distribuição de E-peso do código $\mathscr{C}$ e vice-versa.*

3.1.1 Condições Equivalentes para uma Relação de Equivalência de tipo MacWilliams

Assim como no Capítulo 2, veremos nesta seção condições necessárias e suficientes para que uma relação de equivalência seja de tipo MacWilliams. Tais identidades segundo essa caracterização serão apresentadas na forma de matrizes, digamos P_E e Q_{E^*}. Além disso explicitaremos as entradas de tais matrizes no caso $E = E_H$ e provaremos que uma é unicamente determinada pela outra.

Lema 3.5. *Seja P um poset em $[n]$, E uma relação de equivalência em $I(P)$ e E^* a relação dual de E. Então para qualquer P-código linear $\mathscr{C}$ em $\mathbb{F}_q^n$,*

(i) $A_{\overline{I},E}(\mathscr{C}) = \dfrac{1}{|\mathscr{C}^{\perp}|}\sum_{u\in\mathscr{C}^{\perp}}\sum_{v\in S_{\overline{I},E}}\chi(u\cdot v) = \dfrac{1}{|\mathscr{C}^{\perp}|}\sum_{\overline{J^c}\in I(P^*)/E^*}\left(\sum_{u\in\mathscr{C}^{\perp}\cap S_{\overline{J^c},E^*}}\left(\sum_{v\in S_{\overline{I},E}}\chi(u\cdot v)\right)\right)$,

para $\overline{I}\in I(P)/E$

(ii) $A_{\overline{J^c},E^*}(\mathscr{C}^{\perp}) = \dfrac{1}{|\mathscr{C}|}\sum_{u\in\mathscr{C}}\sum_{v\in S_{\overline{J^c},E^*}}\chi(u\cdot v) = \dfrac{1}{|\mathscr{C}|}\sum_{\overline{I}\in I(P)/E}\left(\sum_{u\in\mathscr{C}\cap S_{\overline{I},E}}\left(\sum_{v\in S_{\overline{J^c},E^*}}\chi(u\cdot v)\right)\right)$,

para $\overline{J^c}\in I(P^*)/E^*$.

Demonstração: Sabemos pelo Lema 1.13 que $\sum_{v\in\mathscr{C}}\chi(v\cdot u) = \begin{cases} 0 & se \quad u\notin\mathscr{C}^{\perp} \\ |\mathscr{C}| & se \quad u\in\mathscr{C}^{\perp} \end{cases}$. Além disso, para um P-código linear $\mathscr{C}$ em $\mathbb{F}_q^n$ temos que $\mathscr{C} = \bigcup_{\overline{I}\in I(P)/E}\mathscr{C}\cap S_{\overline{I},E}$, onde a união é disjunta.

De fato, claramente vemos que $\bigcup_{\overline{I}\in I(P)/E}\mathscr{C}\cap S_{\overline{I},E}\subseteq\mathscr{C}$. Por outro lado, seja $x\in\mathscr{C}$ e tomemos $\langle\mathrm{supp}(x)\rangle_P = J$. Logo $x\in S_J$, com $\langle\mathrm{supp}(x)\rangle_P = J\in I(P)$. Assim existe $\overline{I}$ em $I(P)$ tal que $J\in\overline{I}$, portanto $(\langle\mathrm{supp}(x)\rangle_P, I)\in E$, ou seja, $x\in S_{\overline{I},E}$, donde segue que $x\in\bigcup_{\overline{I}\in I(P)/E}\mathscr{C}\cap S_{\overline{I},E}$. Logo temos a igualdade. Além disso, se $x\in(\mathscr{C}\cap S_{\overline{I},E})\cap(\mathscr{C}\cap S_{\overline{J},E})$ então $(\langle\mathrm{supp}(x)\rangle_P, I)\in E$ e $(\langle\mathrm{supp}(x)\rangle_P, J)\in E$ donde segue que $(I,J)\in E$, ou seja $\overline{I}=\overline{J}$, ou seja, a união é disjunta.

Analogamente temos que $\mathscr{C}^{\perp} = \bigcup_{\overline{J^c}\in I(P^*)/E^*}\mathscr{C}^{\perp}\cap S_{\overline{J^c},E^*}$. Logo teremos:

(i)

$$A_{\overline{I},E}(\mathscr{C}) = |S_{\overline{I},E}\cap\mathscr{C}| = \sum_{v\in\mathscr{C}\cap S_{\overline{I},E}}1 = \sum_{v\in S_{\overline{I},E}}\frac{1}{|\mathscr{C}^{\perp}|}\sum_{u\in\mathscr{C}^{\perp}}\chi(u\cdot v) =$$
$$= \frac{1}{|\mathscr{C}^{\perp}|}\sum_{u\in\mathscr{C}^{\perp}}\sum_{v\in S_{\overline{I},E}}\chi(u\cdot v) = \frac{1}{|\mathscr{C}^{\perp}|}\sum_{\overline{J^c}\in I(P^*)/E^*}\left(\sum_{u\in\mathscr{C}^{\perp}\cap S_{\overline{J^c},E^*}}\left(\sum_{v\in S_{\overline{I},E}}\chi(u\cdot v)\right)\right)$$

(ii)

$$A_{\overline{J^c},E^*}(\mathscr{C}^{\perp}) = |S_{\overline{J^c},E^*}\cap\mathscr{C}^{\perp}| = \sum_{v\in\mathscr{C}^{\perp}\cap S_{\overline{J^c},E^*}}1 = \sum_{v\in S_{\overline{J^c},E^*}}\frac{1}{|\mathscr{C}|}\sum_{u\in\mathscr{C}}\chi(u\cdot v) =$$
$$= \frac{1}{|\mathscr{C}|}\sum_{u\in\mathscr{C}}\sum_{v\in S_{\overline{J^c},E^*}}\chi(u\cdot v) = \frac{1}{|\mathscr{C}|}\sum_{\overline{I}\in I(P)/E}\left(\sum_{u\in\mathscr{C}\cap S_{\overline{I},E}}\left(\sum_{v\in S_{\overline{J^c},E^*}}\chi(u\cdot v)\right)\right)$$

■

Segue do lema acima o seguinte corolário.

Corolário 3.6. *Seja P um poset em $[n]$, E uma relação de equivalência em $I(P)$ e E^* a relação dual. Então para qualquer P-código linear $\mathscr{C}$ 1-dimensional sobre $\mathbb{F}_q^n$ gerado por um vetor não nulo $\boldsymbol{u}$ temos,*

(i) $$A_{\overline{I},E}(\mathscr{C}) = \begin{cases} 1 & se \quad I = \emptyset \\ q-1 & se \quad u \in S_{\overline{I},E}, para \ \overline{I} \in I(P)/E \\ 0 & caso\ contrário \end{cases}$$

(ii) $$A_{\overline{J^c},E^*}(\mathscr{C}^\perp) = \frac{1}{q}\left(|S_{\overline{J^c},E^*}| + (q-1)\sum_{v \in S_{\overline{J^c},E^*}} \chi(u\cdot v)\right) para\ \overline{J^c} \in I(P^*)/E^*$$

Demonstração:

(i) Temos que $\mathscr{C} = \{\alpha u \mid \alpha \in \mathbb{F}_q\}$. Assim, se $I = \emptyset$ então $S_{\overline{I},E} = \{0\}$, logo $|S_{\overline{I},E} \cap \mathscr{C}| = 1$. Se $u \in S_{\overline{I},E}$ então $\alpha u \in S_{\overline{I},E}$ para $\alpha \in \mathbb{F}_q^*$, logo $|S_{\overline{I},E} \cap \mathscr{C}| = |\mathscr{C}/\{0\}| = |\mathbb{F}_q^*| = q-1$. Por outro lado, se $u \notin S_{\overline{I},E}$ então $\alpha u \notin S_{\overline{I},E}$ logo $|S_{\overline{I},E} \cap \mathscr{C}| = |\emptyset| = 0$ e temos o resultado desejado.

(ii) Segue do Lema 3.5 que para $\overline{J^c} \in I(P^*)/E^*$,

$$A_{\overline{J^c},E^*}(\mathscr{C}^\perp) = \frac{1}{|\mathscr{C}|}\sum_{\overline{I} \in I(P)/E}\left(\sum_{w \in \mathscr{C} \cap S_{\overline{I},E}}\left(\sum_{v \in S_{\overline{J^c},E^*}} \chi(w\cdot v)\right)\right) = \frac{1}{|\mathscr{C}|}\sum_{w \in \mathscr{C}}\left(\sum_{v \in S_{\overline{J^c},E^*}} \chi(w\cdot v)\right) =$$
$$= \frac{1}{q}\sum_{\alpha \in \mathbb{F}_q}\left(\sum_{v \in S_{\overline{J^c},E^*}} \chi(\alpha u\cdot v)\right) = \frac{1}{q}\left(\sum_{v \in S_{\overline{J^c},E^*}} \chi(0\cdot v) + \sum_{\alpha \in \mathbb{F}_q^*}\left(\sum_{v \in S_{\overline{J^c},E^*}} \chi((\alpha u)\cdot v)\right)\right) =$$
$$= \frac{1}{q}\left(|S_{\overline{J^c},E^*}| + \sum_{\alpha \in \mathbb{F}_q^*}\sum_{v \in S_{\overline{J^c},E^*}} \chi(u\cdot(\alpha v))\right).$$

Como $S_{\overline{J^c},E^*} = \{\alpha v \mid v \in S_{\overline{J^c},E^*}\}$ para $\alpha \in \mathbb{F}_q^*$ temos,

$$A_{\overline{J^c},E^*}(\mathscr{C}^\perp) = \frac{1}{q}\left(|S_{\overline{J^c},E^*}| + (q-1)\sum_{v \in S_{\overline{J^c},E^*}} \chi(u\cdot v)\right).$$

■

Com isso os autores conseguem o teorema abaixo.

Teorema 3.7. *Seja P um poset em $[n]$, E uma relação de equivalência em $I(P)$ e E^* a relação dual em $I(P^*)$. São equivalentes:*

(i) *E é uma relação de equivalência de tipo MacWilliams em $I(P)$.*

(ii) *Para $\overline{I} \in I(P)/E$ e $\overline{J^c} \in I(P^*)/E^*$, temos:*

(a) *Se u e u' estão em $S_{\overline{I},E}$, então* $\sum_{v \in S_{\overline{J^c},E^*}} \chi(u \cdot v) = \sum_{v \in S_{\overline{J^c},E^*}} \chi(u' \cdot v)$;

(b) *Se v e v' estão em $S_{\overline{J^c},E^*}$,então* $\sum_{u \in S_{\overline{I},E}} \chi(u \cdot v) = \sum_{u \in S_{\overline{I},E}} \chi(u \cdot v')$;

(iii) *Existem matrizes Q_{E^*} e P_E sobre $\mathbb{F}_q$ tal que para qualquer P-código linear $\mathscr{C} \in \mathbb{F}_q^n$*

(a) $W(\mathscr{C}^\perp, P^*, E^*) = \frac{1}{|\mathscr{C}|} W(\mathscr{C}, P, E) P_E^T$;

(b) $W(\mathscr{C}, P, E) = \frac{1}{|\mathscr{C}^\perp|} W(\mathscr{C}^\perp, P^*, E^*) Q_{E^*}^T$;

onde P_E^T e $Q_{E^*}^T$ denotam a matriz transposta de P_E e Q_{E^*} respectivamente.

Demonstração:

(i) ⇒ (ii) Provemos por absurdo. Seja E uma relação de equivalência de tipo MacWilliams e suponha que não vale (a) ou (b) em (ii). Sem perda de generalidade, assuma que u e u' estão em $S_{\overline{I},E}$ e $\sum_{v \in S_{\overline{J^c},E^*}} \chi(u \cdot v) \neq \sum_{v \in S_{\overline{J^c},E^*}} \chi(u' \cdot v)$. Pelo Corolário 3.6 temos que se $\mathscr{C}_1$ e $\mathscr{C}_2$ são os P-códigos lineares 1-dimensional gerados por u e u' respectivamente, então $A_{\overline{I},E}(\mathscr{C}_1) = A_{\overline{I},E}(\mathscr{C}_2)$, logo $W(\mathscr{C}_1, P, E) = W(\mathscr{C}_2, P, E)$ porém, como $\sum_{v \in S_{\overline{J^c},E^*}} \chi(u \cdot v) \neq \sum_{v \in S_{\overline{J^c},E^*}} \chi(u' \cdot v)$ temos pelo Corolário 3.6 (ii) que, $A_{\overline{J^c},E^*}(\mathscr{C}_1^\perp) \neq A_{\overline{J^c},E^*}(\mathscr{C}_2^\perp)$. Portanto teremos $W(\mathscr{C}_1^\perp, P^*, E^*) \neq W(\mathscr{C}_2^\perp, P^*, E^*)$ o que é uma contradição pois assumimos que a relação é de tipo MacWilliams. Portanto (i) ⇒ (ii).

(ii) ⇒ (iii) Seja E uma relação de equivalência em $I(P)$ que admite (a), assim $\sum_{v \in S_{\overline{J^c},E^*}} \chi(u \cdot v)$ é uma constante para qualquer $u \in S_{\overline{I},E}$. Coloque $p_{\overline{J^c},\overline{I}} = \sum_{v \in S_{\overline{J^c},E^*}} \chi(u \cdot v)$ para $u \in S_{\overline{I},E}$. Segue do Lema 3.5 que

$$A_{\overline{J^c},E^*}(\mathscr{C}^\perp) = \frac{1}{|\mathscr{C}|} \sum_{\overline{I} \in I(P)/E} \left(\sum_{w \in \mathscr{C} \cap S_{\overline{I},E}} \left(\sum_{v \in S_{\overline{J^c},E^*}} \chi(w \cdot v) \right) \right) = \frac{1}{|\mathscr{C}|} \sum_{\overline{I} \in I(P)/E} \left(\sum_{w \in \mathscr{C} \cap S_{\overline{I},E}} p_{\overline{J^c},\overline{I}} \right) = \tag{3.1}$$
$$= \frac{1}{|\mathscr{C}|} \sum_{\overline{I} \in I(P)/E} A_{\overline{I},E}(\mathscr{C}) p_{\overline{J^c},\overline{I}}.$$

De forma análoga, como E admite (b) temos que $\sum_{u\in S_{\overline{I},E}} \chi(u\cdot v)$ é uma constante para $v\in S_{\overline{J^c},E^*}$ e colocando $q_{\overline{I},\overline{J^c}} = \sum_{u\in S_{\overline{I},E}} \chi(u\cdot v)$ para $v\in S_{\overline{J^c},E^*}$, segue do Lema 3.5 que

$$\begin{aligned} A_{\overline{I},E}(\mathscr{C}) &= \frac{1}{|\mathscr{C}^\perp|}\sum_{\overline{J^c}\in I(P^*)/E^*}\left(\sum_{w\in\mathscr{C}^\perp\cap S_{\overline{J^c},E^*}}\left(\sum_{v\in S_{\overline{I},E}}\chi(w\cdot v)\right)\right) = \\ &= \frac{1}{|\mathscr{C}^\perp|}\sum_{\overline{J^c}\in I(P^*)/E^*}\left(\sum_{w\in\mathscr{C}^\perp\cap S_{\overline{J^c},E^*}} q_{\overline{I},\overline{J^c}}\right) = \frac{1}{|\mathscr{C}^\perp|}\sum_{\overline{J^c}\in I(P^*)/E^*} A_{\overline{J^c},E^*}(\mathscr{C}^\perp)q_{\overline{I},\overline{J^c}}. \end{aligned} \tag{3.2}$$

Assim, defina as matrizes P_E e Q_{E^*} como segue: $P_E = [p_{\overline{J^c},\overline{I}}]$ e $Q_{E^*} = [q_{\overline{I},\overline{J^c}}]$. Aqui P_E é uma quadrada $|I(P^*)/E^*|\times|I(P)/E|$, visto que E^* é a relação dual de E, com linhas e colunas rotulados pelos elementos de $I(P^*)/E^*$ e $I(P)/E$ respectivamente e Q_{E^*} é uma $|I(P)/E|\times|I(P^*)/E^*|$ matriz com linhas e colunas rotulados pelos elementos de $I(P)/E$ e $I(P^*)/E^*$ respectivamente. Segue de (3.1) que

$$\begin{aligned} W(\mathscr{C}^\perp,P^*,E^*) &= [A_{\overline{J^c},E^*}]_{\overline{J^c}\in I(P^*)/E^*} = \frac{1}{|\mathscr{C}|}\left[\sum_{\overline{I}\in I(P)/E} A_{\overline{I},E}(\mathscr{C})p_{\overline{J^c},\overline{I}}\right]_{\overline{J^c}\in I(P^*)/E^*} = \\ &= \frac{1}{|\mathscr{C}|}W(\mathscr{C},P,E)P_E^T. \end{aligned} \tag{3.3}$$

Analogamente, por (3.2) temos que $W(\mathscr{C},P,E) = \frac{1}{|\mathscr{C}^\perp|}W(\mathscr{C}^\perp,P^*,E^*)Q_{E^*}^T$.

(iii) ⇒ (i) Suponha que uma relação de equivalência E admita (a) e (b) em (iii). Sejam $\mathscr{C}_1$ e $\mathscr{C}_2$ dois P-códigos lineares em $\mathbb{F}_q^n$ tais que $W(\mathscr{C}_1,P,E) = W(\mathscr{C}_2,P,E)$. Como a relação de equivalência E admite (a) em (iii) temos que

$$W(\mathscr{C}_1^\perp,P^*,E^*) = \frac{1}{|\mathscr{C}_1|}W(\mathscr{C}_1,P,E)P_E^T = \frac{1}{|\mathscr{C}_2|}W(\mathscr{C}_2,P,E)P_E^T = W(\mathscr{C}_2^\perp,P^*,E^*).$$

Analogamente, se $W(\mathscr{C}_1^\perp,P^*,E^*) = W(\mathscr{C}_2^\perp,P^*,E^*)$, como E admite (b) em (iii) temos que

$$W(\mathscr{C}_1,P,E) = \frac{1}{|\mathscr{C}_1^\perp|}W(\mathscr{C}_1^\perp,P^*,E^*)Q_{E^*}^T = \frac{1}{|\mathscr{C}_2^\perp|}W(\mathscr{C}_2^\perp,P^*,E^*)Q_{E^*}^T = W(\mathscr{C}_1,P,E).$$

Portanto a relação de equivalência E é uma relação de equivalência de tipo MacWilliams em $I(P)$.

■

Chamamos a matriz P_E de P-matriz com respeito a E e a matriz Q_{E^*} de Q-matriz com respeito a E^*. Vejamos alguns resultados sobre as entradas de tais matrizes.

Lema 3.8. *Seja P um poset em $[n]$. Para $I \in I(P)$, temos*

$$S_I = \left\{ (v_1, v_2, \ldots, v_n) \in \mathbb{F}_q^n | v_i \in \left\{ \begin{array}{lll} \mathbb{F}_q^* & se & i \in M(I), \\ \mathbb{F}_q & se & i \in I_M, \\ \{0\} & se & i \in I^c. \end{array} \right\} \right\}.$$

Demonstração: De fato, da definição de I-esfera temos que $S_I = \{v \in \mathbb{F}_q^n | \langle \text{supp}(v) \rangle_P = I\}$. Como $\langle \text{supp}(v) \rangle_P = I$ temos que $M(I) \subseteq \text{supp}(v)$, assim, se $i \in M(I)$ então $v_i \in \mathbb{F}_q^*$. Como $\text{supp}(v) \in I$, se $i \in I_M$ então $v_i \in \mathbb{F}_q$ e se $i \in I^c$ então $v_i = \{0\}$ pois caso contrário teríamos $\langle \text{supp}(v) \rangle_P \neq I$. ■

Lema 3.9. *Seja P um poset em $[n]$. Para $I, J \in I(P)$, são equivalente:*

(i) $\text{supp}(u) \cap (J^c)_M = \emptyset$ *para* $u \in S_I$.

(ii) $M(I) \cap (J^c)_M = \emptyset$.

(iii) $I \cap (J^c)_M = \emptyset$.

(iv) $I_M \cap J^c = \emptyset$.

Demonstração:

(i)⇒ (ii) Suponha que $\text{supp}(u) \cap (J^c)_M = \emptyset$ para $u \in S_I$, como $M(I) \subseteq \text{supp}(u)$ temos que $M(I) \cap (J^c)_M = \emptyset$.

