Universidade Estadual de Campinas

Instituto de Matemática, Estatística e Computação Científica

Departamento de Matemática

Dissertação de Mestrado

Identidades de MacWilliams para Métricas Poset-Block

Jerry Anderson Pinheiro

Orientador: Prof. Dr. Marcelo Firer

Campinas-SP

Setembro, 2011

Identidades de MacWilliams para Métricas Poset-Block

Este exemplar corresponde à redação final da dissertação devidamente corrigida e defendida por **Jerry Anderson Pinheiro** e aprovada pela comissão julgadora.

Campinas, 23 de setembro de 2011.

Prof. Dr. **Marcelo Firer**
Orientador

Banca Examinadora:

Prof. Dr. Cristiano Torezzan (FCA - UNICAMP)

Prof. Dr. Marcelo Firer (IMECC - UNICAMP)

Prof. Dr. Marcelo Muniz Silva Alves (DM - UFPR)

Dissertação apresentada ao Instituto de Matemática, Estatística e Computação Científica, **UNICAMP**, como requisito parcial para obtenção de Título de **Mestre em Matemática**.

FICHA CATALOGRÁFICA ELABORADA POR
MARIA FABIANA BEZERRA MÜLLER - CRB8/6162
BIBLIOTECA DO INSTITUTO DE MATEMÁTICA, ESTATÍSTICA E
COMPUTAÇÃO CIENTÍFICA - UNICAMP

Pinheiro, Jerry Anderson
P655i Identidades de MacWilliams para métricas Poset-Block / Jerry Anderson Pinheiro. - Campinas, SP:[s.n.], 2011.

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

1. MacWilliams, Identidade de. 2. Códigos de controle de erros (Teoria da Informação). I. Firer, Marcelo, 1961. II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. III. Título.

Título em inglês: MacWilliams identity for Poset-Block metrics.

Palavras-chave em inglês (Keywords):

1. Error-Correcting Codes (Information Theory).
2. MacWilliams identity.

Área de concentração: Matemática

Titulação: Mestre em Matemática

Banca examinadora:

1. Marcelo Firer [Orientador]
2. Marcelo Muniz Silva Alves
3. Cristiano Torezzan

Data da defesa: 23-09-2011

Programa de Pós Graduação: Matemática

Dissertação de Mestrado defendida em 23 de setembro de 2011 e aprovada

Pela Banca Examinadora composta pelos Profs. Drs.

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

Prof. (a). Dr (a). CRISTIANO TOREZZAN

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

Agradecimentos

Agradeço a Deus por me dar força para enfrentar e superar os momentos difíceis, além de mostrar o caminho nas horas incertas.

Agradeço aos meus pais Zilton e Adiles, pelo apoio incondicional, pela ajuda financeira extra, bem vinda nos meses em que a bolsa não suportou os gastos e durante o período de um ano do mestrado no qual fiquei sem receber bolsa.

Agradeço aos meus companheiros de república, em especial ao Cleber e ao Félix, pela convivência durante esses dois anos, pelos momentos divertidos, pelas festas e pelos momentos de descontração.

Agradeço a todos meus amigos de Campinas, em especial ao Marcos, ou "Marquinhos", parceiro nas horas de ir ao Museu de Ciências encontrar com o orientador. Agradeço ao Campello pelas construtivas discussões sobre teoria da informação. Não posso deixar de agradecer o pessoal do Laboratório de Matemática Discreta e Códigos, em especial, Elen, Kênia e Cecília pela companhia durante as refeições no bandejão, durante a hora do café e pela grande amizade que cultivamos.

Agradeço a todos os professores da Unicamp e da Unioeste que participaram de alguma forma da minha formação acadêmica. Agradeço ao Luciano Panek pela motivação dada, em especial, meus sinceros agradecimentos ao meu orientador Marcelo Firer, pela confiança depositada e pelos ensinamentos.

Agradeço a Capes pelo apoio financeiro dado durante os dois últimos semestres do mestrado.

Resumo

Em 1963, F. J. MacWilliams desenvolveu as chamadas identidades de MacWilliams, que estabelecem, em particular, relações entre a distribuição de pesos de códigos possuindo alta taxa de informação e códigos com baixa dimensão. Consideramos neste trabalho a família de métricas poset-block, uma pouco explorada generalização tanto das métricas de bloco quanto das métricas poset, e consequentemente da clássica métrica de Hamming. Efetuamos uma descrição detalhada dos espaços munidos com tais métricas com ênfase na teoria de códigos e em seguida tratamos do problema que surge naturalmente neste contexto: a caracterização dos espaços que admitem uma identidade do tipo MacWilliams, ou seja, a classificação das métricas que permitem relacionar unicamente o espectro de um código com o de seu dual. A principal técnica utilizada nesta classificação é a teoria de caracteres sobre corpos finitos, incluindo aí a transformada de Hadamard, a fórmula da soma discreta de Poisson e as relações de ortogonalidade existente entre caracteres. Tal técnica foi proposta inicialmente por F. J. MacWilliams e utilizada posteriormente por H. K. Kim e D. H. Oh na classificação das métricas poset que admitem identidades do tipo MacWilliams. Nosso principal objetivo é portanto classificar os espaços poset-block que admitem uma identidade do tipo MacWilliams. Como consequência desta classificação, através dos polinômios de Krawtchouk, obteremos expressões explícitas para estas identidades.