(ii)⇒ (iii) Note que $I = I_M \cup M(I)$, logo $I \cap (J^c)_M = (I_M \cup M(I)) \cap (J^c)_M = (I_M \cap (J^c)_M) \cup (M(I) \cap (J^c)_M) = I_M \cap (J^c)_M$ pois estamos admitindo que vale (ii). Suponha que existe $x \in I_M \cap (J^c)_M$, logo temos que $\{z \in M(I) | x \preceq_P z \text{ em } P\} \neq \emptyset$ pois $x \in I_M$. Assim, se $x \in I_M \cap (J^c)_M$, como $(J^c)_M$ é um ideal de ordem em P^*, temos que existe $y \neq 0 \in M(I) \cap (J^c)_M$ para $y \in \{z \in M(I) | x \preceq_P z \text{ em } P\}$, o que é um absurdo pois $M(I) \cap (J^c)_M = \emptyset$. Logo $I_M \cap (J^c)_M = \emptyset$ e temos que $I \cap (J^c)_M = \emptyset$.

(iii)⇒(iv) Suponha que $x \in I_M \cap J^c$ e considere o conjunto $\{z \in M(I) | x \preceq_P z \text{ em } P\}$ que é diferente do vazio pois $x \in I_M$. Logo, como J^c é um ideal de ordem em P^* temos que

$z \in (J^c)_M$, assim existe $y \neq 0 \in I \cap (J^c)_M$ para $y \in \{z \in M(I) | x \preceq_P z \text{ em } P\}$. Absurdo pois estamos supondo que $I \cap (J^c)_M = \emptyset$. Logo $I_M \cap J^c = \emptyset$.

(iv)⇒(i) Suponha que $x \in \text{supp}(u) \cap (J^c)_M$, então temos $\{z \in M(J^c) | x \preceq_{P^*} z \text{ em } P^*\} \neq \emptyset$, logo existe $z \in M(J^c)$ tal que $z \in I_M \cap J^c$, absurdo pois estamos assumindo que $I_M \cap J^c = \emptyset$. Portanto $\text{supp}(u) \cap (J^c)_M = \emptyset$.

■

Calculemos agora a soma de caracteres de uma esfera de um ideal de ordem.

Lema 3.10. *Seja P um poset em $[n]$. Para $I, J \in I(P)$ e $u \in S_I$, temos*

$$\sum_{v \in S_{Jc}} \chi(u \cdot v) = \begin{cases} (-1)^{|I \cap J^c|}(q-1)^{|M(J^c)|-|I \cap J^c|} q^{|(J^c)_M|} & \text{se} \quad I_M \cap J^c = \emptyset \\ 0 & \text{se} \quad I_M \cap J^c \neq \emptyset \end{cases}$$

Demonstração: Das propriedades de caracteres temos que $\sum_{v \in S_{Jc}} \chi(u \cdot v) = \sum_{v \in S_{Jc}} \prod_{i=1}^{n} \chi(u_i \cdot v_i)$. Além disso, tomando $|M(J^c)| = n_1$, $|(J^c)_M| = n_2$ e $|J| = n_3$, então pelo Lema 3.8, a menos de permutar coordenadas, podemos escrever $S_{J^c} = (\mathbb{F}_q^*)^{n_1} \times (\mathbb{F}_q)^{n_2} \times \{0\}^{n_3}$ logo, segue deste fato e do Lema 1.11 que

$$\sum_{v \in S_{Jc}} \chi(u \cdot v) = \sum_{v \in S_{Jc}} \left(\prod_{i=1}^{n} \chi(u_i \cdot v_i) \right) = \sum_{(v_1, v_2, 0) \in S_{Jc}} \left(\prod_{i=1}^{n_1} \chi(u_i \cdot v_i^1) \prod_{i=n_1+1}^{n_1+n_2} \chi(u_i \cdot v_i^2) \right) =$$

$$= \sum_{v_1 \in (\mathbb{F}_q^*)^{n_1}} \left(\sum_{v_2 \in (\mathbb{F}_q)^{n_2}} \left(\prod_{i=1}^{n_1} \chi(u_i \cdot v_i^1) \prod_{i=n_1+1}^{n_1+n_2} \chi(u_i \cdot v_i^2) \right) \right) =$$

$$= \left(\sum_{v_1 \in (\mathbb{F}_q^*)^{n_1}} \left(\prod_{i=1}^{n_1} \chi(u_i \cdot v_i^1) \right) \right) \left(\sum_{v_2 \in (\mathbb{F}_q)^{n_2}} \left(\prod_{i=n_1+1}^{n_1+n_2} \chi(u_i \cdot v_i^2) \right) \right) =$$

$$= \prod_{i=1}^{n_1} \left(\sum_{\alpha \in \mathbb{F}_q^*} \chi(u_i \cdot \alpha) \right) \prod_{i=n_1+1}^{n_1+n_2} \left(\sum_{\alpha \in \mathbb{F}_q} \chi(u_i \cdot \alpha) \right) =$$

$$= \prod_{i \in M(J^c)} \left(\sum_{\alpha \in \mathbb{F}_q^*} \chi(u_i \cdot \alpha) \right) \prod_{i \in (J^c)_M} \left(\sum_{\alpha \in \mathbb{F}_q} \chi(u_i \cdot \alpha) \right) =$$

$$= \prod_{i \in \text{supp}(u) \cap M(J^c)} \left(\sum_{\alpha \in \mathbb{F}_q^*} \chi(u_i \cdot \alpha) \right) \prod_{i \in \text{supp}(u)^c \cap M(J^c)} \left(\sum_{\alpha \in \mathbb{F}_q^*} \chi(u_i \cdot \alpha) \right)$$

$$\prod_{i \in \text{supp}(u) \cap (J^c)_M} \left(\sum_{\alpha \in \mathbb{F}_q} \chi(u_i \cdot \alpha) \right) \prod_{i \in \text{supp}(u)^c \cap (J^c)_M} \left(\sum_{\alpha \in \mathbb{F}_q} \chi(u_i \cdot \alpha) \right).$$

Agora, se $I_M \cap J^c \neq \emptyset$ então $\text{supp}(u) \cap (J^c)_M \neq \emptyset$ logo, pelo Lema 1.12, o terceiro termo na expressão acima é nulo e temos $\sum_{v \in S_{Jc}} \chi(u \cdot v) = 0$. Por outro lado, se $I_M \cap J^c = \emptyset$ então pelo Lema 3.9 temos que $\text{supp}(u) \cap (J^c)_M = \emptyset$, assim podemos escrever os produtos como potências de (-1), q e $(q-1)$.

De fato, se $I_M \cap J^c = \emptyset$ então $\text{supp}(u) \cap (J^c)_M = \emptyset$, assim $(J^c)_M \subseteq \text{supp}(u)^c$, logo $|\text{supp}(u)^c \cap (J^c)_M| = |(J^c)_M|$ e como $\text{supp}(u) \subseteq I$ temos que $|\text{supp}(u) \cap J^c| = |I \cap J^c|$, além disso temos que $|\text{supp}(u)^c \cap M(J^c)| = |M(J^c)| - |\text{supp}(u) \cap M(J^c)| = |M(J^c)| - |I \cap J^c|$ assim substituindo as igualdades acima temos $\sum_{v \in S_{Jc}} \chi(u \cdot v) = (-1)^{|I \cap J^c|}(q-1)^{|M(J^c)|-|I \cap J^c|} q^{|(J^c)_M|}$. Portanto obtemos:

$$\sum_{v \in S_{Jc}} \chi(u \cdot v) = \begin{cases} (-1)^{|I \cap J^c|}(q-1)^{|M(J^c)|-|I \cap J^c|} q^{|(J^c)_M|} & \text{se} \quad I_M \cap J^c = \emptyset \\ 0 & \text{se} \quad I_M \cap J^c \neq \emptyset \end{cases}$$

■

Com base no lema anterior, podemos descrever explicitamente as entradas das matrizes P_E e Q_{E^*}.

Proposição 3.11. *Seja P um poset em $[n]$, E uma relação de equivalência em $I(P)$ e E^* a relação dual de E em $I(P^*)$, tal que se $(I,J) \in E$ então $|M(I)| = |M(J)|$ e se $(I^c, J^c) \in E^*$ então $|M(I^c)| = |M(J^c)|$. Então as entradas de P_E e Q_{E^*} são dadas como segue:*

(i) $p_{\overline{J^c},\overline{I}} = (q-1)^{|M(J^c)|} q^{|(J^c)_M|} \sum_{\substack{K^c \in \overline{J^c}, \\ I_M \cap K^c = \emptyset}} \left(\frac{-1}{q-1}\right)^{|I \cap K^c|}$ *para $u \in S_{\overline{I},E}$,*

(ii) $q_{\overline{I},\overline{J^c}} = (q-1)^{|M(I)|} q^{|I_M|} \sum_{\substack{K \in \overline{I}, \\ (J^c)_M \cap K = \emptyset}} \left(\frac{-1}{q-1}\right)^{|J^c \cap K|}$ *para $v \in S_{\overline{J^c},E^*}$.*

Demonstração:

(i) Da observação 3.1 (ii), temos que $S_{\overline{J^c},E^*} = \overset{\circ}{\bigcup_{K^c \in \overline{J^c}}} S_{K^c}$, assim, pelo Lema 3.10 temos, para $u \in S_{\overline{I},E}$ que

$$p_{\overline{J^c},\overline{I}} = \sum_{v \in S_{\overline{J^c},E^*}} \chi(u \cdot v) = \sum_{K^c \in \overline{J^c}} \left(\sum_{v \in S_{K^c}} \chi(u \cdot v) \right) = \sum_{\substack{K^c \in \overline{J^c}, \\ I_M \cap K^c = \emptyset}} (-1)^{|I \cap K^c|}(q-1)^{|M(K^c)|-|I \cap K^c|} q^{|(K^c)_M|}.$$

Note que de $|M(K^c)| = |M(J^c)|$, se $K^c \in \overline{J^c}$ então $|(K^c)_M| = |(J^c)_M|$, logo teremos

$$p_{\overline{J^c},\overline{I}} = (q-1)^{|M(J^c)|} q^{|(J^c)_M|} \sum_{\substack{K^c \in \overline{J^c}, \\ I_M \cap K^c = \emptyset}} \left(\frac{-1}{q-1}\right)^{|I \cap K^c|} \text{ para } u \in S_{\overline{I},E}$$

(ii) Analogamente, da observação 3.1 (i), temos que $S_{\overline{I},E} = \overset{\circ}{\bigcup_{K\in\overline{I}}} S_K$, e pelo Lema 3.10 temos, para $v \in S_{\overline{J^c},E^*}$ que

$$\sum_{u\in S_J} \chi(u\cdot v) = \begin{cases} (-1)^{|I^c\cap J|}(q-1)^{|M(J)|-|I^c\cap J|}q^{|J_M|} & se \quad (I^c)_M \cap J = \emptyset \\ 0 & se \quad (I^c)_M \cap J \neq \emptyset \end{cases}$$

Logo teremos, para $v \in S_{\overline{J^c},E^*}$ que

$$q_{\overline{I},\overline{J^c}} = \sum_{u\in S_{\overline{I},E}} \chi(u\cdot v) = \sum_{K\in\overline{I}} \left(\sum_{u\in S_k} \chi(u\cdot v) \right) = \sum_{\substack{k\in\overline{I} \\ (J^c)_M\cap K=\emptyset}} (-1)^{|J^c\cap K|}(q-1)^{|M(K)|-|J^c\cap K|}q^{|K_M|}.$$

Como $|M(K)| = |M(I)|$ se $K \in \overline{I}$ então $|K_M| = |I_M|$ e assim temos

$$q_{\overline{I},\overline{J^c}} = (q-1)^{|M(I)|}q^{|I_M|} \sum_{\substack{K\in\overline{I}, \\ (J^c)_M\cap K=\emptyset}} \left(\frac{-1}{q-1}\right)^{|J^c\cap K|} \text{ para } v \in S_{\overline{J^c},E^*}.$$

■

Assim conseguimos determinar explicitamente as entradas das matrizes P_E e Q_{E^*}.

3.2 Três relações de equivalência de tipo MacWilliams

Nesta seção veremos em que condições, ou seja, para quais posets as três relações de equivalência vistas na seção anterior são de tipo MacWilliams. Além disso relacionaremos as matrizes P_E e Q_{E^*} para tais casos.

Primeiramente, pela fórmula de inversão de Mobius temos que se f e g são funções nos subconjuntos de um conjunto finito X, então

$f(A) = \sum_{B\subseteq A} g(B)$ se e somente se, $g(A) = \sum_{B\subseteq A} (-1)^{|A|-|B|} f(B)$ para $A \subseteq X$.

A prova pode ser encontrada em [16] e no apêndice deste trabalho.

Assim, podemos agora enunciar e demonstrar o teorema apresentado por Choi et al. em [2], que classifica os posets admitindo as relações de equivalência de tipo MacWilliams.

Teorema 3.12. *Seja P um poset em $[n]$ e H um subgrupo de Aut(P).*

(i) *E_H é uma relação de equivalência de tipo MacWilliams em $I(P)$.*

(ii) *São equivalentes:*

(a) *P é um poset hierárquico.*

(b) *As duas relações de equivalência E_C e $E_{Aut(P)}$ são as mesmas.*

(c) *E_C é uma relação de equivalência de tipo MacWilliams em $I(P)$.*

(iii) *São equivalentes:*

(a) *P é um poset complemento de isomorfismo.*

(b) *E_S é uma relação de equivalência de tipo MacWilliams em $I(P)$.*

Demonstração:

(i) Note que $(I,J)\in E_H \Leftrightarrow (I^c,J^c)\in E_H^*$. Assim, para u e u' em $S_{\overline{I},E_H}$, sejam $I_1=\langle \mathrm{supp}(u)\rangle_P$ e $I_2=\langle \mathrm{supp}(u')\rangle_P$. Existe um automorfismo $\sigma\in H$ tal que $\sigma(I_1)=I_2$. Seja $J\in I(P)$, temos que $|M(I_1)|=|M(I_2)|$ logo, segue da Proposição 3.11 que

$$\sum_{v\in S_{\overline{J^c},E_H^*}}\chi(u'\cdot v)=(q-1)^{|M(J^c)|}q^{|(J^c)_M|}\sum_{\substack{K^c\in\overline{J^c},\\ (I_2)_M\cap K^c=\emptyset}}\left(\frac{-1}{q-1}\right)^{|I_2\cap K^c|}.$$

Temos que para $A,B\subseteq P$, $\sigma(A\cap B)=\sigma(A)\cap\sigma(B)$ para todo $\sigma\in\mathrm{Aut}(P)$.

De fato, se $A\cap B=\emptyset$ não temos o que mostrar. Suponha que $A\cap B\neq\emptyset$ e seja $x\in A\cap B$, logo, como $x\in A$ temos que $\sigma(x)\in\sigma(A)$ e como $x\in B$ temos que $\sigma(x)\in\sigma(B)$, logo $\sigma(x)\in\sigma(A)\cap\sigma(B)$ e portanto $\sigma(A\cap B)\subseteq\sigma(A)\cap\sigma(B)$.

Por outro lado, se $x\in\sigma(A)\cap\sigma(B)$, como $x\in\sigma(A)$ temos que $\sigma^{-1}(x)\in A$ e como $x\in\sigma(B)$ temos que $\sigma^{-1}(x)\in B$, logo $\sigma^{-1}(x)\in A\cap B$ e temos que $x\in\sigma(A\cap B)$. Portanto $\sigma(A)\cap\sigma(B)\subseteq\sigma(A\cap B)$.

Além disso, vemos claramente que $\mathrm{Aut}(P)=\mathrm{Aut}(P^*)$. Logo teremos

$$\sum_{v\in S_{\overline{J^c},E_H^*}}\chi(u'\cdot v)=(q-1)^{|M(J^c)|}q^{|(J^c)_M|}\sum_{\substack{\sigma(K^c)\in\overline{J^c},\\ (I_2)_M\cap\sigma(K^c)=\emptyset}}\left(\frac{-1}{q-1}\right)^{|I_2\cap\sigma(K^c)|}=$$

$$=(q-1)^{|M(J^c)|}q^{|(J^c)_M|}\sum_{\substack{\sigma(K^c)\in\overline{J^c},\\ \sigma((I_1)_M)\cap\sigma(K^c)=\emptyset}}\left(\frac{-1}{q-1}\right)^{|\sigma(I_1)\cap\sigma(K^c)|}=$$

$$=(q-1)^{|M(J^c)|}q^{|(J^c)_M|}\sum_{\substack{\sigma(K^c)\in\overline{J^c},\\ \sigma((I_1)_M\cap K^c)=\emptyset}}\left(\frac{-1}{q-1}\right)^{|\sigma(I_1\cap K^c)|}=$$

$$=(q-1)^{|M(J^c)|}q^{|(J^c)_M|}\sum_{\substack{K^c\in\overline{J^c},\\ (I_1)_M\cap K^c=\emptyset}}\left(\frac{-1}{q-1}\right)^{|I_1\cap K^c|}=\sum_{v\in S_{\overline{J^c},E_H^*}}\chi(u\cdot v).$$

De forma análoga, para v e v' em $S_{\overline{J^c},E_H^*}$ teremos $\sum_{u\in S_{\overline{I},E_H}}\chi(u\cdot v)=\sum_{u\in S_{\overline{I},E_H}}\chi(u\cdot v')$.

Portanto, pelo Teorema 3.7 (ii) temos que a relação E_H é uma relação de tipo MacWilliams.

(ii) **(a)** $\Rightarrow$ **(b)** Segue diretamente do Lema 3.3.

(b) $\Rightarrow$ **(c)** Se $E_C = E_{\mathrm{Aut}(P)}$ então pelo item (i), como E_H é de tipo MacWilliams, tomando $H = \mathrm{Aut}(P)$ teremos que $E_C = E_{\mathrm{Aut}(P)}$ é de tipo MacWilliams.

(c) $\Rightarrow$ **(a)** Pelo Teorema 2.9 temos que P admite identidades de MacWilliams se, e somente se, P é hierárquico. Assim, se E_C é uma relação de equivalência de tipo MacWilliams, como a cardinalidade dos ideais é a única levada em conta no caso clássico, temos que o poset P admite identidades de MacWilliams, e portanto o poset P é hierárquico.

(iii) **(a)** $\Rightarrow$ **(b)** Suponha que P é um poset complemento de isomorfismo. Para $u, u' \in S_{\overline{I},E_S}$, existe um isomorfismo de ordem f, satisfazendo $f(\langle \mathrm{supp}(u)\rangle_P) = \langle \mathrm{supp}(u')\rangle_P$. Sejam $I_1 = \langle \mathrm{supp}(u)\rangle_P$ e $I_2 = \langle \mathrm{supp}(u')\rangle_P$. Note que $|M(I_1)| = |M(I_2)|$, logo segue do Lema 3.9 e da Proposição 3.11 que, para $\overline{J^c} \in I(P^*)/E_S^*$ temos

$$\sum_{v \in S_{\overline{J^c},E_S^*}} \chi(u\cdot v) = (q-1)^{|M(J^c)|} q^{|(J^c)_M|} \sum_{\substack{K^c \in \overline{J^c},\\ (I_1)_M \cap K^c = \emptyset}} \left(\frac{-1}{q-1}\right)^{|I_1 \cap K^c|} =$$

$$= (q-1)^{|M(J^c)|} q^{|(J^c)_M|} \sum_{\substack{K^c \in \overline{J^c},\\ I_1 \cap K^c \subseteq M(I_1)}} \left(\frac{-1}{q-1}\right)^{|I_1 \cap K^c|}.$$

Substituindo $I_1 \cap K^c$ por A, teremos

$$\sum_{v \in S_{\overline{J^c},E_S^*}} \chi(u\cdot v) = (q-1)^{|M(J^c)|} q^{|(J^c)_M|} \sum_{A \subseteq M(I_1)} \left(\frac{-1}{q-1}\right)^{|A|} \sum_{\substack{k^c \in \overline{J^c}\\ I_1 \cap K^c = A}} 1.$$

Aplicando a fórmula de inversão de Mobius a $\sum_{\substack{k^c \in \overline{J^c}\\ I_1 \cap K^c = A}} 1$ teremos

$$\frac{1}{(q-1)^{|M(J^c)|} q^{|(J^c)_M|}} \sum_{v \in S_{\overline{J^c},E_S^*}} \chi(u\cdot v) = \sum_{A \subseteq M(I_1)} \left(\frac{-1}{q-1}\right)^{|A|} \sum_{B \subseteq A} (-1)^{|A\setminus B|} \sum_{\substack{k^c \in \overline{J^c}\\ I_1 \cap K^c \subseteq B}} 1.$$

Sejam $B \subseteq A \subseteq M(I_1)$, logo $|A| = |f(A)|$, $|A\setminus B| = |f(A)\setminus f(B)|$ e $(I_1\setminus B, I_2\setminus f(B)) \in E_S$, uma vez que $f : I_1 \to I_2$ é um isomorfismo de ordem.

Como P é um poset complemento de isomorfismo, $(I_1\setminus B)^c \simeq (I_2\setminus f(B))^c$. Logo teremos

$$\sum_{\substack{k^c \in \overline{J^c}\\ I_1 \cap K^c \subseteq B}} 1 = \sum_{\substack{k^c \in \overline{J^c}\\ K^c \subseteq (I_1\setminus B)^c}} 1 = \sum_{\substack{K^c \in \overline{J^c}\\ K^c \subseteq (I_2\setminus f(B))}} 1 = \sum_{\substack{k^c \in \overline{J^c}\\ I_2 \cap K^c \subseteq f(B)}} 1.$$

Portanto teremos

$$\frac{1}{(q-1)^{|M(J^c)|}q^{|(J^c)_M|}}\sum_{v\in S_{\overline{J^c},E_S^*}}\chi(u\cdot v)=\sum_{A\subseteq M(I_1)}\left(\frac{-1}{q-1}\right)^{|A|}\sum_{B\subseteq A}(-1)^{|A\setminus B|}\sum_{\substack{k^c\in\overline{J^c}\\ I_1\cap K^c\subseteq B}}1=$$

$$=\sum_{f(A)\subseteq M(I_2)}\left(\frac{-1}{q-1}\right)^{|f(A)|}\sum_{f(B)\subseteq f(A)}(-1)^{|f(A)\setminus f(B)|}\sum_{\substack{k^c\in\overline{J^c}\\ I_2\cap K^c\subseteq f(B)}}1=$$

$$=\frac{1}{(q-1)^{|M(J^c)|}q^{|(J^c)_M|}}\sum_{v\in S_{\overline{J^c},E_S^*}}\chi(u^{'}\cdot v).$$

De forma análoga conseguimos o resultado para v e $v^{'}$ em $S_{\overline{J^c},E_S^*}$. Lolo, pelo Teorema 3.7 (ii), temos que E_S é uma relação de equivalência de tipo MacWilliams.

(b) ⇒ (a) Provemos pela contrapositiva.

De fato, suponha que o poset P não é um complemento de isomorfismo, logo existem I_1 e I_2 em $I(P)$ tal que $I_1\simeq I_2$ e $(I_1)^c$ não é isomorfo com poset a $(I_2)^c$. Sejam $\mathscr{C}_1$ e $\mathscr{C}_2$ códigos lineares em $\mathbb{F}_q^n$ tal que $\mathscr{C}_i=\{x\in\mathbb{F}_q^n|\,\mathrm{supp}(x)\subseteq I_i\}, i=1,2$. Como $I_1\simeq I_2$ temos que $A_{\overline{I_1},E_S}(\mathscr{C}_1)=A_{\overline{I_2},E_S}(\mathscr{C}_2)$, logo $W(\mathscr{C}_1,P,E_S)=W(\mathscr{C}_2,P,E_S)$. Os códigos duais são dados por $\mathscr{C}_i^{\perp}=\{x\in\mathbb{F}_q^n|\,\mathrm{supp}(x)\subseteq(I_i)^c\}, i=1,2$. Segue do Lema 3.8 que $A_{\overline{(I_1)^c},E_S^*}(\mathscr{C}_1^{\perp})=(q-1)^{|M(I_1^c)|}q^{|(I_1^c)_M|}$. Note que como $I_1\simeq I_2$ temos $|I_1|=|I_2|$ e assim $|I_1^c|=|I_2^c|$.

Se $x\in\mathscr{C}_2^{\perp}$ é tal que $\langle\mathrm{supp}(x)\rangle_{P^*}\simeq I_1^c$, então $|\langle\mathrm{supp}(x)\rangle_{P^*}|=|I_1^c|=|I_2^c|$. Segue do fato de $\langle\mathrm{supp}(x)\rangle_{P^*}\subseteq I_2^c$ que $I_2=\langle\mathrm{supp}(x)\rangle_{P^*}\simeq I_1^c$, contradição. Logo $W(\mathscr{C}_1^{\perp},P^*,E_S^*)\neq W(\mathscr{C}_1^{\perp},P^*,E_S^*)$ e assim E_S não é uma relação de equivalência de tipo MacWilliams. Portanto, pela contrapositiva temos que se E_S é uma relação de equivalência de tipo MacWilliams então o poset P é um complemento de isomorfismo.

■

Vemos no teorema acima que a relação E_C é de tipo MacWilliams se, e somente se, o poset é hierárquico, mas que neste caso, a relação E_C é igual a relação $E_{\mathrm{Aut}(P)}$. Além disso, pelo item (iii) do teorema vemos que E_S é de tipo MacWilliams se, e somente se, o poset é um complemento de isomorfismo. Porém, conseguimos mostrar que neste caso, todo isomorfismo entre ideais pode ser estendido a um automorfismo do poset. Apresentaremos tal resultado na forma de teorema.

Teorema 3.13. *Seja P um poset complemento de isomorfismo, sejam I,J ideais de P e seja $f: I\to J$ um isomorfismo. Então existe um automorfismo $\tilde{f}$ de P tal que $\tilde{f}|_I=f$.*

Demonstração: Seja $f: I\to J$ um isomorfismo e x um elemento de $M(I^c)$ tal que $x\not> y$, para qualquer $y\in I$. Afirmamos que existe um elemento w em $M(J^c)$ tal que $w\not> z$ para qualquer $z\in J$.

De fato, como P é um complemento de isomorfismo, se $f : I \to J$ é um isomorfismo então existe um isomorfismo $g : I^c \to J^c$. Assim, suponha que não existe $w \in M(J^c)$ tal que $w \not\succ z$ para qualquer $z \in J$. Denotemos por $\tilde{g}$ a restrição de g a $I^c - \{x\}$, assim temos que $\tilde{g} : I^c - \{x\} \to J^c - \{g(x)\}$ é um isomorfismo, logo como P é um complemento de isomorfismo, existe um isomorfismo $\varphi : I \cup \{x\} \to J \cup \{g(x)\}$. Absurdo pois $x \in I \cup \{x\}$ é tal que $x \not\succ y$, para qualquer $y \in I$ mas em $J \cup \{g(x)\}$ temos por hipótese que $g(x)$ se relaciona com ao menos um elemento de J, logo, como $f : I \to J$ é um isomorfismos o número de elementos em I e J que não se relacionam devem ser o mesmo, mas em $I \cup \{x\}$ temos um elemento a mais que não se relaciona com nenhum outro do que em $J \cup \{g(x)\}$, portanto estes conjuntos não podem ser isomorfos.

Logo se existe x um elemento de $M(I^c)$ tal que $x \not\succ y$, para qualquer $y \in I$ temos que existe $w \in M(J^c)$ tal que $w \not\succ z$, para qualquer $z \in I$. Assim, basta tomarmos $\tilde{f} : I \cup \{x\} \to J \cup \{w\}$ com $\tilde{f}|_I = f$ e $f(x) = w$ e assim, $\tilde{f}$ é um isomorfismo e preserva ordem. Portanto podemos estender f para todos os elementos de I^c dessa forma.

Agora seja x um elemento de $M(I^c)$ tal que $\langle x \rangle_M \subseteq I$, onde $\langle x \rangle_M$ denota o conjunto dos elementos não maximais do ideal gerado por x com $\langle x \rangle_M \neq \emptyset$, e suponha que $|M(\langle x \rangle_M)| = k$. Denotemos $L = f(\langle x \rangle_M)$, então temos que existe $h : \langle x \rangle_M^c \to L^c$ o qual é um isomorfismo e assim $h : \langle x \rangle_M^c - \{x\} \to L^c - \{h(x)\}$ é também um isomorfismo, logo existe um isomorfismo $\tau : \langle x \rangle_M \cup \{x\} = \langle x \rangle \to L \cup \{h(x)\}$, visto que $\langle x \rangle_M \cup \{x\} = (\langle x \rangle_M^c - \{x\})^c$ e $L \cup \{h(x)\} = (L^c - \{h(x)\})^c$. Note que se existisse um elemento $z \in L^c$ tal que $h(x) \succ z$ então $L \cup \{h(x)\}$ não seria um ideal, assim temos que $M(\langle h(x) \rangle_M) \subseteq L$ e que se $z \in L^c$ então $h(x) \not\succ z$.

Como τ é um isomorfismo, $|M(L \cup \{h(x)\})| = 1$, mas temos que $h(x) \in M(L \cup \{h(x)\})$, pois caso contrário existiria um elemento $z \in L$ tal que $z \succ h(x)$ e teríamos que $h(x) \in L$ o que é uma contradição. Logo temos que $|M(\langle h(x) \rangle_M)| = k$. Assim definimos $\tilde{f} : I \cup \{x\} \to J \cup \{h(x)\}$ por $\tilde{f}|_I = f$ e $\tilde{f}(x) = h(x)$ o qual é um isomorfismo e preserva ordem, pois se $x \succ y$ então $h(x) \succ f(y)$ visto que $L = \langle h(x) \rangle_M$. Além disso, temos que $\tilde{f}^{-1} : J \cup \{h(x)\} \to I \cup \{x\}$ é dado por $\tilde{f}^{-1}|_J = f^{-1}$ e $\tilde{f}^{-1}(h(x)) = x$. Portanto podemos estender f a todos os elementos dessa forma em I^c.

Note que $|I^c| = r < \infty$ e o par (I, f) pode ser estendido para $(I_1 = I \cup \{x\}, \tilde{f}_1)$, continuando esse processo r vezes, conseguiremos $I_r = P$ e o automorfismo $\tilde{f}_r$ o qual é uma extensão de f para o poset todo, ou seja, neste caso temos $E_S = E_H$. ∎

Com base nos resultados obtidos, podemos então provar a proposição abaixo, apresentada em [2], que diz respeito à relação entre as entradas das matrizes P_E e Q_E^* para as três relações de equivalências vistas neste capítulo.

Proposição 3.14. *Seja P um poset em $[n]$, E uma das três relações de equivalência E_C, $E_{Aut(P)}$ ou E_S e E^* a relação dual de E. Se E é de tipo MacWilliams em $I(P)$ então*

$$\frac{|\overline{I}|}{(q-1)^{|M(J^c)|}q^{|(J^c)_M|}}p_{\overline{J^c},\overline{I}} = \frac{|\overline{J^c}|}{(q-1)^{|M(I)|}q^{|I_M|}}q_{\overline{I},\overline{J^c}} \quad \textit{para} \quad \overline{I} \in I(P)/E \textit{ e } \overline{J^c} \in I(P^*)/E^*.$$

Demonstração: De fato, do Teorema 3.12 temos que se E_C é de tipo MacWilliams então o poset é hierárquico e que neste caso $E_C = E_{\mathrm{Aut}(P)}$. Da mesma forma temos que se E_S é de tipo MacWilliams então o poset é um complemento de isomorfismo, e pelo Teorema 3.13 temos que neste caso $E_S = E_{\mathrm{Aut}(P)}$. Logo, como a hipótese da proposição é que a relação de equivalência é de tipo MacWilliams, basta mostramos a igualdade para o caso E_H, com $H \subseteq \mathrm{Aut}(P)$.

Seja H um subgrupo de $\mathrm{Aut}(P)$. Lembremos que se $A, B \subset P$ e $\sigma \in H$ então $\sigma(A \cap B) = \sigma(A) \cap \sigma(B)$, $|\sigma(A)| = |A|$ e $\sigma H = H$. Considere a relação de equivalência E_H, a qual é de tipo MacWilliams em $I(P)$. Temos que se $L \in \overline{I}$, então existe $\sigma \in H$ tal que $\sigma(I) = L$; da mesma forma, se $K^c \in \overline{J^c}$, então existe $\varphi \in H$ tal que $\varphi(J^c) = K^c$. Em outras palavras, $\overline{I}$ é a órbita de I sobre a ação de H. Lembramos que o estabilizador de I é o subgrupo $H_I = \{\sigma \in J | \sigma(I) = I\}$ (mais detalhes sobre subgrupos estabilizadores podem ser encontrados no apêndice).

Tomemos o conjunto $A = \{(L, K^c) | L \equiv I, K^c \equiv J^c, I_M \cap K^c = I \cap (K^c)_M = \emptyset\}$ e definamos a aplicação $\delta : I(P) \times I(P^*) \to \mathbb{R}$ dada por $\delta(L, K^c) = \begin{cases} 1 & \text{se} \quad (L, K^c) \in A \\ 0 & \text{caso contrário} \end{cases}$.

Denotemos $\left(\frac{1}{q-1}\right) = \alpha$, então temos:

$$\frac{|\overline{I}|}{(q-1)^{|M(J^c)|}q^{|(J^c)_M|}}p_{\overline{J^c},\overline{I}} = |\overline{I}| \sum_{K^c \in \overline{J^c}, I \cap (K^c)_M = \emptyset} \alpha^{|I \cap K^c|}$$

Segue do Teorema A.3 [Teorema da Órbita e Estabilizador] que $|\overline{I}| = \frac{|H|}{|H_I|}$, logo teremos

$$|\overline{I}| \sum_{K^c \in \overline{J^c}, I \cap (K^c)_M = \emptyset} \alpha^{|I \cap K^c|} = |\overline{I}| \frac{1}{|H_{J^c}|} \sum_{\varphi \in H} \alpha^{|I \cap \varphi(J^c)|} \delta(I, \varphi(J^c)) =$$

$$= \frac{|H|}{|H_I|} \frac{1}{|H_{J^c}|} \sum_{\varphi \in H} \alpha^{|I \cap \varphi(J^c)|} \delta(I, \varphi(J^c)) = \frac{1}{|H_I|} \frac{1}{|H_{J^c}|} \sum_{\sigma \in H} \sum_{\varphi \in H} \alpha^{|I \cap \varphi(J^c)|} \delta(I, \varphi(J^c)) =$$

$$= \frac{1}{|H_I|} \frac{1}{|H_{J^c}|} \sum_{\sigma \in H} \sum_{\varphi \in H} \alpha^{|I \cap \sigma^{-1}\varphi(J^c)|} \delta(I, \sigma^{-1}\varphi(J^c)) =$$

$$= \frac{1}{|H_I|} \frac{1}{|H_{J^c}|} \sum_{\sigma \in H} \sum_{\varphi \in H} \alpha^{|\sigma(I \cap \sigma^{-1}\varphi(J^c))|} \delta(I, \sigma^{-1}\varphi(J^c)) =$$

$$= \frac{1}{|H_I|} \frac{1}{|H_{J^c}|} \sum_{\sigma \in H} \sum_{\varphi \in H} \alpha^{|\sigma(I) \cap \sigma\sigma^{-1}\varphi(J^c)|} \delta(\sigma(I), \sigma\sigma^{-1}\varphi(J^c)) =$$

$$= \frac{1}{|H_I|}\frac{1}{|H_{J^c}|}\sum_{\sigma\in H}\sum_{\varphi\in H}\alpha^{|\sigma(I)\cap\varphi(J^c)|}\delta(\sigma(I),\varphi(J^c)) =$$

$$= \frac{1}{|H_I|}\frac{1}{|H_{J^c}|}\sum_{\sigma\in H}\sum_{\varphi\in H}\alpha^{|\varphi\varphi^{-1}\sigma(I)\cap\varphi(J^c)|}\delta(\varphi\varphi^{-1}\sigma(I),\varphi(J^c)) =$$

$$= \frac{1}{|H_I|}\frac{1}{|H_{J^c}|}\sum_{\varphi\in H}\sum_{\sigma\in H}\alpha^{|\varphi^{-1}\sigma(I)\cap J^c|}\delta(\varphi^{-1}\sigma(I),J^c) =$$

$$= \frac{1}{|H_I|}\frac{|H|}{|H_{J^c}|}\sum_{\sigma\in H}\alpha^{|\sigma(I)\cap J^c|}\delta(\sigma(I),J^c) = |\overline{J^c}|\sum_{L\in\overline{I},L\cap(J^c)_M=\emptyset}\alpha^{|L\cap J^c|} =$$

$$= \frac{|\overline{J^c}|}{(q-1)^{|M(I)|}q^{|I_M|}}q_{\overline{I},\overline{J^c}}.$$

Temos assim o resultado desejado. ■

Capítulo 4

Dualidades MacWilliams e a Métrica R-T

Em 1997 Rosenbloom e Tsfasman [12] introduziram na teoria de códigos uma métrica ρ em $\mathrm{Mat}_{n,s}(\mathbb{F}_q)$, o espaço das matrizes $n \times s$ com entradas em $\mathbb{F}_q$. Estes códigos tem sido estudados tanto do ponto de vista de combinatória quanto de aplicações em teoria de informação. É bem conhecido na literatura que a ρ-métrica é um tipo de métrica poset assim, neste capítulo, utilizamos os resultados obtidos no capítulo anterior para provar os resultados apresentados por Dougherty e Skriganov em [3] através da P-métrica. Para isso introduziremos os conceitos referentes à ρ-métrica e faremos a conexão entre esta e a P-métrica apresentada no Capítulo 3.

4.1 A Métrica ρ

Denotaremos por $\mathrm{Mat}_{n,s}(\mathbb{F}_q)$ o espaço linear de todas as matrizes $n \times s$ com entradas em $\mathbb{F}_q$, munido com as operações usuais de soma e produto por escalar de matrizes. Um código linear, assim como nos casos vistos até aqui, é um subespaço vetorial de $\mathrm{Mat}_{n,s}(\mathbb{F}_q)$.

Por definição, o peso de Hamming de uma matriz $\Omega \in \mathrm{Mat}_{n,s}(\mathbb{F}_q)$, indicado por $\kappa(\Omega)$, é igual ao número de entradas não nulas da matriz Ω. Nesse caso $\kappa(\Omega_1 - \Omega_2)$ define a métrica de Hamming em $\mathrm{Mat}_{n,s}(\mathbb{F}_q)$.

Introduzamos o seguinte peso não-Hamming, ρ em $\mathrm{Mat}_{n,s}(\mathbb{F}_q)$. Primeiramente, seja $n = 1$ e $v = (\xi_1, \xi_2, \ldots, \xi_s) \in \mathrm{Mat}_{1,s}(\mathbb{F}_q)$, então colocamos $\rho(0) = 0$ e $\rho(v) = \max\{i : \xi_i \neq 0\}$ para $v \neq 0$. Agora seja $\Omega = (v_1, \ldots, v_n)^T \in \mathrm{Mat}_{n,s}(\mathbb{F}_q)$, $v_j \in \mathrm{Mat}_{1,s}(\mathbb{F}_q)$, $1 \leq j \leq n$ e $(\cdot)^T$ denotando a matriz transposta. Colocamos $\rho(\Omega) = \sum_{j=1}^{n} \rho(v_j)$ e temos que ρ é uma métrica em $\mathrm{Mat}_{n,s}(\mathbb{F}_q)$.

Para um código linear $\mathscr{C} \subset \mathrm{Mat}_{n,s}(\mathbb{F}_q)$, chamamos de espectro de ρ-peso do código $\mathscr{C}$ o

conjunto de inteiros $w_r(\mathscr{C}) = |\{\Omega \in \mathscr{C} : \rho(\Omega) = r\}|$, $0 \leq r \leq ns$.