Palavras-chave: Códigos Corretores de Erros (Teoria da Informação), métricas poset-block, identidade de MacWilliams.

Abstract

In 1963, F. J. MacWilliams developed the so-called MacWilliams identities, which establish, in particular, relations between the weight distribution of codes having high information rate and codes with low dimension. In this work we consider the family of poset-block metrics, a little explored generalization of both error-block and poset metrics, and hence also of the classic Hamming metric. We perform a detailed description of the spaces equipped with such metrics with emphasis in the coding theory and then we treat the problem that arises naturally in this context: the characterization of the poset-block metrics that admit a MacWilliams-type identity, in other words, the classification of metrics that allow to relate uniquely the spectrum of a code with the spectrum of its dual. The main technique used in this classification is the theory of characters over finite fields, including the Hadamard transform, the discrete Poisson summation formula and the orthogonality relations between characters. Such techniques were proposed initially by F. J. MacWilliams and used posteriorly by H. K. Kim and D. H. Oh in the classification of the metrics that admit a type of MacWilliams identity. Our main goal is therefore to classify the poset-block spaces that admit a MacWilliams type identity. As consequence of this classification, through the Krawtchouk polynomials, we will obtain explicit expressions for those identities.

Keywords: Error-Correcting Codes (Information Theory), poset-block metrics, MacWilliams identity.

Lista de Notações

$[m] = \{1, \cdots, m\}$

$\mathscr{C}_i = \{u \in \mathscr{C} : \widetilde{u^{i+1}} = 0 \in \mathbb{F}_q^{\widehat{b_i}}\}$

$\mathscr{C}_i^0 = \{u \in \mathscr{C}_i : u^i = 0 \in \mathbb{F}_q^{b_i}\}$ e $\mathscr{C}_i^1 = \{u \in \mathscr{C}_i : u^i \neq 0 \in \mathbb{F}_q^{b_i}\}$

$\gamma_i = (q^{d_i} - 1)$

$\Gamma_P^i = \{r_i + 1, \cdots, r_i + m_1\}$

$\pi(j) = k_j$ e $k_0 = 0$

$\widehat{b_i} = n - (b_0 + b_1 + \cdots + b_i)$ e $b_0 = 0$

$\widehat{m_i} = m - (m_0 + m_1 + \cdots + m_i)$ e $m_0 = 0$

$\widetilde{u^{i+1}} = (u^{i+1}, \cdots, u^t) \in \mathbb{F}_q^{\widehat{b_i}}$

$a_i(x) = q^{\widehat{b_i}} \left(\frac{1+\gamma_i x}{x}\right)^{m-\widehat{m_i}} (1-x)^{\widehat{m_{i-1}}}$

$b_i = \sum_{j \in \Gamma_P^i} k_j$,

$c_i(x) = x^{\widehat{m_i}} q^{\widehat{b_i}} \left(\frac{1-x}{Q_i(x)}\right)^{m_i}$

$d_i = \pi(r_i + j) = k_{(r_i+j)}$ para todo $j \in \{1, \cdots, m_i\}$

$g_j = \sum_{i=j+1}^{t} c_i(x) z_i$, se $0 \leqslant j \leqslant t-1$ e $g_t = 0$

$h_j = \sum_{i=j}^{t} z_i x^{\widehat{m_i}} q^{\widehat{b_i}}$ se $1 \leqslant j \leqslant t$ e $h_0 = \sum_{i=1}^{t} z_i x^{\widehat{m_i}} q^{\widehat{b_i}}$

$Q_i(x) = \left(\frac{1-x}{1+\gamma_i x}\right)$

Se $i \neq 0$, $r_i = m_0 + m_1 + \cdots + m_{i-1}$

Sumário

Introdução

Em 1948, com a publicação do célebre artigo "A Mathematical Theory of Communication" [25], Claude E. Shannon desenvolveu um modelo matemático para a teoria de comunicação. Um sistema de comunicação pode ser esquematizado de forma resumida como na figura abaixo:

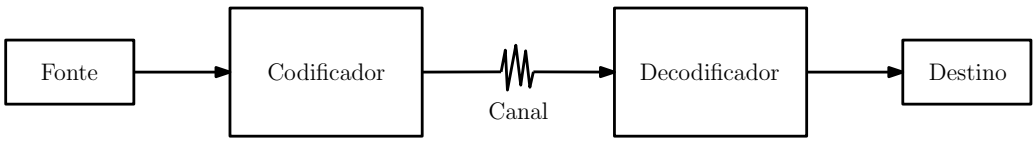


Figura 1: Estrutura de um sistema de comunicação.