Definição 4.1. *Seja $\mathscr{C} \subset Mat_{n,s}(\mathbb{F}_q)$ um código linear, definimos o enumerador de ρ-peso de $\mathscr{C}$ por*

$$W(\mathscr{C}|z) = \sum_{r=0}^{ns} w_r(\mathscr{C}) z^r = \sum_{\Omega \in \mathscr{C}} z^{\rho(\Omega)}.$$

Introduzamos o seguinte produto interno em $\mathrm{Mat}_{n,s}(\mathbb{F}_q)$. Primeiramente, seja $n = 1$ e $v_1 = (\xi_1, \ldots, \xi_s)$, $v_2 = (\xi_1', \ldots, \xi_s') \in \mathrm{Mat}_{1,s}(\mathbb{F}_q)$. Coloque

$$\langle v_1, v_2 \rangle_D = \sum_{i=1}^{s} \xi_i \xi'_{s+1-i}. \tag{4.1}$$

Agora seja $\Omega_i = (v_i^{(1)}, \ldots, v_i^{(n)})^T \in \mathrm{Mat}_{n,s}(\mathbb{F}_q)$, $i = 1, 2$; $v_i^{(j)} \in \mathrm{Mat}_{1,s}(\mathbb{F}_q)$, $1 \leq j \leq n$, coloque

$$\langle \Omega_1, \Omega_2 \rangle_{DS} = \sum_{j=1}^{n} \langle v_1^{(j)}, v_2^{(j)} \rangle_D. \tag{4.2}$$

Para um código linear $\mathscr{C} \subset \mathrm{Mat}_{n,s}(\mathbb{F}_q)$ dado, definimos seu código dual $\mathscr{C}^\perp \subset \mathrm{Mat}_{n,s}(\mathbb{F}_q)$ por

$$\mathscr{C}^\perp = \{\Omega_2 \in \mathrm{Mat}_{n,s}(\mathbb{F}_q) : \langle \Omega_2, \Omega_1 \rangle_{DS} = 0 \ \ \forall \Omega_1 \in \mathscr{C}\}.$$

Vemos que $\mathscr{C}^\perp$ é também um código linear com $(\mathscr{C}^\perp)^\perp = \mathscr{C}$. Além disso, se d é a dimensão de $\mathscr{C}$ e $d^\perp$ é a dimensão de $\mathscr{C}^\perp$, então $d + d^\perp = ns$, $|\mathscr{C}||\mathscr{C}^\perp| = q^{ns}$, $|\mathscr{C}| = q^d$, $|\mathscr{C}^\perp| = q^{ns-d}$. Provaremos tais afirmações na próxima seção.

Como vimos nos capítulos anteriores, as identidades de MacWilliams trazem relações entre o polinômio enumerador dos códigos mutuamente duais $\mathscr{C}$ e $\mathscr{C}^\perp$. Para o caso $s = 1$ e n arbitrário temos que a métrica ρ coincide com a métrica de Hamming e assim os polinômios satisfazem a identidade de MacWilliams dada no Teorema 2.1. No caso oposto, onde temos $n = 1$ e s arbitrário, a seguinte identidade foi dada em [15]:

$$(qz-1)W(\mathscr{C}^\perp|z) + 1 - z = |\mathscr{C}^\perp| z^{s+1} (q(1-z)W(\mathscr{C}|\frac{1}{qz}) + qz - 1).$$

Assim, objetivo é estender as identidades de MacWilliams para o caso em que n e s são arbitrários. Porém podemos ver no exemplo a seguir que extensões diretas não existem para o enumerador de ρ-peso.

Exemplo 4.1. Considere dois códigos lineares $\mathscr{C}_1$ e $\mathscr{C}_2$ em $\mathrm{Mat}_{2,2}(\mathbb{F}_2)$

$$\mathscr{C}_1=\left\{\begin{pmatrix}0&0\\0&0\end{pmatrix},\begin{pmatrix}1&0\\1&0\end{pmatrix}\right\}\ ,\ \mathscr{C}_2=\left\{\begin{pmatrix}0&0\\0&0\end{pmatrix},\begin{pmatrix}0&0\\0&1\end{pmatrix}\right\}.$$

Assim $W(\mathscr{C}_1|z)=z^0+z^2=1+z^2=W(\mathscr{C}_2|z)$.

Os códigos duais $\mathscr{C}_1^\perp$ e $\mathscr{C}_2^\perp\subset\mathrm{Mat}_{2,2}(\mathbb{F}_2)$ são:

$$\mathscr{C}_1^\perp=\left\{\begin{pmatrix}0&0\\0&0\end{pmatrix},\begin{pmatrix}0&1\\0&1\end{pmatrix},\begin{pmatrix}1&1\\1&1\end{pmatrix},\begin{pmatrix}1&1\\0&1\end{pmatrix},\begin{pmatrix}0&1\\1&1\end{pmatrix},\begin{pmatrix}1&0\\0&0\end{pmatrix},\begin{pmatrix}0&0\\1&0\end{pmatrix},\begin{pmatrix}1&0\\1&0\end{pmatrix}\right\},$$

$$\mathscr{C}_2^\perp=\left\{\begin{pmatrix}0&0\\0&0\end{pmatrix},\begin{pmatrix}1&0\\0&0\end{pmatrix},\begin{pmatrix}0&1\\0&0\end{pmatrix},\begin{pmatrix}1&1\\0&0\end{pmatrix},\begin{pmatrix}1&0\\0&1\end{pmatrix},\begin{pmatrix}0&1\\0&1\end{pmatrix},\begin{pmatrix}1&1\\0&1\end{pmatrix},\begin{pmatrix}0&0\\0&1\end{pmatrix}\right\}.$$

Assim o enumerador de ρ-peso de $\mathscr{C}_1^\perp$ e $\mathscr{C}_2^\perp$ é respectivamente $W(\mathscr{C}_1^\perp|z)=1+2z+z^2+4z^4$ e $W(\mathscr{C}_2^\perp|z)=1+z+3z^2+z^3+2z^4$. Logo os polinômios não podem ser relacionados por uma relação de tipo MacWilliams.

Poderíamos pensar que o problema está no produto interno definido em (4.2), porém já para o caso $n=1$, utilizando o produto interno usual, vemos que os polinômios não podem ser relacionados por identidades de tipo MacWilliams.

Exemplo 4.2. Considere os códigos lineares $\mathscr{C}_1$, $\mathscr{C}_2\subset\mathrm{Mat}_{1,4}(\mathbb{F}_2)$ dados por

$$\mathscr{C}_1=\{(0000,1100,1001,0101)\},\ \ \mathscr{C}_2=\{0000,0100,0001,0101\}.$$

Seus códigos duais com relação ao produto interno definido em (4.1) são dados por

$$\mathscr{C}_1^\perp=\{0000,0100,1111,1011\},\ \ \mathscr{C}_2^\perp=\{0000,0100,0001,0101\}$$

e assim os 4 códigos possuem o mesmo enumerador de ρ-peso dado por

$$W(\mathscr{C}_i|z)=W(\mathscr{C}_i^\perp|z)=1+z^2+2z^4,\ \ i=1,2.$$

Com respeito ao produto interno usual, denotando os códigos duais por $\mathscr{C}_1^*$ e $\mathscr{C}_2^*$ temos

$$\mathscr{C}_1^*=\{0000,0010,1111,1101\},\ \ \mathscr{C}_2^*=\{0000,0010,1000,1010\}.$$

Os enumeradores de ρ-peso são dados por

$$W(\mathscr{C}_1^*|z)=1+z^3+2z^4,\ \ W(\mathscr{C}_2^*|z)=1+z+2z^3.$$

Portanto os enumeradores de ρ-peso $W(\mathscr{C}|z)$ e $W(\mathscr{C}^*|z)$ não podem ser relacionados por identidades de tipo MacWilliams.

O objetivo torna-se então procurar por definições de enumeradores de peso mais adequadas.

Consideremos bolas e esferas em $\mathrm{Mat}_{n,s}(\mathbb{F}_q)$ centradas na origem, com respeito a métrica ρ :

$$B^{(n,s)}(r) = \{\Omega \in \mathrm{Mat}_{n,s}(\mathbb{F}_q) : \rho(\Omega) \leq r\},$$
$$S^{(n,s)}(r) = \{\Omega \in \mathrm{Mat}_{n,s}(\mathbb{F}_q) : \rho(\Omega) = r\}, \text{ onde } 0 \leq r \leq ns \text{ é um inteiro.}$$

Tomemos $n = 1$, logo, pelas definições teremos que

$$B^{(1,s)}(r) = \{(\xi_1, \ldots, \xi_s) \in \mathrm{Mat}_{1,s}(\mathbb{F}_q) : \xi_i = 0 \text{ para } i > r\}$$

é um subespaço de dimensão r e $S^{(1,s)}(0) = B^{(1,s)}(0)$, $S^{(1,s)}(r) = B^{(1,s)}(r) - B^{(1,s)}(r-1)$, $r \geq 1$. Note ainda que $\mathrm{Mat}_{1,s}(\mathbb{F}_q)$ se divide em uma união disjunta de esferas: $\mathrm{Mat}_{1,s}(\mathbb{F}_q) = \bigcup_{r=0}^{s} S^{(1,s)}(r)$.

Para n arbitrário, denotamos por $Q_{n,s} \subset \mathbb{Z}^n$ o subconjunto de vetores inteiros

$$Q_{n,s} = \{(r_1, \ldots, r_n) : \ 0 \leq r_j \leq s, \ 1 \leq j \leq n\}.$$

Consideramos ainda o espaço $\mathrm{Mat}_{n,s}(\mathbb{F}_q)$ como um produto direto de n cópias de $\mathrm{Mat}_{1,s}(\mathbb{F}_q)$:

$$\mathrm{Mat}_{n,s}(\mathbb{F}_q) = \underbrace{\mathrm{Mat}_{1,s}(\mathbb{F}_q) \times \cdots \times \mathrm{Mat}_{1,s}(\mathbb{F}_q)}_{n}.$$

Introduzamos os subconjuntos $F_R \subset \mathrm{Mat}_{n,s}(\mathbb{F}_q)$, dados por

$$F_R = \prod_{j=1}^{n} S^{(1,s)}(r_j), \quad R = (r_1, \ldots, r_n) \in Q_{n,s}.$$

Os subconjuntos F_R são chamados fragmentos. Note que $\mathrm{Mat}_{n,s}(\mathbb{F}_q)$ se divide em uma união disjunta de fragmentos: $\mathrm{Mat}_{n,s}(\mathbb{F}_q) = \bigcup_{R \in Q_{n,s}} F_R$.

Seja S_n o grupo simétrico de todas as permutações de linhas da matriz $\Omega \in \mathrm{Mat}_{n,s}(\mathbb{F}_q)$, o qual preserva ρ-peso. Para um vetor inteiro $R = (r_1, \ldots, r_n) \in Q_{n,s}$, e uma permutação $\sigma \in S_n$, escrevemos $\sigma R = (r_{\sigma(1)}, \ldots, r_{\sigma(n)})$. O conjunto quociente $Q_{n,s}/S_n$ pode ser identificado com o

seguinte subconjunto de vetores inteiros:

$$Q_{n,s}/S_n = \{(r_1,\ldots,r_n):\ 0 \le r_1 \le r_2 \le \cdots \le r_n \le s\}.$$

De fato, note que tomando qualquer elemento R de $Q_{n,s}$, podemos fazer uma permutação nas coordenadas de R de tal forma que $\sigma R \in Q_{n,s}/S_n$.

Para um $R=(r_1,\ldots,r_n)\in Q_{n,s}/S_n$ introduzimos o subgrupo estabilizador $S_n^{(R)} \subset S_n$ por $S_n^{(R)} = \{\sigma \in S_n:\ \sigma R = R\}$.

Consideremos ainda a seguinte união disjunta de fragmentos

$$\Phi_R = \bigcup_{\sigma \in S_n/S_n^{(R)}} F_{\sigma R},\ \ R \in Q_{n,s}/S_n,$$

onde σ percorre um conjunto fixado de representantes para as classes laterais (à esquerda) de $S_n/S_n^{(R)}$.

Definição 4.2. *Seja $\mathscr{C} \subset Mat_{n,s}(\mathbb{F}_q)$ um código linear. Definimos os T-espectros e H-espectros como sendo, respectivamente os inteiros*

$t_R(\mathscr{C}) = |\mathscr{C} \cap F_R|,\ \ R \in Q_{n,s}$ *e*
$h_R(\mathscr{C}) = |\mathscr{C} \cap \Phi_R|,\ \ R \in Q_{n,s}/S_n,$

Note que da definição de Φ_R vista, teremos que

$$h_R(\mathscr{C}) = |\mathscr{C} \cap \Phi_R| = \sum_{\sigma \in S_n/S_n^{(R)}} t_R(\mathscr{C}) = \sum_{\sigma \in S_n} \alpha_R\, t_{\sigma R}(\mathscr{C}),\ \ R \in Q_{n,s}/S_n, \tag{4.3}$$

onde α_Ré o inverso do número de elementos do estabilizador de R.

Definição 4.3. *Seja $\mathscr{C} \subset Mat_{n,s}(\mathbb{F}_q)$. Definimos os T-enumeradores do código $\mathscr{C}$ como sendo*

$T(\mathscr{C}|Z_1,\ldots,Z_n) = \sum_{R \in Q_{n,s}} t_R(\mathscr{C}) \prod_{j=1}^{n} z_{r_j}^{(j)}$, *onde* $Z_j = (z_0^{(j)},\ldots,z_s^{(j)}) \in \mathbb{C}[z_{i,j}],\ 0 \le i \le s, 1 \le j \le n$, *com a notação* $z_{i,j} = z_i^{(j)}$.

Definição 4.4. *Seja $\mathscr{C} \subset Mat_{n,s}(\mathbb{F}_q)$. Definimos os H-enumeradores do código $\mathscr{C}$ por*

$H(\mathscr{C}|Z) = \sum_{R \in Q_{n,s}/S_n} h_R(\mathscr{C}) \prod z_{r_j}$, *onde* $Z \in \mathbb{C}[z_j],\ 0 \le j \le s$.

Comparando os dois enumeradores acima vemos que $H(\mathscr{C}|Z) = T(\mathscr{C}|Z,\ldots,Z)$.

Em [3], Dougherty e Skriganov introduzem a transformação linear $\Theta_s : \mathbb{C}[z_0,\ldots,z_s] \to \mathbb{C}[z_0,\ldots,z_s]$ colocando $Z' = \Theta_s Z$, onde

$$
\begin{aligned}
z_0^{'} &= z_0+(q-1)z_1+q(q-1)z_2+q^2(q-1)z_3+\cdots+q^{s-2}(q-1)z_{s-1}+q^{s-1}(q-1)z_s,\\
z_1^{'} &= z_0+(q-1)z_1+q(q-1)z_2+q^2(q-1)z_3+\cdots+q^{s-2}(q-1)z_{s-1}-q^{s-1}z_s,\\
&\vdots\\
z_{s-2}^{'} &= z_0+(q-1)z_1+q(q-1)z_2-q^2z_3,\\
z_{s-1}^{'} &= z_0+(q-1)z_1-qz_2,\\
z_s^{'} &= z_0-z_1.
\end{aligned}
$$

Ou seja, a matriz $\Theta_s=[\theta_{lk}]$, $0\leq l,k\leq s$ tem as seguintes entradas:

$$
\theta_{lk}=\begin{cases}
1 & se \quad k=0\\
q^{k-1}(q-1) & se \quad 0<k\leq s-l\\
-q^{k-1} & se \quad l+k=s+1\\
0 & se \quad l+k>s+1
\end{cases}
\tag{4.4}
$$

No artigo os autores obtém a matriz Θ_s utilizando transformada de Fourier e aplicando a fórmula da soma de Poisson entre outros resultados. Porém, como mostraremos na próxima seção, tal matriz pode ser obtida de forma mais direta aplicando-se os conceitos do capítulo anterior.

Com os conceitos apresentados nesta seção, Dougherty e Skriganov conseguem também, identidades de tipo MacWilliams para os T e H-enumeradores de códigos mutuamente duais, dadas pelos seguintes teoremas:

Teorema 4.1. *Os T-enumeradores dos códigos lineares mutuamente duais $\mathscr{C}$ e $\mathscr{C}^{\perp}\subset Mat_{n,s}(\mathbb{F}_q)$ são relacionados por*

$$T(\mathscr{C}|Z_1,\ldots,Z_n)=\frac{1}{|\mathscr{C}^{\perp}|}T(\mathscr{C}^{\perp}|\Theta_sZ_1,\ldots,\Theta_sZ_n).$$

Teorema 4.2. *Os H-enumeradores dos códigos lineares mutuamente duais $\mathscr{C}$ e $\mathscr{C}^{\perp}\subset Mat_{n,s}(\mathbb{F}_q)$ são relacionados por*

$$H(\mathscr{C}|Z)=\frac{1}{|\mathscr{C}^{\perp}|}H(\mathscr{C}^{\perp}|\Theta_sZ)$$

Provaremos tais resultados na próxima seção, utilizando os conceitos de posets vistos nos Capítulos 1 e 2 e os resultados obtidos no Capítulo 3. Por ora, vejamos um exemplo englobando os conceitos visto até o momento e as relações apresentadas nos teoremas acima.

Exemplo 4.3. Tomemos o código $\mathscr{C}_1$ dado no Exemplo 4.1, ou seja, tomemos $\mathscr{C} \subset \mathrm{Mat}_{2,2}(\mathbb{F}_2)$ dado por $\mathscr{C} = \left\{\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}\right\}$ e consideremos

$Q_{2,2} = \{R_0 = (0,0), R_1 = (1,0), R_2 = (2,0), R_3 = (0,1), R_4 = (0,2), R_5 = (1,1), R_6 = (1,2), R_7 = (2,1), R_8 = (2,2)\}$.

Assim, considerando o grupo simétrico das permutações S_2 teremos

$$Q_{2,2}/S_2 = \{R_0 = (0,0), R_3 = (0,1), R_4 = (0,2), R_5 = (1,1), R_6 = (1,2), R_8 = (2,2)\}.$$

Logo, pela definição de fragmentos teremos

$$F_{R_0} = \left\{\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\right\}, F_{R_1} = \left\{\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\right\}, F_{R_2} = \left\{\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\right\}, F_{R_3} = \left\{\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\right\},$$
$$F_{R_4} = \left\{\begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\right\}, F_{R_5} = \left\{\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}\right\}, F_{R_6} = \left\{\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right\},$$
$$F_{R_7} = \left\{\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right\}, F_{R_8} = \left\{\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}\right\}.$$

Temos ainda, pela definição 4.2 que $t_R(\mathscr{C}) = |\mathscr{C} \cap F_R|, \ \ R \in Q_{2,2}$, logo obtemos

$$t_{R_0}(\mathscr{C}) = t_{R_5}(\mathscr{C}) = 1 \ \text{ e} t_{R_1}(\mathscr{C}) = t_{R_2}(\mathscr{C}) = t_{R_3}(\mathscr{C}) = t_{R_4}(\mathscr{C}) = t_{R_6}(\mathscr{C}) = t_{R_7}(\mathscr{C}) = t_{R_8}(\mathscr{C}) = 0.$$

Ainda por (4.3) temos que $h_R(\mathscr{C}) = |\mathscr{C} \cap \Phi_R| = \sum_{\sigma \in S_2/S_2^{(R)}} t_{\sigma R}(\mathscr{C}), \ \ R \in Q_{2,2}/S_2$, logo obtemos

$$h_{R_0}(\mathscr{C}) = t_{R_0}(\mathscr{C}) = 1 \ , h_{R_3}(\mathscr{C}) = t_{R_3}(\mathscr{C}) + t_{R_1}(\mathscr{C}) = 0 \ , h_{R_4}(\mathscr{C}) = t_{R_4}(\mathscr{C}) + t_{R_2}(\mathscr{C}) = 0 \ ,$$

$$h_{R_5}(\mathscr{C}) = t_{R_5}(\mathscr{C}) = 1 \ , h_{R_6}(\mathscr{C}) = t_{R_6}(\mathscr{C}) + t_{R_7}(\mathscr{C}) = 0 \ , h_{R_8}(\mathscr{C}) = t_{R_8}(\mathscr{C}) = 0.$$

Portanto pela definição 4.3 teremos

$$T(\mathscr{C}|Z_1, Z_2) = \sum_{R \in Q_{2,2}} t_R(\mathscr{C}) \prod_{j=1}^{2} z_{r_j}^{(j)} = t_{R_0} \prod_{j=1}^{2} z_{r_j}^{(j)} + t_{R_5} \prod_{j=1}^{2} z_{r_j}^{(j)} = z_0^{(1)} z_0^{(2)} + z_1^{(1)} z_1^{(2)}.$$

Pela definição 4.4 teremos

$$H(\mathscr{C}|Z) = \sum_{R \in Q_{2,2}/S_2} h_R(\mathscr{C}) \prod_{j=1}^{2} z_{r_j} = h_{R_0}(\mathscr{C}) \prod_{j=1}^{2} z_{r_j} + h_{R_5} \prod_{j=1}^{2} z_{r_j} = z_0 z_0 + z_1 z_1,$$

e vemos que $H(\mathscr{C}|Z) = T(\mathscr{C}|Z,Z)$.

Por (4.4), como q=2, teremos $\Theta_2 = \begin{pmatrix} 1 & 1 & 2 \\ 1 & 1 & -2 \\ 1 & -1 & 0 \end{pmatrix}$.

Pela métrica ρ temos que o código dual $\mathscr{C}^\perp$ é dado por

$$\mathscr{C}^\perp = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \right\}.$$

Logo teremos

$$t_{R_0}(\mathscr{C}^\perp) = t_{R_1}(\mathscr{C}^\perp) = t_{R_3}(\mathscr{C}^\perp) = t_{R_5}(\mathscr{C}^\perp) = 1,$$
$$t_{R_2}(\mathscr{C}^\perp) = t_{R_4}(\mathscr{C}^\perp) = t_{R_6}(\mathscr{C}^\perp) = t_{R_7}(\mathscr{C}^\perp) = 0 \text{ e } t_{R_8}(\mathscr{C}^\perp) = 4.$$

Além disso temos

$$h_{R_0}(\mathscr{C}^\perp) = t_{R_0}(\mathscr{C}^\perp) = 1 \ , h_{R_3}(\mathscr{C}^\perp) = t_{R_3}(\mathscr{C}^\perp) + t_{R_1}(\mathscr{C}^\perp) = 2 \ , h_{R_4}(\mathscr{C}^\perp) = t_{R_4}(\mathscr{C}^\perp) + t_{R_2}(\mathscr{C}^\perp) = 0 \ ,$$
$$h_{R_5}(\mathscr{C}^\perp) = t_{R_5}(\mathscr{C}^\perp) = 1 \ , h_{R_6}(\mathscr{C}^\perp) = t_{R_6}(\mathscr{C}^\perp) + t_{R_7}(\mathscr{C}^\perp) = 0 \ , h_{R_8}(\mathscr{C}^\perp) = t_{R_8}(\mathscr{C}^\perp) = 4.$$

Assim, aplicando tais resultados na Definição 4.3, de T-enumerador obtemos

$$\begin{aligned} T(\mathscr{C}^\perp|Z_1,Z_2) &= \sum_{R\in Q_{2,2}} t_R(\mathscr{C}^\perp) \prod_{j=1}^{2} z_{r_j}^{(j)} = \\ &= t_{R_0}(\mathscr{C}^\perp) \prod_{j=1}^{2} z_{r_j}^{(j)} + t_{R_1}(\mathscr{C}^\perp) \prod_{j=1}^{2} z_{r_j}^{(j)} + t_{R_3}(\mathscr{C}^\perp) \prod_{j=1}^{2} z_{r_j}^{(j)} + t_{R_5}(\mathscr{C}^\perp) \prod_{j=1}^{2} z_{r_j}^{(j)} + t_{R_8}(\mathscr{C}^\perp) \prod_{j=1}^{2} z_{r_j}^{(j)} = \\ &= z_0^{(1)} z_0^{(2)} + z_1^{(1)} z_0^{(2)} + z_0^{(1)} z_1^{(2)} + z_1^{(1)} z_1^{(2)} + 4 z_2^{(1)} z_2^{(2)}. \end{aligned}$$

Da mesma forma, aplicando os resultados na Definição 4.4, de H-enumerador obtemos

$$\begin{aligned} H(\mathscr{C}^\perp|Z) &= \sum_{R\in Q_{2,2}/S_2} h_R(\mathscr{C}^\perp) \prod_{j=1}^{2} z_{r_j} = \\ &= h_{R_0}(\mathscr{C}^\perp) \prod_{j=1}^{2} z_{r_j} + h_{R_3}(\mathscr{C}^\perp) \prod_{j=1}^{2} z_{r_j} + h_{R_5}(\mathscr{C}^\perp) \prod_{j=1}^{2} z_{r_j} + h_{R_8}(\mathscr{C}^\perp) \prod_{j=1}^{2} z_{r_j} = \\ &= z_0 z_0 + 2 z_0 z_1 + z_1 z_1 + 4 z_2 z_2. \end{aligned}$$

Assim, tomando Θ_2 encontrada acima, e considerando $Z_j^{'} = \Theta_2 Z_j$ teremos

$$Z_j^{'} = \Theta_2 Z_j = \begin{bmatrix} 1 & 1 & 2 \\ 1 & 1 & -2 \\ 1 & -1 & 0 \end{bmatrix} \begin{bmatrix} z_0^{(j)} \\ z_1^{(j)} \\ z_2^{(j)} \end{bmatrix} = \begin{bmatrix} z_0^{(j)} + z_1^{(j)} + 2 z_2^{(j)} \\ z_0^{(j)} + z_1^{(j)} - 2 z_2^{(j)} \\ z_0^{(j)} - z_1^{(j)} \end{bmatrix} = \begin{bmatrix} z_0^{'(j)} \\ z_1^{'(j)} \\ z_2^{'(j)} \end{bmatrix}.$$

Logo, substituindo em $T(\mathscr{C}^{\perp}|Z_1', Z_2')$ e fazendo cálculos básicos encontramos $T(\mathscr{C}^{\perp}|Z_1', Z_2') = 8z_0^{(1)}z_0^{(2)} + 8z_1^{(1)}z_1^{(2)}$ e assim temos que $T(\mathscr{C}|Z_1, Z_2) = \frac{1}{|\mathscr{C}^{\perp}|}T(\mathscr{C}^{\perp}|Z_1', Z_2') = \frac{1}{|\mathscr{C}^{\perp}|}T(\mathscr{C}^{\perp}|\Theta_2 Z_1, \Theta_2 Z_2)$.

4.2 Identidades de MacWilliams para T e H-enumeradores

Nesta seção provaremos os resultados apresentados no final da seção anterior. Para isso, utilizaremos os resultados obtidos nos demais capítulos. Assim, primeiramente precisamos fazer a ligação entre a métrica ρ e a P-métrica vista no Capítulo 1 e utilizada no Capítulo 3, bem como a relação entre os conceitos apresentados para ambas as métricas.

Considere o poset P em $[ns]$, união disjunta de n cadeias de comprimento s, com relação de ordem dada por $i \preceq n+i \preceq 2n+i \preceq \cdots \preceq (s-1)n+i, \ \ 1 \leq i \leq n$.

Definição 4.5. *Seja $\Omega \in Mat_{n,s}(\mathbb{F}_q)$, com $\Omega = [a_{i,j}]$. Definamos as seguintes transformações lineares:*

$$T : Mat_{n,s}(\mathbb{F}_q) \to \mathbb{F}_q^{ns} \ \ \textit{dada por} \ \ T(\Omega) = T([a_{i,j}]) = [v_{(j-1)n+i}], \ \ \textit{onde} \ \ v_{(j-1)n+i} = a_{i,j} \ \ e$$

$$D : Mat_{n,s}(\mathbb{F}_q) \to Mat_{n,s}(\mathbb{F}_q) \ \ \textit{dada por} \ \ D([a_{i,j}]) = [a_{i,s-j+1}]_{n,s}.$$

Note que pelas definições apresentadas temos que $\rho(\Omega) = \omega_P(T(\Omega))$.

Agora, denotemos $R \in Q_{n,s}$ por $((1,r_1),\ldots,(n,r_n))$, ou seja $R = ((j,r_j), 1 \leq j \leq n)$. Note que um ideal $I \in I(P)$ é inteiramente determinado pelos seu elementos maximais, assim denotemos $M(I) = \{m_1,\ldots,m_k\}$. Pelo algoritmo da divisão de Euclides, podemos escrever cada elemento maximal na forma $m_l = x_l n + t_l, \ \ n > t_l \geq 0$. Analogamente para $J^c \in I(P^*)$.

Conseguimos assim uma aplicação $\varphi : Q_{n,s} \to I(P)$ dada por

$$\varphi(R) = \varphi((j,r_j)) = \langle (r_j - 1)n + j ; r_j \neq 0 \rangle_P.$$

Da mesma forma, notando que se $I \in I(P)$, temos $I = \langle a = x_a n + t_a ; \ \ n > t_a \geq 0, \ \ a \in M(I) \rangle_P$, podemos definir uma aplicação $\varphi' : I(P) \to Q_{n,s}$ dada por $\varphi'(I) = ((j,r_j)), \ $, onde

$$\begin{cases} (j,r_j) = (n, x_a) & se \quad t_a = 0 \\ (j,r_j) = (t_a, x_a + 1) & se \quad t_a \neq 0 \\ (j,0) & \text{para as demais posições} \end{cases}$$

Analogamente podemos definir uma aplicação $\psi : Q_{n,s} \to I(P^*)$ dada por

$$\psi(R) = \psi((j,r_j)) = \langle (s - r_j)n + j ; r_j \neq 0 \rangle_{P^*}.$$

Notando que se $J^c \in I(P^*)$, temos $J^c = \langle b = x_b n + t_b;\ \ n > t_b \geq 0,\ \ b \in M(J^c)\rangle_{P^*}$, conseguimos uma aplicação $\psi' : I(P^*) \to Q_{n,s}:$ definida por $\psi'(J^c) = ((j, r_j))$, onde

$$\begin{cases} (j, r_j) = (n, s - x_b + 1) & se \quad t_b = 0 \\ (j, r_j) = (t_b, s - x_b) & se \quad t_b \neq 0 \\ (j, 0) & \text{para as demais posições} \end{cases}$$

Assim vemos que para cada $R \in Q_{n,s}$ podemos associar um ideal $I \in I(P)$ e um ideal $J^c \in I(P^*)$. Logo, seja $\Omega = (w_1, \ldots, w_n)^T \in \mathrm{Mat}_{n,s}(\mathbb{F}_q)$ onde $w_i \in F_q^s$, conseguimos assim uma relação entre F_R e $S_{I=\varphi(R)}$ e entre F_R e $S_{J^c=\psi(R)}$.

Proposição 4.3. *Seja $F_R \subset Mat_{n,s}(\mathbb{F}_q)$, $R \in Q_{n,s}$. Então:*

(i) $T(F_R) = S_{\varphi(R)}$.

(ii) $TD(F_R) = S_{\psi(R)}$.

Demonstração:

(i) De fato, temos que $F_R = \prod_{j=1}^{n} S_{r_j}^{(1,s)} = \{\Omega \in \mathrm{Mat}_{n,s}(\mathbb{F}_q) | \rho(w_j) = r_j\}$, assim aplicando T em Ω, φ em R e do fato de que $\rho(w_j) = \omega_P(T(w_j))$ teremos

$$F_R = \{\Omega \in \mathrm{Mat}_{n,s}(\mathbb{F}_q) | \rho(w_j) = r_j\} = \{T(\Omega) \in \mathbb{F}_q^{ns} | \langle \mathrm{supp}(T(\Omega))\rangle_P = \varphi(R) = I\} = S_{\varphi(R)}.$$

(ii) Aplicando TD em Ω e ψ em R teremos

$$F_R = \{T(D(\Omega)) \in \mathbb{F}_q^{ns} | \langle \mathrm{supp}(T(D(\Omega)))\rangle_{P^*} = \psi(R) = J^c\} = S_{\psi(R)}.$$

■

Temos também que $\Phi_R = \bigcup_{\sigma \in S_n / S_n^{(R)}} F_{\sigma R}$, $R \in Q_{n,s}/S_n$ logo conseguimos o seguinte corolário

Corolário 4.4. *Seja $\Phi_R \subset Mat_{n,s}(\mathbb{F}_q)$. Então:*

(i) $\Phi_R = S_{\overline{\varphi(R)}}$.

(ii) $\Phi_R = S_{\overline{\psi(R)}}$.

Demonstração: Pela Proposição 4.3 temos :

(i) $\Phi_R = \bigcup_{\sigma \in S_n / S_n^{(R)}} F_{\sigma R} = \bigcup_{\varphi(R) \in \overline{\varphi(R)}} S_{\varphi(R)} = S_{\overline{\varphi(R)}} = S_{\overline{I}}$ onde $I = \varphi(R)$.

(ii) $\Phi_R = \bigcup_{\sigma \in S_n/S_n^{(R)}} F_{\sigma R} = \bigcup_{\psi(R)\in\overline{\psi(R)}} S_{\psi(R)} = S_{\overline{\psi(R)}} = S_{J^c}$ onde $J^c = \psi(R)$.

■

Além disso, tomando $H = S_n = \mathrm{Aut}(P)$, temos que se $R \in Q_{n,s}/S_n$, podemos restringir φ e ψ a $Q_{n,s}/S_n$ e conseguimos aplicações entre $Q_{n,s}/S_n$ e $I(P)/E_H$ e $I(P^*)/E_H^*$ respectivamente.

Notemos também que dado um código linear $\mathscr{C} \subset \mathrm{Mat}_{n,s}(\mathbb{F}_q)$, aplicando T aos elementos de $\mathscr{C}$, obtemos $\mathscr{C}' = T(\mathscr{C}) \subset \mathbb{F}_q^{ns}$ onde $v' \in \mathscr{C}'$ é tal que $v' = T(v)$, com $v \in \mathscr{C}$. Como T é uma transformação linear, temos que $\mathscr{C}'$ é um código linear em $\mathbb{F}_q^{ns}$. Além disso, se a dimensão de $\mathscr{C}$ é k então, como T é uma isometria e preserva dimensão, teremos que a dimensão de $\mathscr{C}'$ será k. Analogamente se $\mathscr{C}^\perp$ é o código dual do código $\mathscr{C}$ então, aplicando TD aos elementos de $\mathscr{C}^\perp$ obtemos $T(D(\mathscr{C}^\perp)) \subset \mathbb{F}_q^{ns}$ onde $u' = T(D(u))$, com $u \in \mathscr{C}^\perp$.

Denotemos o produto interno usual em $\mathbb{F}_q^s$ por $\langle\cdot,\cdot\rangle$, e definamos o produto interno

$$\langle \Omega_1, \Omega_2 \rangle_M = \sum_{j=1}^{n} \langle v_1^{(j)}, v_2^{(j)} \rangle.$$

Assim, utilizando o produto interno dado em (4.2) conseguimos o seguinte resultado:

Lema 4.5. *Sejam* $\Omega_i = (v_i^{(1)}, \ldots, v_i^{(n)}) \in Mat_{n,s}(\mathbb{F}_q)$, $i = 1,2$; $v_i^j \in Mat_{1,s}(\mathbb{F}_q)$, $1 \le j \le n$. *Então:*

(i) $\langle \Omega_1, \Omega_2 \rangle_{DS} = \langle \Omega_1, D(\Omega_2) \rangle_M$.

(ii) *Se* $\mathscr{C} \subset Mat_{n,s}(\mathbb{F}_q)$ *é um código linear e* $\mathscr{C}' = T(\mathscr{C})$ *então* $\mathscr{C}'^\perp = TD(\mathscr{C}^\perp)$.

Demonstração:

(i) De fato, denotemos $v_1^{(j)} = (\xi_1^{(j)}, \ldots, \xi_s^{(j)})$ e $v_2^{(j)} = (\xi_1'^{(j)}, \ldots, \xi_s'^{(j)})$, logo por (4.2) e (4.1), teremos

$$\langle \Omega_1, \Omega_2 \rangle_{DS} = \sum_{j=1}^{n} \langle v_1^{(j)}, v_2^{(j)} \rangle_D = \sum_{j=1}^{n} \left(\sum_{i=1}^{s} \xi_i^{(j)} \xi_{s+1-i}'^{(j)} \right) = \sum_{j=1}^{n} \langle v_1^{(j)}, D(v_2^{(j)}) \rangle = \langle \Omega_1, D(\Omega_2) \rangle_M.$$

(ii) Sejam $u, v \in \mathrm{Mat}_{n,s}(\mathbb{F}_q)$ logo temos

$$u \in \mathscr{C}^\perp \Leftrightarrow 0 = \langle u, v \rangle_{DS}, \forall\, v \in \mathscr{C} \Leftrightarrow \langle D(u), v \rangle_M = 0, \forall\, v \in \mathscr{C} \Leftrightarrow$$
$$\langle T(D(u)), T(v) \rangle = 0, \forall\, T(v) \in \mathscr{C}' \Leftrightarrow T(D(u)) \in \mathscr{C}'^\perp.$$

■

Note assim que, como T e D são isometrias, pelo lema acima, se a dimensão de $\mathscr{C}$ é k então a dimensão de $\mathscr{C}'$ será k e teremos que a dimensão de $\mathscr{C}'^\perp$ é $ns-k$, ou seja, a dimensão de $\mathscr{C}^\perp$ é $ns-k$, como mencionamos na seção anterior.

Consideremos agora $H = Id \in \mathrm{Aut}(P)$, logo teremos $I(P) = I(P)/E_H$, $I(P^*) = I(P^*)/E_H^*$, $S_I = S_{\overline{I},E_H}$ e $S_{J^c} = S_{\overline{J^c},E_H^*}$. Assim, podemos denotar $A_{\overline{I},E_H}(\mathscr{C}')$ por $A_{I,E_H}(\mathscr{C}')$ e $A_{\overline{J^c},E_H^*}(\mathscr{C}'^{\perp})$ por $A_{J^c,E_H^*}(\mathscr{C}'^{\perp})$. Obtemos então o seguinte corolário:

Corolário 4.6. *Sejam $\mathscr{C}, \mathscr{C}^{\perp} \subset Mat_{n,s}(\mathbb{F}_q)$ e $H = Id \in Aut(P)$. Então:*

(i) $t_R(\mathscr{C}) = A_{I,E_H}(\mathscr{C}')$.

(ii) $t_R(\mathscr{C}^{\perp}) = A_{J^c,E_H^*}(\mathscr{C}'^{\perp})$

Demonstração:

(i) De fato, note que da Proposição 4.3 (i) temos $T(F_R) = S_{\varphi(R)}$, logo teremos

$$v \in \mathscr{C} \cap F_R \Leftrightarrow T(v) \in T(\mathscr{C}) \cap S_{\varphi(R)} \Leftrightarrow T(v) \in \mathscr{C}' \cap S_I \text{ com } I = \varphi(R).$$

Assim obtemos

$$t_R(\mathscr{C}) = |\mathscr{C} \cap F_R| = |T(\mathscr{C}) \cap S_{\varphi(R)}| = |\mathscr{C}' \cap S_I| = A_{I,E_H}(\mathscr{C}'), \text{ onde } I = \varphi(R).$$

(ii) Analogamente, da Proposição 4.3 (ii) temos que $TD(F_R) = S_{\psi(R)}$, logo teremos

$$u \in \mathscr{C}^{\perp} \cap F_R \Leftrightarrow T(D(u)) \in T(D(\mathscr{C}^{\perp})) \cap S_{\psi(R)} \Leftrightarrow T(D(u)) \in \mathscr{C}'^{\perp} \cap S_{J^c} \text{ com } J^c = \psi(R).$$

Assim obtemos

$$t_R(\mathscr{C}^{\perp}) = |\mathscr{C}^{\perp} \cap F_R| = |T(D(\mathscr{C}^{\perp})) \cap S_{\psi(R)}| = |\mathscr{C}'^{\perp} \cap S_{J^c}| = A_{J^c,E_H^*}(\mathscr{C}'^{\perp}), \text{ onde } J^c = \psi(R).$$

■

Vejamos um exemplo englobando as aplicações vistas até aqui nesta seção.

Exemplo 4.4. Consideremos o espaço das matrizes 2×2 com entradas em $\mathbb{F}_2$ e tomemos os códigos $\mathscr{C}$ e $\mathscr{C}^{\perp}$ apresentados no Exemplo 4.3, bem como os conjuntos

$Q_{2,2} = \{R_0 = (0,0), R_1 = (1,0), R_2 = (2,0), R_3 = (0,1), R_4 = (0,2), R_5 = (1,1), R_6 = (1,2), R_7 = (2,1), R_8 = (2,2)\}$ e

$Q_{2,2}/S_2 = \{R_0 = (0,0), R_3 = (0,1), R_4 = (0,2), R_5 = (1,1), R_6 = (1,2), R_8 = (2,2)\}$.

Aplicando T em $\mathscr{C}$ obtemos $\mathscr{C}' = \{(0,0,0,0), (1,1,0,0)\}$ e aplicando TD em $\mathscr{C}^{\perp}$ obtemos

$$\mathscr{C}'^{\perp} = \{(0,0,0,0), (1,1,0,0), (1,1,1,1), (1,1,1,0), (1,1,0,1), (0,0,1,0), (0,0,0,1), (0,0,1,1)\}.$$

Tomemos então o poset P em [4] com relação de ordem dada por $1 \preceq 3$ e $2 \preceq 4$, ou seja, o poset é uma união de duas cadeias disjuntas de comprimento 2.

Aplicando φ nos elementos de $Q_{2,2}$ teremos:

$\varphi(R_0)=\langle 0\rangle_P=\emptyset=I_0$, $\varphi(R_1)=\langle 1\rangle_P=\{1\}=I_1$, $\varphi(R_2)=\langle 3\rangle_P=\{1,3\}=I_2$,
$\varphi(R_3)=\langle 1\rangle_P=\{2\}=I_3$, $\varphi(R_4)=\langle 4\rangle_P=\{2,4\}=I_4$, $\varphi(R_5)=\langle 1,2\rangle_P=\{1,2\}=I_5$,
$\varphi(R_6)=\langle 1,4\rangle_P=\{1,2,4\}=I_6$, $\varphi(R_7)=\langle 3,2\rangle_P=\{1,2,3\}=I_7$, $\varphi(R_8)=\langle 3,4\rangle_P=P=I_8$.

Ou seja, temos

$$I(P)=\varphi(Q_{2,2})=\{\emptyset,\{1\},\{1,3\},\{2\},\{2,4\},\{1,2\},\{1,2,4\},\{1,2,3\},P\}.$$

Restringindo φ aos elementos de $Q_{2,2}/S_2$ e tomando $H=S_2$ teremos

$$I(P)/E_H=\{\overline{\varphi(R_0)},\overline{\varphi(R_3)},\overline{\varphi(R_4)},\overline{\varphi(R_5)},\overline{\varphi(R_6)},\overline{\varphi(R_8)}\}=\{\overline{\emptyset},\overline{\{2\}},\overline{\{2,4\}},\overline{\{1,2\}},\overline{\{1,2,4\}},\overline{P}\}.$$

Assim, da definição de I-esfera apresentada no Capítulo 3 teremos:

$S_{I_0}=S_{\varphi(R_0)}=\{(0,0,0,0)\}$, $S_{I_1}=S_{\varphi(R_1)}=\{(1,0,0,0)\}$, $S_{I_2}=S_{\varphi(R_2)}=\{(0,0,1,0),(1,0,1,0)\}$,
$S_{I_3}=S_{\varphi(R_3)}=\{(0,1,0,0)\}$, $S_{I_4}=S_{\varphi(R_4)}=\{(0,0,0,1),(0,1,0,1)\}$, $S_{I_5}=S_{\varphi(R_5)}=\{(1,1,0,0)\}$,
$S_{I_6}=S_{\varphi(R_6)}=\{(1,0,0,1),(1,1,0,1)\}$, $S_{I_7}=S_{\varphi(R_7)}=\{(0,1,1,0),(1,1,1,0)\}$,
$S_{I_8}=S_{\varphi(R_8)}=\{(0,0,1,1),(1,0,1,1),(0,1,1,1),(1,1,1,1)\}$.

Assim vemos que aplicando φ em $R\in Q_{2,2}$ e T em $v\in F_R$ no Exemplo 4.3, obtemos $T(F_{R_i})=S_{\varphi(R_i)}=S_{I_i}$, $0\leq i\leq 8$. Logo, tomando $H=Id$ teremos $I(P)/E_H=I(P)$, e lembrando que $A_{\overline{I},E_H}(\mathscr{C})=|S_{\overline{I}}\cap\mathscr{C}|$ teremos:

$A_{I_0,E_H}(\mathscr{C}')=A_{I_5,E_H}(\mathscr{C}')=1$ e

$A_{I_0,E_H}(\mathscr{C}')=A_{I_1,E_H}(\mathscr{C}')=A_{I_2,E_H}(\mathscr{C}')=A_{I_3,E_H}(\mathscr{C}')=A_{I_4,E_H}(\mathscr{C}')=A_{I_6,E_H}(\mathscr{C}')=A_{I_7,E_H}(\mathscr{C}')=A_{I_8,E_H}(\mathscr{C}')=0$.

Logo vemos que $t_{R_i}(\mathscr{C})=A_{I_i,E_H}(\mathscr{C}')=A_{\varphi(R_i),E_H}(\mathscr{C}')$, $0\leq i\leq 8$.

Da mesma forma, pela definição de $\overline{I}$-esfera apresentada no Capítulo 3, tomando $H=S_2$ temos

$S_{\overline{I_0},E_H}=S_{\overline{\varphi(R_0)},E_H}=\{(0,0,0,0)\}$, $S_{\overline{I_3},E_H}=S_{\overline{\varphi(R_3)},E_H}=\{(0,1,0,0),(1,0,0,0)\}$,
$S_{\overline{I_4},E_H}=S_{\overline{\varphi(R_4)},E_H}=\{(0,0,1,0),(1,0,1,0),(0,0,0,1),(0,1,0,1)\}$,
$S_{\overline{I_5},E_H}=S_{\overline{\varphi(R_5)},E_H}=\{(1,1,0,0)\}$, $S_{\overline{I_6},E_H}=S_{\overline{\varphi(R_6)},E_H}=\{(1,0,0,1),(1,1,0,1),(0,1,1,0),(1,1,1,0)\}$,
$S_{\overline{I_8},E_H}=S_{\overline{\varphi(R_8)},E_H}=\{(0,0,1,1),(1,0,1,1),(0,1,1,1),(1,1,1,1)\}$.

Assim, obtemos

$A_{\overline{I_0},E_H}(\mathscr{C}')=A_{\overline{I_5},E_H}(\mathscr{C}')=1$ e
$A_{\overline{I_3},E_H}(\mathscr{C}')=A_{\overline{I_4},E_H}(\mathscr{C}')=A_{\overline{I_6},E_H}(\mathscr{C}')=A_{\overline{I_8},E_H}(\mathscr{C}')=0$.

Vemos então que $h_{R_i}(\mathscr{C})=A_{\overline{I_i},E_H}(\mathscr{C}')=A_{\overline{\varphi(R_i)},E_H}(\mathscr{C}')$, $0\leq i\leq 8$.

Por outro lado, aplicando ψ nos elementos de $Q_{2,2}$ teremos

$\psi(R_0)=\langle 0\rangle_{P^*}=\emptyset=J_0^c$, $\psi(R_1)=\langle 3\rangle_{P^*}=\{3\}=J_1^c$, $\psi(R_2)=\langle 1\rangle_{P^*}=\{1,3\}=J_2^c$,
$\psi(R_3)=\langle 4\rangle_{P^*}=\{4\}=J_3^c$, $\psi(R_4)=\langle 2\rangle_{P^*}=\{2,4\}=J_4^c$, $\psi(R_5)=\langle 3,4\rangle_{P^*}=\{3,4\}=J_5^c$,

$\psi(R_6)=\langle 3,2\rangle_{P^*}=\{3,2,4\}=J_6^c$, $\psi(R_7)=\langle 1,4\rangle_{P^*}=\{1,3,4\}=J_7^c$, $\psi(R_8)=\langle 1,2\rangle_{P^*}=P^*=J_8^c$.

Logo teremos

$S_{J_0^c}=S_{\psi(R_0)}=\{(0,0,0,0)\}$, $S_{J_1^c}=S_{\psi(R_1)}=\{(0,0,1,0)\}$, $S_{J_2^c}=S_{\psi(R_2)}=\{(1,0,0,0),(1,0,1,0)\}$,
$S_{J_3^c}=S_{\psi(R_3)}=\{(0,0,0,1)\}$, $S_{J_4^c}=S_{\psi(R_4)}=\{(0,1,0,0),(0,1,0,1)\}$, $S_{J_5^c}=S_{\psi(R_5)}=\{(0,0,1,1)\}$,
$S_{J_6^c}=S_{\psi(R_6)}=\{(0,1,1,0),(0,1,1,1)\}$, $S_{J_7^c}=S_{\psi(R_7)}=\{(1,0,0,1),(1,0,1,1)\}$,
$S_{J_8^c}=S_{\psi(R_8)}=\{(1,1,0,0),(1,1,1,0),(1,1,0,1),(1,1,1,1)\}$.

Assim, vemos que aplicando ψ em $R\in Q_{2,2}$ e TD em $v\in F_R$ obtemos $TD(F_{R_i})=S_{\psi(R_i)}=S_{J_i^c}$, $\quad 0\le i\le 8$.

Tomando $H=Id$ teremos $I(P^*)/E_H^*=I(P^*)$ e assim obtemos

$A_{J_0^c,E_H^*}(\mathscr{C}'^{\perp})=A_{J_1^c,E_H^*}(\mathscr{C}'^{\perp})=A_{J_3^c,E_H^*}(\mathscr{C}'^{\perp})=A_{J_5^c,E_H^*}(\mathscr{C}'^{\perp})=1$,
$A_{J_2^c,E_H^*}(\mathscr{C}'^{\perp})=A_{J_4^c,E_H^*}(\mathscr{C}'^{\perp})=A_{J_6^c,E_H^*}(\mathscr{C}'^{\perp})=A_{J_7^c,E_H^*}(\mathscr{C}'^{\perp})=0$ e
$A_{J_8^c,E_H^*}(\mathscr{C}'^{\perp})=4$.

Logo vemos que $t_{R_i}(\mathscr{C}^{\perp})=A_{J_i^c,E_H^*}(\mathscr{C}'^{\perp})=A_{\psi(R_i),E_H^*}(\mathscr{C}'^{\perp})$.

Porém, se tomarmos $H=S_2$ e restringirmos N ao conjunto $Q_{2,2}/S_2$ teremos

$$I(P^*)/E_H^*=\{\overline{\psi(R_0)},\overline{\psi(R_3)},\overline{\psi(R_4)},\overline{\psi(R_5)},\overline{\psi(R_6)},\overline{\psi(R_8)}\}=\{\overline{\emptyset},\overline{\{4\}},\overline{\{2,4\}},\overline{\{3,4\}},\overline{\{3,2,4\}},\overline{P^*}\}.$$

Assim temos

$S_{\overline{J_0^c},E_H^*}=S_{\overline{\psi(R_0)},E_H^*}=\{(0,0,0,0)\}$, $S_{\overline{J_3^c},E_H^*}=S_{\overline{\psi(R_3)},E_H^*}=\{(0,0,0,1),(0,0,1,0)\},\}$
$S_{\overline{J_4^c},E_H^*}=S_{\overline{\psi(R_4)},E_H^*}=\{(1,0,0,0),(1,0,1,0),(0,1,0,0),(0,1,0,1)\}$, $S_{\overline{J_5^c},E_H^*}=S_{\overline{\psi(R_5)},E_H^*}=\{(0,0,1,1)\}$,
$S_{\overline{J_6^c},E_H^*}=S_{\overline{\psi(R_6)},E_H^*}=\{(0,1,1,0),(0,1,1,1),(1,0,0,1),(1,0,1,1)\}$,
$S_{\overline{J_8^c},E_H^*}=S_{\overline{\psi(R_8)},E_H^*}=\{(1,1,0,0),(1,1,1,0),(1,1,0,1),(1,1,1,1)\}$.

Logo obtemos

$A_{\overline{J_0^c},E_H^*}(\mathscr{C}'^{\perp})=A_{\overline{J_5^c},E_H^*}(\mathscr{C}'^{\perp})=1$,
$A_{\overline{J_4^c},E_H^*}(\mathscr{C}'^{\perp})=A_{\overline{J_6^c},E_H^*}(\mathscr{C}'^{\perp})=0$,
$A_{\overline{J_3^c},E_H^*}(\mathscr{C}'^{\perp})=2$ e $A_{\overline{J_8^c},E_H^*}(\mathscr{C}'^{\perp})=4$.

Assim vemos que $h_{R_i}(\mathscr{C}^{\perp})=A_{\overline{J_i^c},E_H^*}(\mathscr{C}'^{\perp})$, $0\le i\le 8$.

Agora, denotemos o produtório $\prod_{j=1}^{n} z_{r_j}^{(j)}$ por $X_{\varphi(R)}=X_I$, logo da definição 4.3 teremos

$$T(\mathscr{C}|Z_1,\ldots,Z_n)=\sum_{R\in Q_{n,s}} t_R(\mathscr{C})\prod_{j=1}^{n} z_{r_j}^{(j)}\simeq\sum_{\varphi(R)\in I(P)} A_{\varphi(R),E_H}(\mathscr{C}')X_{\varphi(R)}=\sum_{I\in I(P)} A_{I,E_H}(\mathscr{C}')X_I.$$

Agora, denotando por X o vetor $[X_I]_{I\in I(P)}$ e lembrando que $W(\mathscr{C},P,E_H)=[A_{\overline{I},E_H}(\mathscr{C})]_{\overline{I}\in I(P)/E_H}$ teremos

$$T(\mathscr{C}|Z_1,\ldots,Z_n)=\sum_{I\in I(P)} A_{I,E_H}(\mathscr{C}')X^T=W(\mathscr{C}',P,E_H)X^T.$$

Assim, segue do Teorema 3.7 (iii) que

$$T(\mathscr{C}|Z_1,\ldots,Z_n) = W(\mathscr{C}',P,E_H)X^T = \frac{1}{|\mathscr{C}'^{\perp}|}W(\mathscr{C}'^{\perp},P^*,E_H^*)Q_{E_H^*}^T X^T \tag{4.5}$$

Pela definição de $Q_{E_H^*}$ temos $Q_{E_H^*} = [q_{\overline{I},\overline{J^c}}]$ onde $Q_{E_H^*}$ é uma matriz $|I(P)/E_H| \times |I(P^*)/E_H^*|$. Como, neste caso temos $\overline{I} = I$ e $\overline{J^c} = J^c$ teremos

$$Q_{E_H^*}^T X^T = \left[\sum_{I\in I(P)} q_{I,J^c}\right]_{J^c\in I(P^*)} \tag{4.6}$$

Com os resultados obtidos, conseguimos um teorema que mostra que podemos obter as matrizes $Q_{E_H^*}$ e P_{E_H} apenas com as entradas referentes à primeira cadeia.

Teorema 4.7. *Sejam P um poset união de n cadeias disjuntas de comprimento s e $H = Id$.*

(i) Se $n = 1$, então a matriz $Q_{E_H^*}^T$ obtida é a matriz Θ_s, além disso, $Q_{E_H^*}^T = P_{E_H}^T$.

(ii) Se $n > 1$, as matrizes $Q_{E_H^*}$ e P_{E_H} são totalmente determinadas pelas entradas obtidas no item (i) respectivamente.

Demonstração:

(i) Seja $n = 1$, ou seja, o poset P é uma cadeia de comprimento s. Logo, consideremos $I_k \in I(P)$, com $I_k = \varphi(R_k)$ onde $R_k = k \in Q_{1,s} = \{0,1,\ldots,s\}$, e à cada R_k desta forma está também associado um ideal $J_k^c = \psi(R_k) \in I(P^*)$. Assim sejam R_k e $R_l \in Q_{n,s}$ da forma vista acima, com $\varphi(R_k) = I_k$ e $\psi(R_l) = J_l^c$. Note que neste caso se $k \neq 0$ então $M(I_k) = M(\varphi(R_k)) = k$, logo $|M(I_k)| = |M(\varphi(R_k))| = 1$ e $|(I_k)_M| = |(\varphi(R_k))_M| = k-1$. Segue da Proposição 3.11 (ii) que

$$q_{I_k,J_l^c} = q_{\varphi(R_k),\psi(R_l)} = (q-1)^{|M(\varphi(R_k))|}q^{|(\varphi(R_k))_M|}\left(\frac{-1}{q-1}\right)^{|\psi(R_l)\cap\varphi(R_k)|} \quad \text{se} \quad (\psi(R_l))_M \cap \varphi(R_k) = \emptyset$$
$$q_{I_k,J_l^c} = q_{\varphi(R_k),\psi(R_l)} = 0 \quad \text{se} \quad (\psi(R_l))_M \cap \varphi(R_k) \neq \emptyset.$$

Porém, temos que $(\psi(R_l))_M \cap \varphi(R_k) \neq \emptyset \Leftrightarrow k > s-l+1$ e $(\psi(R_l))_M \cap \varphi(R_k) = \emptyset \Leftrightarrow k \leq s-l+1$, e neste caso teremos $|\psi(R_l) \cap \varphi(R_k)| = 0$ se $k \leq s-l$ e $|\psi(R_l) \cap \varphi(R_k)| = 1$ se $k = s-l+1$, logo teremos

$$q_{I_k,J_l^c} = \begin{cases} 1 & \text{se} \quad k = 0 \\ q^{k-1}(q-1) & \text{se} \quad 0 < k \leq s-l \\ -q^{k-1} & \text{se} \quad k+l = s+1 \\ 0 & \text{se} \quad k+l > s+1 \end{cases}$$

Comparando este resultado com as entradas da matriz Θ_s dadas em (4.4) temos que $\theta_{l,k} = q_{I_k,J_l^c}$ ou seja, a matriz Θ_s é a matriz $Q_{E_H^*}^T$ referente aos ideais da primeira cadeia do poset P.

Analogamente, tomemos $\psi(R_k) = J_k^c$ e $\varphi(R_l) = I_l$, assim, se $k \neq 0$ então então $M(J_k^c) = M(\psi(R_k)) = k$ logo $|M(J_k^c)| = |M(\psi(R_k))| = 1$ e consequentemente $|(J_k^c)_M| = k-1$. Segue da Proposição 3.11 (i) que

$$\begin{array}{ll} p_{J_k^c,I_l} = p_{\psi(R_k),\varphi(R_l)} = (q-1)^{|M(\psi(R_k))|} q^{|(\psi(R_k))_M|} \left(\dfrac{-1}{q-1}\right)^{|\varphi(I_l)\cap\psi(R_k)|} & \text{se} \quad (\varphi(R_l))_M \cap \psi(R_k) = \emptyset \\ p_{J_k^c,I_l} = p_{\psi(R_k),\varphi(R_l)} = 0 & \text{se} \quad (\varphi(R_l))_M \cap \psi(R_k) \neq \emptyset. \end{array}.$$

Porém, temos que $(\varphi(R_l))_M \cap \psi(R_k) \neq \emptyset \Leftrightarrow k > s-l+1$ e $(\varphi(R_l))_M \cap \psi(R_k) = \emptyset \Leftrightarrow k \leq s-l+1$ e neste caso teremos $|\varphi(R_l) \cap \psi(R_k)| = 0$ se $k \leq s-l$ e $|\varphi(R_l) \cap \psi(R_k)| = 1$ se $k = s-l+1$, logo teremo

$$p_{J_k^c,I_l} = \begin{cases} 1 & \text{se} \quad k = 0 \\ q^{k-1}(q-1) & \text{se} \quad 0 < k \leq s-l \\ -q^{k-1} & \text{se} \quad k+l = s+1 \\ 0 & \text{se} \quad k+l > s+1 \end{cases}$$

Assim vemos que $\theta_{l,k} = p_{J_k^c,I_l}$ e obtemos $Q_{E_H^*}^T = P_{E_H}^T = \Theta_s$, como queríamos.

(ii) Agora seja $n > 1$. Indexemos os ideais referentes à primeira cadeia do poset P da seguinte maneira: $I_i = \varphi(R_i)$ onde $R_i = (i, 0, \ldots, 0) \in Q_{n,s}$ com $0 \leq i \leq s$.

Sejam $I \in I(P)$ com $I = \varphi(R)$ onde $R = (r_1, \ldots, r_n) \in Q_{n,s}$, $0 \leq r_j \leq s$ e $J^c \in I(P^*)$ com $J^c = \psi(R')$ onde $R' = (r_1', \ldots, r_n') \in Q_{n,s}$, $0 \leq r_j' \leq s$.

Mostremos que $q_{I,J^c} = q_{\varphi(R),\psi(R')} = \prod_{j=1}^{n} q_{I_{r_j},J_{r_j'}^c}$.

Mostraremos por indução em n. Para $n = 1$ não há o que se mostrar, vejamos para $n = 2$.

Sejam $R = (r_1, r_2)$ e $R' = (r_1', r_2') \in Q_{2,s}$ logo teremos:

$$\begin{aligned} &\prod_{j=1}^{2} q_{I_{r_j},J_{r_j'}^c} = q_{I_{r_1},J_{r_1'}^c} q_{I_{r_2},J_{r_2'}^c} = \\ &= \left[(q-1)^{|M(I_{r_1})|} q^{|(I_{r_1})_M|} \left(\frac{-1}{q-1}\right)^{|J_{r_1'}^c \cap I_{r_1}|}\right]\left[(q-1)^{|M(I_{r_2})|} q^{|(I_{r_2})_M|} \left(\frac{-1}{q-1}\right)^{|J_{r_2'}^c \cap I_{r_2}|}\right] = \\ &= (q-1)^{(|M(I_{r_1})|+|M(I_{r_2})|-(|J_{r_1'}^c \cap I_{r_1}|+|J_{r_2'}^c \cap I_{r_2}|))} q^{|(I_{r_1})_M|+|(I_{r_2})_M|} (-1)^{|J_{r_1'}^c \cap I_{r_1}|+|J_{r_2'}^c \cap I_{r_2}|} = \\ &= (q-1)^{(|M(I)|-|J^c \cap I|)} q^{|I_M|} (-1)^{|J^c \cap I|} = q_{I,J^c} \end{aligned} \tag{4.7}$$

Assim, para $n=2$ vale. Suponha que vale para $n-1$, mostremos que vale para n.

Note que podemos tomar $R=(r_1,\ldots,r_n)$ como $R=(R\_,r_n)$ onde $R\_=(r_1,\ldots,r_{n-1})$ e da mesma forma temos $R'=(R'\_,r'_n)$ onde $R'\_=(r'_1,\ldots,r'_{n-1})$, assim, por (4.7) teremos $q_{I,J^c}=q_{I_{r_n},J^c_{r'_n}}q_{\varphi(R\_),\psi(R'\_)}$ e pela hipótese indutiva temos que $q_{\varphi(R\_),\psi(R'\_)}=\prod_{j=1}^{n-1}q_{I_{r_j},J^c_{r'_j}}$, logo teremos $q_{I,J^c}=q_{I_{r_n},J^c_{r'_n}}\prod_{j=1}^{n-1}q_{I_{r_j},J^c_{r'_j}}=\prod_{j=1}^{n}q_{I_{r_j},J^c_{r'_j}}$. E temos o resultado desejado.

Para o caso da matriz P_{E_H} a demonstração é completamente análoga.

■

Exemplo 4.5. Consideremos os resultados obtidos para o Exemplo 4.4 com $H=Id$. Logo teremos que os ideais referentes à primeira cadeia do poset P e P^* são os referentes aos elementos $R_0,R_1,\text{e}R_2\in Q_{2,2}$, ou seja:

$I_0=\emptyset=\varphi(R_0),\quad I_1=\{1\}=\varphi(R_1),\quad I_2=\{1,3\}=\varphi(R_2)$ e

$J_0^c=\emptyset=\psi(R_0),\quad J_1^c=\{3\}=\psi(R_1),\quad J_2^c=\{1,3\}=\psi(R_2).$

Logo, como neste caso temos $q=2$ obtemos

$$q_{I,J^c}=\begin{cases}1^{|M(I)|}2^{|I_M|}(-1)^{|J^c\cap I|} & \text{se}\quad (J^c)_M\cap I=\emptyset\\ 0 & \text{se}\quad (J^c)_M\cap I\neq\emptyset\end{cases}$$

Portanto obtemos

$$Q_{E_H^*}=\begin{bmatrix}q_{I_0,J_0^c} & q_{I_0,J_1^c} & q_{I_0,J_2^c}\\ q_{I_1,J_0^c} & q_{I_1,J_1^c} & q_{I_1,J_2^c}\\ q_{I_2,J_0^c} & q_{I_2,J_1^c} & q_{I_2,J_2^c}\end{bmatrix}=\begin{bmatrix}1 & 1 & 1\\ 1 & 1 & -1\\ 2 & -2 & 0\end{bmatrix}.$$

Analogamente, temos que

$$p_{J^c,I}=\begin{cases}1^{|M(J^c)|}2^{|(J^c)_M|}(-1)^{|I\cap J^c|} & \text{se}\quad (I)_M\cap J^c=\emptyset\\ 0 & \text{se}\quad (I)_M\cap J^c\neq\emptyset\end{cases}$$

Logo obtemos

$$P_{E_H}=\begin{bmatrix}p_{J_0^c,I_0} & p_{J_0^c,I_1} & p_{J_0^c,I_2}\\ p_{J_1^c,I_0} & p_{J_1^c,I_1} & p_{J_1^c,I_2}\\ p_{J_2^c,I_0} & p_{J_2^c,I_1} & p_{J_2^c,I_2}\end{bmatrix}=\begin{bmatrix}1 & 1 & 1\\ 1 & 1 & -1\\ 2 & -2 & 0\end{bmatrix}$$

Consideremos então $R=(1,2)$ e $R'=(1,1)$, logo temos que $\varphi(R)=\{1,2,4\}=I$ e $\psi(R')=\{3,4\}=J^c$. Note que $(J^c)_M=\emptyset$ logo $(J^c)_M\cap I=\emptyset$, assim temos $q_{I,J^c}=1^2\cdot 2^1\cdot(-1)^1=-2$. Por outro lado temos

$\prod_{j=1}^{2}q_{I_{r_j},J^c_{r'_j}}=q_{I_{r_1},J^c_{r'_1}}q_{I_{r_2},J^c_{r'_2}}=q_{I_1,J_1^c}q_{I_2,J_1^c}=1\cdot(-2)=-2$, como era esperado.

Analogamente temos $(I)_M=\{2\}$ logo $(I)_M\cap J^c=\emptyset$ e temos $p_{J^c,I}=1^2\cdot 2^0\cdot(-1)^1=-1$. Por outro lado temos

$\prod_{j=1}^{2} p_{J^c_{r'_j},I_{r_j}} = p_{J^c_{r'_1},I_{r_1}} p_{J^c_{r'_2},I_{r_2}} = p_{J_1^c,I_1} p_{J_1^c,I_2} = 1\cdot(-1) = -1$, como era esperado.

Analisemos agora o restultado obtido em (4.6) aplicando o Teorema 4.7.

Em (4.6) encontramos $Q^T_{E^*_H} X^T = \left[\sum_{I\in I(P)} q_{I,J^c}\right]_{J^c\in I(P^*)}$, onde $I=\varphi(R)$ e $X_I = X_{\varphi(R)} = \prod_{j=1}^{n} z^{(j)}_{r_j}$.

Assim, temos

$$\sum_{I\in I(P)} q_{I,J^c} X_I = \sum_{R\in Q_{n,s}} q_{\varphi(R),\psi(R')} X_{\varphi(R)} = \sum_{R\in Q_{n,s}} q_{\varphi(R),\psi(R')} \prod_{j=1}^{n} z^{(j)}_{r_j}.$$

Pelo item (ii) do teorema acima temos que $q_{\varphi(R),\psi(R')} = \prod_{j=1}^{n} q_{I_{r_j},J^c_{r'_j}}$ logo teremos

$$\sum_{I\in I(P)} q_{I,J^c} X_I = \sum_{R\in Q_{n,s}} \left(\prod_{j=1}^{n} q_{I_{r_j},J^c_{r'_j}} \prod_{j=1}^{n} z^{(j)}_{r_j}\right) = \sum_{R\in Q_{n,s}} \left(\prod_{j=1}^{n} q_{I_{r_j},J^c_{r'_j}} z^{(j)}_{r_j}\right)$$

e aplicando o resultado obtido no item (i) do mesmo teorema teremos

$$\sum_{I\in I(P)} q_{I,J^c} X_I = \sum_{R\in Q_{n,s}} \left(\prod_{j=1}^{n} \theta_{r'_j,r_j} z^{(j)}_{r_j}\right).$$

Agora, aplicando o Teorema 1.11 teremos

$$\sum_{I\in I(P)} q_{I,J^c} X_I = \sum_{R\in Q_{n,s}} \left(\prod_{j=1}^{n} \theta_{r'_j,r_j} z^{(j)}_{r_j}\right) = \prod_{j=1}^{n} \left(\sum_{k=0}^{s} \theta_{r'_j,k} z^{(j)}_{k}\right) = \prod_{j=1}^{n} z'^{(j)}_{r'_j}.$$

Assim, denotando $\prod_{j=1}^{n} z'^{(j)}_{r'_j}$ por $X'_{\psi(R')} = X'_{J^c}$ teremos $Q^T_{E^*_H} X^T = [X'_{J^c}]^T_{J^c\in I(P^*)} = [X']^T$. Logo substituindo em (4.5) teremos

$$\begin{aligned}
&T(\mathscr{C}|Z_1,\ldots,Z_n) = \frac{1}{|\mathscr{C}'^{\perp}|} W(\mathscr{C}'^{\perp}, P^*, E^*_H) Q^T_{E^*_H} X^T = \\
&= \frac{1}{|\mathscr{C}'^{\perp}|} W(\mathscr{C}'^{\perp}, P^*, E^*_H)[X']^T = \\
&= \frac{1}{|\mathscr{C}'^{\perp}|} \sum_{J^c\in I(P^*)} A_{J^c,E^*_H}(\mathscr{C}'^{\perp}) X'_{J^c} = \\
&= \frac{1}{|\mathscr{C}'^{\perp}|} \sum_{R'\in Q_{n,s}} t_{R'}(\mathscr{C}'^{\perp}) \prod_{j=1}^{n} z'^{(j)}_{r'_j} = \\
&= \frac{1}{|\mathscr{C}^{\perp}|} T(\mathscr{C}^{\perp}|\Theta_s Z_1,\ldots,\Theta_s Z_n).
\end{aligned}$$

Assim, obtemos a demonstração do Teorema 4.1 apresentado ao final da seção anterior, o qual reapresentamos abaixo:

Teorema 4.1 . *Os T-enumeradores dos códigos lineares mutuamente duais, $\mathscr{C}$ e $\mathscr{C}^{\perp}$ em $Mat_{n,s}(\mathbb{F}_q)$ são relacionados por*

$$T(\mathscr{C}|Z_1,\ldots,Z_n)=\frac{1}{|\mathscr{C}^{\perp}|}T(\mathscr{C}^{\perp}|\Theta_s Z_1,\ldots,\Theta_s Z_n).$$

Além disso conseguimos demonstrar o Teorema 4.2, o qual é dado por:

Teorema 4.2 . *Os H-enumeradores dos códigos lineares mutuamente duais, $\mathscr{C}$ e $\mathscr{C}^{\perp}$ em $Mat_{n,s}(\mathbb{F}_q)$ são relacionados por*

$$H(\mathscr{C}|Z)=\frac{1}{|\mathscr{C}^{\perp}|}H(\mathscr{C}^{\perp}|\Theta_s Z)$$

Demonstração: De fato, como $H(\mathscr{C}|Z)=T(\mathscr{C}|Z,\ldots,Z)$, pelo teorema anterior teremos

$$H(\mathscr{C}|Z)=T(\mathscr{C}|Z,\ldots,Z)=\frac{1}{|\mathscr{C}^{\perp}|}T(\mathscr{C}^{\perp}|\Theta_s Z,\ldots,\Theta_s Z)=\frac{1}{|\mathscr{C}^{\perp}|}H(\mathscr{C}^{\perp}|\Theta_s Z).$$

■

4.2.1 Relações entre T e H-espectro para códigos mutuamente duais

Conseguimos também uma relação entre o T- e H-espectro do código $\mathscr{C}$ e do seu dual $\mathscr{C}^{\perp}$.

Teorema 4.8. *Os T-espectros dos códigos lineares mutuamente duais $\mathscr{C}$ e $\mathscr{C}^{\perp}\subset Mat_{n,s}(\mathbb{F}_q)$ são relacionados por*

$$t_R(\mathscr{C})=\frac{1}{|\mathscr{C}^{\perp}|}\sum_{R'\in Q_{n,s}} t_{R'}(\mathscr{C}^{\perp})\prod_{j=1}^{n}\theta_{r'_j,r_j}$$

Demonstração: De fato, temos que $t_R(\mathscr{C})=A_{\varphi(R),E_H}(\mathscr{C}')$ e pelo Lema 3.5 teremos

$$t_R(\mathscr{C})=A_{\varphi(R),E_H}(\mathscr{C}')=\frac{1}{|\mathscr{C}'^{\perp}|}\sum_{\psi(R')\in I(P^*)}\left(\sum_{u\in\mathscr{C}'^{\perp}\cap S_{\psi(R')}}\left(\sum_{v\in S_{\varphi(R)}}\chi(u\cdot v)\right)\right)=$$

$$=\frac{1}{|\mathscr{C}'^{\perp}|}\sum_{\psi(R')\in I(P^*)}|\mathscr{C}'^{\perp}\cap S_{\psi(R'}|q_{\varphi(R),\psi(R')}=$$

$$=\frac{1}{|\mathscr{C}'^{\perp}|}\sum_{R'\in Q_{n,s}}A_{\psi(R'),E_H^*}(\mathscr{C}'^{\perp})q_{\varphi(R),\psi(R')}.$$

Pelo item (ii) do Teorema 4.7 temos que $q_{\varphi(R),\psi(R')}=\prod_{j=1}^{n}q_{I_{r_j},J^c_{r'_j}}$ e como $q_{I_{r_j},J^c_{r'_j}}=\theta_{r'_j,r_j}$ teremos $q_{\varphi(R),\psi(R')}=\prod_{j=1}^{n}\theta_{r'_j,r_j}$. Assim obtemos

$$t_R(\mathscr{C}) = \frac{1}{|\mathscr{C}'^{\perp}|} \sum_{R' \in Q_{n,s}} A_{\psi(R'),E_H^*}(\mathscr{C}'^{\perp}) q_{\varphi(R),\psi(R')} = \frac{1}{|\mathscr{C}^{\perp}|} \sum_{R' \in Q_{n,s}} t_{R'}(\mathscr{C}^{\perp}) \prod_{j=1}^{n} \theta_{r'_j, r_j}.$$

E temos o resultado desejado. ∎

Teorema 4.9. *Os H-espectros dos códigos lineares mutuamente duais $\mathscr{C}$ e $\mathscr{C}^{\perp} \subset Mat_{n,s}(\mathbb{F}_q)$ são relacionados por*

$$h_R(\mathscr{C}) = \frac{1}{|\mathscr{C}^{\perp}|} \sum_{R' \in Q_{n,s}/S_n} \alpha_R h_{R'}(\mathscr{C}^{\perp}) \sum_{\sigma \in S_n} \prod_{j=1}^{n} \theta_{r_{\sigma(j)}, r'_j},$$

onde α_R é o inverso do número de elementos do estabilizador de R.

Demonstração: De fato, segue da definição 4.2 e do teorema anterior que

$$\begin{aligned}
h_R(\mathscr{C}) &= \sum_{\sigma \in S_n} \alpha_R t_{\sigma R}(\mathscr{C}) = \sum_{\sigma \in S_n} \alpha_R \left(\frac{1}{|\mathscr{C}^{\perp}|} \sum_{R' \in Q_{n,s}} t_{R'}(\mathscr{C}^{\perp}) \prod_{j=1}^{n} \theta_{r_{\sigma(j)}, r'_j} \right) = \\
&= \frac{1}{|\mathscr{C}^{\perp}|} \sum_{\sigma \in S_n} \alpha_R \sum_{R' \in Q_{n,s}/S_n} \left(\sum_{\lambda \in S_n} \alpha_{R'} t_{\lambda R'}(\mathscr{C}^{\perp}) \prod_{j=1}^{n} \theta_{r_{\sigma(j)}, r'_{\lambda(j)}} \right) = \\
&= \frac{1}{|\mathscr{C}^{\perp}|} \sum_{R' \in Q_{n,s}/S_n} \left(\sum_{\lambda \in S_n} \left(\sum_{\sigma \in S_n} \alpha_R \alpha_{R'} t_{\lambda R'}(\mathscr{C}^{\perp}) \prod_{j=1}^{n} \theta_{r_{\sigma(j)}, r'_{\lambda(j)}} \right) \right) = \\
&= \frac{1}{|\mathscr{C}^{\perp}|} \sum_{R' \in Q_{n,s}/S_n} \left(\sum_{\lambda \in S_n} \left(\sum_{\sigma \in S_n} \alpha_R \alpha_{R'} t_{\lambda R'}(\mathscr{C}^{\perp}) \prod_{j=1}^{n} q_{I_{r'_{\lambda(j)}}, J^c_{r_{\sigma(j)}}} \right) \right).
\end{aligned}$$

Note que pela Proposição 3.11 temos que $q_{I_{r'_{\lambda(j)}}, J^c_{r_{\sigma(j)}}} = (q-1)^{|M(I_{r'_{\lambda(j)}})|} q^{|(I_{r'_{\lambda(j)}})_M|} \left(\frac{-1}{q-1}\right)^{|I_{r'_{\lambda(j)}} \cap J^c_{r_{\sigma(j)}}|}$. Como a cardinalidade dos maximais, não maximais e a interseção em $q_{I_{r'_{\lambda(j)}}, J^c_{r_{\sigma(j)}}}$ é invariante pela ação de S_n, teremos $q_{I_{r'_{\lambda(j)}}, J^c_{r_{\sigma(j)}}} = q_{I_{r'_j}, J^c_{r_{\lambda^{-1}\sigma(j)}}}$. Logo, somando sobre todo S_n, o resultado da soma de $\lambda^{-1}\sigma$ é igual ao da soma de σ:

$$\sum_{\sigma} \left(\prod_{j=1}^{n} q_{I_{r'_{\lambda(j)}}, J^c_{r_{\sigma(j)}}} \right) = \sum_{\sigma} \left(\prod_{j=1}^{n} q_{I_{r'_j}, J^c_{r_{\lambda^{-1}\sigma(j)}}} \right) = \sum_{\sigma} \left(\prod_{j=1}^{n} q_{I_{r'_j}, J^c_{r_{\sigma(j)}}} \right).$$

Portanto teremos:

$$\begin{aligned}
h_R(\mathscr{C}) &= \frac{1}{|\mathscr{C}^{\perp}|} \sum_{R' \in Q_{n,s}/S_n} \left(\sum_{\lambda \in S_n} \left(\sum_{\sigma \in S_n} \alpha_R \alpha_{R'} t_{\lambda R'}(\mathscr{C}^{\perp}) \prod_{j=1}^{n} q_{I_{r'_j}, J^c_{r_{\sigma(j)}}} \right) \right) = \\
&= \frac{1}{|\mathscr{C}^{\perp}|} \sum_{R' \in Q_{n,s}/S_n} \left(\sum_{\sigma \in S_n} \alpha_R \sum_{\lambda \in S_n} \alpha_{R'} t_{\lambda R'}(\mathscr{C}^{\perp}) \prod_{j=1}^{n} \theta_{r_{\sigma(j)}, r'_j} \right) = \\
&= \frac{1}{|\mathscr{C}^{\perp}|} \sum_{R' \in Q_{n,s}/S_n} \left(\sum_{\sigma \in S_n} \alpha_R h_{R'}(\mathscr{C}^{\perp}) \prod_{j=1}^{n} \theta_{r_{\sigma(j)}, r'_j} \right) = \\
&= \frac{1}{|\mathscr{C}^{\perp}|} \sum_{R' \in Q_{n,s}/S_n} \alpha_R h_{R'}(\mathscr{C}^{\perp}) d\, s \sum_{\sigma \in S_n} \prod_{j=1}^{n} \theta_{r_{\sigma(j)}, r'_j}.
\end{aligned}$$

E temos o resultado desejado. ∎

Considerações Finais

Neste trabalho, nosso objetivo foi estudar as Identidades de MacWilliams para códigos poset e em seguida relacionar os trabalhos [3] e [2]. Para este fim, primeiramente apresentamos os conceitos básicos sobre códigos lineares e posets a fim de termos ferramentas para trabalhar com as identidades de MacWillams. Apresentamos tais identidades para o caso de códigos lineares em espaços de Hamming e então mostramos que as mesmas só valem no caso de posets quando o poset P é hierárquico.

Começamos então a estudar o trabalho de Choi et al. [2], o qual deriva tais identidades com relação a relações de equivalência no conjunto de ideais de ordem do poset P. Apresentamos então, três relações de equivalência em $I(P)$ bem como, condições suficientes e necessárias para que estas relações de equivalência sejam de tipo MacWilliams, onde tais identidades, segundo essa caracterização, foram apresentadas na forma de matrizes, P_E e Q_{E^*}, sendo as entradas de tais matrizes explicitadas.

Um resultado importante que encontramos neste estudo foi que, no caso em que a relação de equivalência que leva em conta os isomorfismos entre ideais do poset P é uma relação de equivalência de tipo MacWilliams, então tal relação é, na verdade, a mesma que a relação de equivalência dos automorfismos do poset P, ou seja, que todo isomorfismo, neste caso, é uma extensão de um automorfismo.

Em seguida passamos a estudar o trabalho de Dougherty e Skriganov [3], relacionando este, com os resultados obtidos no estudo de [2], a fim de tentar obter uma prova mais simples para os resultados em [3]. Para isso, conseguimos relacionar a ρ-métrica com a P-métrica e os conceitos referentes à tais métricas através de algumas isometrias obtendo assim todos os resultados apresentados em [3] utilizando-se os resultados apresentados para posets.

Neste processo, vimos que a ρ-métrica para o espaço das matrizes $n \times s$ com entradas em $\mathbb{F}_q$, pode ser identificada com a P-métrica, onde o poset P é uma união disjunta de n cadeias de mesmo comprimento, neste caso, comprimento s. Com isso conseguimos mostrar que a matriz Θ_s apresentada em [3], a qual é utilizada para relacionar os T e H-enumeradores, nada

mais é que a matriz P_E ou Q_{E^*} para a primeira cadeia do poset P, e que neste caso tais matrizes são iguais.

Assim, conseguimos outro resultado muito importante: mostramos que, neste caso, ao invés de precisarmos encontrar todas as entradas da matriz P_E ou Q_{E^*}, as quais são da forma

$$p_{\overline{J^c},\overline{I}} = (q-1)^{|M(J^c)|} q^{|(J^c)_M|} \sum_{\substack{K^c \in \overline{J^c}, \\ I_M \cap K^c = \emptyset}} \left(\frac{-1}{q-1}\right)^{|I \cap K^c|} \quad \text{para a matriz } P_E$$

e

$$q_{\overline{I},\overline{J^c}} = (q-1)^{|M(I)|} q^{|I_M|} \sum_{\substack{K \in \overline{I}, \\ (J^c)_M \cap K = \emptyset}} \left(\frac{-1}{q-1}\right)^{|J^c \cap K|} \quad \text{para a matriz } Q_{E^*},$$

e geram um gasto computacional elevado para n grande, mostramos que basta encontramos tais entradas para os ideais referentes à primeira cadeia, que são poucas comparadas ao número de entradas total, e as demais são obtidas através de uma multiplicação de algumas dessas entradas. Assim, conseguimos reduzir consideravelmente o trabalho e consequentemente o gasto, para determinar tais matrizes neste caso.

Por fim ficam algumas perguntas: a relação encontrada para determinar as demais entradas das matrizes P_E e Q_E^* para este poset, pode ser generalizada para outros posets? Como identificar facilmente se um poset é um complemento de isomorfismos? Existem outras relações de equivalência de tipo MacWilliams?

As respostas à tais perguntas ficam como sugestões para trabalhos futuros.

Apêndice A

Ações de Grupos e Fórmula de inversão de Moebius

Neste apêndice veremos alguns resultados sobre ações de grupos utilizadas ao longo do trabalho e também, ao final deste, a demonstração da fórmula de inversão de Moebius.

Ações de Grupos

Denotemos por G um grupo e X um conjunto não vazio.

Definição A.1. *Um grupo G age em um conjunto X quando existe uma função $\phi : G \times X \to X$, chamada ação de $g \in G$ em $x \in X$, satisfazendo:*

(A1) $\phi(g_1, \phi(g_2, x)) = \phi(g_1 g_2, x), \quad \forall g_1, g_2 \in G, \ \forall x \in X.$

(A2) $\phi(e, x) = x, \ \forall x \in X$ *($e \in G$ é a identidade de G).*

Afim de simplificarmos a notação denotaremos $\phi(g, x)$ por $g \cdot x$. Logo as propriedades (A1) e (A2) ficarão:

(A1) $g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x, \quad \forall g_1, g_2 \in G, \ \forall x \in X$

(A2) $e \cdot x = x, \ \forall x \in X$ ($e \in G$ é a identidade de G)

Diremos que dois elementos x e $x' \in X$ são equivalentes sob a ação de G se existe $g \in G$ tal que $g x = x'$.

Se G é um grupo multiplicativo e $X = G$, a função $(g, x) \mapsto g x g^{-1}$ define uma ação de G em G chamada ação por conjugação.

Definição A.2. *Se um grupo G age em um conjunto X e $x \in X$, o subconjunto de X,*

$$\mathcal{O}(x) = \{g \cdot x : g \in G\},$$

é chamado de órbita de x.

Note que a órbita de $x \in X$ é a classe de equivalência de x.

Lema A.1. *Seja G um grupo agindo em um conjunto X. Então*

(a) $X = \bigcup_{x \in X} \mathcal{O}(x)$.

(b) *Se $x, y \in X$, ou $\mathcal{O}(x) \cap \mathcal{O}(y) = \emptyset$ ou $\mathcal{O}(x) = \mathcal{O}(y)$.*

Demonstração:

(a) Como $x \in \mathcal{O}(x)$ temos que $X = \bigcup_{x \in X} \mathcal{O}(x)$.

(b) Suponha que $z \in \mathcal{O}(x) \cap \mathcal{O}(y)$, então $z = g_1 \cdot x = g_2 \cdot y$, para certos $g_1, g_2 \in G$. Logo, por (A1) temos que $x = (g_1^{-1} g_2) \cdot y$ e assim $x \in \mathcal{O}(y)$. Por outro lado, $y = (g_2^{-1} g_1) \cdot x$ logo $y \in \mathcal{O}(x)$ e temos o resultado desejado.

■

Chamaremos de conjunto de representantes de órbitas, denotado por T, um subconjunto de X que toma um representante de cada órbita. Assim, pelo Lema A.1, temos que $X = \overset{\circ}{\bigcup_{x \in T}} \mathcal{O}(x)$, onde $\overset{\circ}{\bigcup}$ representa a união disjunta.

Denotaremos ainda o conjunto das órbitas da ação de G em X por $G\backslash X$. Assim, é fácil ver que temos uma bijeção entre T e $G\backslash X$ dada por $x \in T \longmapsto \mathcal{O}(x) \in G\backslash X$.

Definição A.3. *Se G age em um conjunto X e $x \in X$, o subgrupo de G*

$$G_x = \{g \in G : g \cdot x = x\}$$

é chamado estabilizador de x ou grupo de isotropia de x.

Teorema A.2 (Lagrange)**.** *Sejam G um grupo finito e H um subgrupo de G. Então $|G| = |H||T|$, onde T é um conjunto de representantes de órbitas para a ação de H em G dada pela multiplicação pela esquerda.*

Demonstração: Tomemos $X = G$. Assim, a função dada por $h \cdot x = hx$, para todo $h \in H$ e todo $x \in X$, é uma ação de H sobre X. A função $\sigma : H \longrightarrow \mathcal{O}(x)$ definida por $\sigma(h) = hx$ é uma bijeção.

De fato, é fácil ver que σ é injetora. Além disso, se $x' \in \mathcal{O}(x)$, então $x' = hx$ para algum $h \in H$, logo $x' = \sigma(h)$.

Assim temos que $|H| = |\mathcal{O}(x)|$ para todo $x \in X$. Como $X = \overset{\circ}{\bigcup_{x \in T}} \mathcal{O}(x)$ teremos

$$|G| = |X| = |\overset{\circ}{\bigcup_{x \in T}} \mathcal{O}(x)| = \sum_{x \in T} |\mathcal{O}(x)| = \sum_{x \in T} |H| = |T||H|.$$

■

Definição A.4. *Sejam G um grupo, H um subgrupo de G e $x \in G$, o subconjunto de G*

$$Hx = \{hx : h \in H\}$$

é chamado de classe lateral à esquerda de H em G.

Analogamente definimos a classe lateral à direita de H em G.

Quando o conjunto das classes laterais de H em G for finito, dizemos que H é um subgrupo de índice finito em G, e o número de classes laterais é chamado o *índice* de H em G, e denotado $|G : H|$.

Teorema A.3 (Teorema da Órbita e Estabilizador)**.** *Se um grupo finito G age em um conjunto X, então o número de pontos na órbita de um ponto $x \in X$ é o índice de G_x em G, $|G : G_x|$.*

Demonstração: De fato, da definição de órbita temos que esta consiste dos pontos gx, enquanto que $g_1 x = g_2 x \Leftrightarrow g_2^{-1} g_1 \in G_x$, isto é, se, e somente se as classes laterais $g_2 G_x$ e $g_1 G_x$ são iguais. Assim, a função definida por $gG_x \longmapsto gx$ é bijetora e temos $|G : G_x| = |\mathcal{O}(x)|$. ■

Note ainda que $|T| = |G : G_x| = |\mathcal{O}(x)|$, assim, pelo Teorema de Lagrange temos

$$|G| = |T||G_x| = |G : G_x||G_x| = |\mathcal{O}(x)||G_x| \quad \text{logo} \quad |\mathcal{O}(x)| = \frac{|G|}{|G_x|}.$$

Em particular, com isso podemos escrever o Teorema de Lagrange em sua forma usual:

Teorema A.4 (Lagrange)**.** *Sejam G um grupo finito e H um subgrupo de G. Então $|G| = |H||G : H|$.*

Com estes resultados finalizamos a parte referente à ações de grupos utilizada no trabalho.

Fórmula de Inversão de Moebius

Vejamos agora o resultado utilizado no Teorema 3.12 sobre fórmula de inversão de Moebius.

Primeiramente sejam P um poset finito e denotemos por $\mathrm{Int}(P)$ o conjunto de intervalos de P, $[x,y]=\{z\in P; x\leq z\leq y\}$ (lembrando que o conjunto vazio não é um intervalo). Seja $\mathbb{F}$ um corpo. Se $f:\mathrm{Int}(P)\longrightarrow\mathbb{F}$, então escrevemos $f(x,y)$ para $f([x,y])$.

Definição A.5. *A álgebra de Incidência $I(P,\mathbb{F})$ de P sobre $\mathbb{F}$ é a $\mathbb{F}$-álgebra de todas as funções $f:Int(P)\longrightarrow\mathbb{F}$ (com a estrutura usual de espaço vetorial sobre $\mathbb{F}$), onde a multiplicação (ou convolução) é definida por*

$$(fg)(x,y)=\sum_{x\leq z\leq y} f(x,z)g(z,y).$$

Note que a soma acima é finita pois P é finito.

A identidade nessa $\mathbb{F}$-álgebra é dada por

$$\delta(x,y)=\begin{cases} 1, & se \quad x=y \\ 0, & se \quad x\neq y \end{cases}.$$

Assim, $f\in I(P,\mathbb{F})$ tem inversa a direita se $fg=\delta$. Logo devemos ter $f(x,x)g(x,x)=1 \ \ \forall x\in P$, portanto $f(x,x)\neq 0 \ \ \forall x\in P$ e assim $g(x,x)$ está bem definida pois $g(x,x)=\frac{1}{f(x,x)}$. Por outro lado $fg(x,y)=\delta(x,y)=0$ para $x\neq y$. Logo, tomando $[x,y]$ contendo apenas x e y com $x\neq y$ teremos

$0=fg(x,y)=\sum_{x\leq z\leq y} f(x,z)g(z,y)=f(x,x)g(x,y)+f(x,y)g(y,y)$ portanto

$g(x,y)=-f(x,x)^{-1}f(x,y)g(y,y)$ que está bem definido pois $f(x,x)\neq 0$ e $g(y,y)$ é bem definido.

Assim, por indução recursiva no tamanho do intervalo, que é finito, temos que g está bem definida e teremos

$$fg(x,y)=0\Leftrightarrow\sum_{x\leq z\leq y} f(x,z)g(z,y)=0\Leftrightarrow f(x,x)g(x,y)+\sum_{x\prec z\leq y} f(x,z)g(z,y)=0\Leftrightarrow$$
$$g(x,y)=-f(x,x)^{-1}\sum_{x\prec z\leq y} f(x,z)g(z,y).$$

Analogamente, para a inversa à esquerda teremos:

$$gf(x,y)=0 \Leftrightarrow \sum_{x\preceq z\preceq y} g(x,z)f(z,y)=0 \Leftrightarrow \left(\sum_{x\preceq z\prec y} g(x,z)f(z,y)\right)+g(x,y)f(y,y)=0 \Leftrightarrow$$
$$g(x,y)=-f(y,y)^{-1}\sum_{x\preceq z\prec y} g(x,z)f(z,y).$$

Logo provamos que f tem inversa se e somente se $f(x,x)\neq 0$ para todo $x\in P$.

Agora consideremos a função zeta $\zeta\in I(P,\mathbb{F})$ definida por $\zeta(x,y)=1$, para todo $x\preceq y$ em P.

Logo temos $\zeta(x,x)\neq 0 \ \ \forall x\in P$ e portanto existe a inversa de ζ em $I(P,\mathbb{F})$, chamada função de Moebius de P e denotada por μ. Utilizando a fórmula para inversa à esquerda, temos que μ é definida por

$$\begin{aligned} &\mu(x,x)=1, && \forall x\in P \\ &\mu(x,y)=-\sum_{x\preceq z\prec y}\mu(x,z), && \forall x\prec y \ \text{ em } \ P. \end{aligned}$$

Assim, conseguimos o seguinte teorema:

Teorema A.5 (Fórmula da inversão de Moebius)**.** *Seja P um poset finito. Sejam $f,g:P\longrightarrow\mathbb{C}$. Então*

$$g(x)=\sum_{y\preceq x} f(y), \ \ \forall x\in P \Leftrightarrow$$

$$f(x)=\sum_{y\preceq x} g(y)\mu(y,x), \ \ \forall x\in P.$$

Demonstração: O conjunto $\mathbb{C}^P$ de todas as funções $P\longrightarrow\mathbb{C}$ forma um espaço vetorial no qual $I(P,\mathbb{C})$ age (à direita) como uma álgebra de transformações lineares, isto é, $\mathbb{C}^P$ é um $I(P,\mathbb{C})$-módulo à direita. A ação é dada por

$$(fh)(x)=\sum_{y\preceq x} f(y)h(y,x),$$

onde $f\in\mathbb{C}^P$ e $h\in I(P,\mathbb{C})$.

Um estudo mais detalhado sobre módulos pode ser encontrado em [13].

Assim, consideremos a função zeta $\zeta\in I(P,\mathbb{C})$, temos então que

$$g(x)=\sum_{y\preceq x} f(y) \Leftrightarrow g=f\zeta \Leftrightarrow g\mu=f\zeta\mu \Leftrightarrow g\mu=f$$

e temos o resultado desejado. ■

Note que se consideramos $P = X$ como um conjunto com relação de ordem dada pela inclusão, teremos pelo teorema acima que

$$g(A) = \sum_{B \subseteq A} f(B), \quad \forall A \subseteq X \Leftrightarrow$$
$$f(A) = \sum_{B \subseteq A} g(B)\mu(B,A), \quad \forall A \subseteq X.$$

Provemos por indução, que neste caso, $\mu(B,A) = (-1)^{|A|-|B|}$.
De fato, temos que se $B = A$ então $\mu(B,A) = \mu(A,A) = 1 = (-1)^0 = (-1)^{|A|-|A|}$.
Note que

$$\sum_{Z \subseteq X} (-1)^{|Z|} = \sum_{l=0}^{|X|} \left(\sum_{\substack{Z \subseteq X \\ |Z|=l}} (-1)^{|Z|} \right) = \sum_{l=0}^{|X|} \binom{|X|}{l} (-1)^l = (1-1)^{|X|} = 0. \tag{A.1}$$

Além disso, temos que $(-1)^k = (-1)^{-k}$.
Suponha então que para $B \subseteq C \subset A$ vale a igualdade $\mu(B,C) = (-1)^{|B|-|C|}$, logo teremos

$$\begin{aligned} \mu(B,A) &= -\sum_{B \subseteq C \subset A} \mu(B,C) = -\sum_{B \subseteq C \subset A} (-1)^{|B|-|C|} = \\ &= -\sum_{B \subseteq C \subset A} (-1)^{|B|}(-1)^{-|C|} = -\left(\sum_{B \subseteq C \subset A} (-1)^{|C|} \right)(-1)^{|B|}. \end{aligned} \tag{A.2}$$

Note porém que

$$\left(\sum_{B \subseteq C \subseteq A} (-1)^{|C|} \right)(-1)^{|B|} = \left(\sum_{l=0}^{|A|-|B|} \left(\sum_{\substack{B \subseteq C \subseteq A \\ |C|-|B|=l}} (-1)^{|C|} \right) \right)(-1)^{|B|} = \sum_{l=0}^{|A|-|B|} \left(\sum_{\substack{B \subseteq C \subseteq A \\ |C|-|B|=l}} (-1)^{|C|-|B|} \right) =$$
$$= \sum_{l=0}^{|X|} \left(\sum_{\substack{Z \subseteq X \\ |Z|=l}} (-1)^{|Z|} \right), \quad \text{onde} \quad X = A - B \quad \text{e} \quad Z = C - B$$

e por A.1 temos $\left(\sum_{B\subseteq C\subseteq A}(-1)^{|C|}\right)(-1)^{|B|}=0$, logo obtemos

$$0=(-1)^{|A|}(-1)^{|B|}+\left(\sum_{B\subseteq C\subset A}(-1)^{|C|}\right)(-1)^{|B|},$$

e assim $-\left(\sum_{B\subseteq C\subset A}(-1)^{|C|}\right)(-1)^{|B|}=(-1)^{|A|-|B|}$ e substituindo em A.2 teremos $\mu(B,A)=(-1)^{|A|-|B|}$ como desejávamos.

Note que este é o resultado utilizado na demonstração do Teorema 3.12.

Referências Bibliográficas

[1] BRUALDI, R. A., GRAVES, J. S., AND LAWRENCE, K. M. Codes with a poset metric. *Discrete Math. 147*, 1-3 (Dec. 1995), 57–72.

[2] CHOI, S., HYUN, J. Y., KIM, H. K., AND OH, D. Y. MacWilliams-type equivalence relations. *ArXiv e-prints* (May 2012).

[3] DOUGHERTY, S. T., AND SKRIGANOV, M. M. Macwilliams duality and the rosenbloom-tsfasman metric. *Moscow Mathematical Journal 2*, 1 (2002), 81–97.

[4] HAMMING, R. W. Error detecting and error correcting codes. *BELL SYSTEM TECHNICAL JOURNAL 29*, 2 (1950), 147–160.

[5] HEFEZ, A., AND VILLELA, M. *Códigos corretores de erros*. Série de computação e Matemática. Instituto de Matemática Pura e Aplicada, 2008.

[6] HUFFMAN, W., AND PLESS, V. *Fundamentals of Error-Correcting Codes*. Cambridge, Ma University Press, 2003.

[7] KIM, H. K., AND OH, D. Y. A classification of posets admitting the macwilliams identity. *IEEE Trans. Inf. Theor. 51*, 4 (Apr. 2005), 1424–1431.

[8] LANE, S., AND BIRKHOFF, G. *Algebra*. Chelsea Publishing Series. Chelsea Publishing Company, 1999.

[9] LIDL, R., AND NIEDERREITER, H. *Finite Fields*. No. v. 20,pt. 1 in Encyclopedia of Mathematics and its Applications. Cambridge University Press, 1997.

[10] MACWILLIAMS, F., AND SLOANE, N. *The Theory of Error-Correcting Codes*, 2nd ed. Northholland Publishing Company, 1978.

[11] MARTIN, P. A. *Grupos, corpos e teoria de galois*, vol. 2. Editora Livraria da Física, 2010.

[12] ROSENBLOOM, M, Y. T. M. A. Codes for the m-metric. *Probl. Peredachi Inf. 33*, 1 (1997), 55 – 63.

[13] ROTMAN, J. *Advanced Modern Algebra*. Prentice Hall, 2002.

[14] SHANNON, C. E. A mathematical theory of communication. *Bell System Technical Journal 27* (1948), 379–423.

[15] SKRIGANOV, M. M. Coding Theory and Uniform Distributions. *Algebra i Analiz 13*, 2 (Sept. 2001), 191 – 239.

[16] STANLEY, R. *Enumerative Combinatorics*. No. v. 1 in Cambridge studies in advanced mathematics. Cambridge University Press, 2002.