A *fonte* é a parte do processo de comunicação responsável por gerar as mensagens que deverão ser enviadas a um destinatário. O *codificador* tem a função de codificar a informação de maneira que ela possa ser enviada por um meio, tal meio é chamado de *canal* e a informação codificada é chamada de *código de fonte*. O canal representa um modelo matemático do meio físico pelo qual o código de canal trafega, por exemplo: fibra óptica, wireless, etc. Para que o destinatário possa interpretar a mensagem gerada pela fonte, é necessário um processo de decodificação, transformando assim o código de canal em uma mensagem que deverá ser entregue ao destinatário, tal função é desempenhada pelo *decodificador*.

Através do meio pelo qual a mensagem codificada trafega, é possível e esperado que hajam *ruídos* (tais ruídos resultam em interferência na transmissão e consequentemente em erros na recepção do código de canal). O estudo da teoria de códigos consiste portanto em transformar a mensagem em código de canal, detectar e corrigir erros na recepção e em decodificar o código de canal.

Como ponto de partida para a criação de um código corretor de erros, tomamos um conjunto finito A chamado de *alfabeto*. Um *código corretor de erros* é um subconjunto de A^n, ou seja,

é um subconjunto das *palavras* de comprimento n geradas pelo alfabeto A. Os elementos do código são chamados de *palavras-código*. Em particular, se o alfabeto é um corpo finito $\mathbb{F}_q$, um subespaço vetorial de $\mathbb{F}_q^n$ é chamado de *código linear*, tais códigos são significativamente importantes nessa teoria pois permitem uma fácil implementação.

No processo de codificação de uma mensagem, acrescentamos redundância para que possamos detectar os erros ocorridos. Uma medida para a quantidade de informação contida num código $\mathscr{C}$, e consequentemente da quantidade de redundância utilizada no código, é a *taxa de informação*. Sendo $R = (\log_q M)/n$, onde q é a cardinalidade do alfabeto, n é o comprimento das palavras e M é a quantidade de mensagens da fonte, dizemos que a taxa de informação do código $\mathscr{C}$ é R dígitos por palavra-código. Em geral, buscamos construir códigos eficientes que possuem a maior taxa de informação possível.

Sendo $\mathbb{F}_q^n$ o espaço vetorial das n-uplas sobre o corpo finito $\mathbb{F}_q$, a decodificação é feita por máxima verossimilhança, considerando apenas a estrutura probabilística do canal, ou seja, interpreta-se uma mensagem recebida como sendo a palavra código mais provável de ter sido enviada. Este tipo de decodificação pode ser definido em termos métricos, considerando-se a *métrica de Hamming*, apresentada em [5] por R. Hamming: interpreta-se a mensagem recebida como sendo a palavra código que difere desta em uma quantidade mínima de coordenadas. Devido ao interesse em generalizar problemas clássicos da teoria de códigos e aplicações em criptografia (veja, [20] e [4]), em meados da década de 90, surgiram novas famílias de métricas com o objetivo de serem utilizadas no contexto de códigos corretores de erros. Dentre essas famílias estão as métricas poset e as métricas de bloco. Em 2008, Firer, *et al* [1] apresentaram a família de métricas poset-block que generaliza tanto as famílias de métricas poset quanto as de métricas de bloco e consequentemente a métrica de Hamming. Muito da teoria clássica tem sido generalizada para códigos em espaços munidos com essas métricas, como pode ser visto por exemplo em [10], [15] [9] e [8].

Misturando as métricas poset e de bloco, obtemos espaços com características métricas particulares surgindo um amplo campo de pesquisa, com questões como, por exemplo, a classificação dos códigos perfeitos. Tais problemas surgem pois as métricas poset e de bloco possuem efeitos opostos nas distâncias: as métricas de bloco diminuem as distâncias quando aumentamos a dimensão dos blocos e as métricas poset aumentam as distâncias quando aumentamos as relações do poset.

Ao se considerar apenas códigos lineares, buscar códigos eficientes possuindo alta taxa de informação é equivalente a maximizar a dimensão do código pois, nesse caso $R = k/n$ onde k é a dimensão do código. Neste contexto é natural que o código dual possua dimensão baixa. Portanto a busca por relações entre invariantes de um código e de seu dual é um problema de valor singular, pois de modo geral é mais fácil determinar os invariantes de códigos de dimensão baixa. Uma dessas relações foi proposta em [17] por F. J. MacWilliams, permitindo determinar a *distribuição de pesos* de um código através da distribuição de seu dual. Estas relações recebem o nome de *Identidades de MacWilliams*. Com o surgimento de novas métricas aplicadas a teoria de códigos, pesquisadores tem se esforçado para expressar identidades do tipo MacWilliams (identidades que estabelecem relações entre a distribuição de pesos de um código e de seu dual) nessas novas famílias de métricas, tal interesse se deve pela importância prática da distribuição de pesos de um código, pois permite por exemplo calcular a probabilidade de erro do código. Em 2005, Kim e Oh [12] mostraram que para um espaço admitir uma identidade do tipo MacWilliams é necessário e suficiente que o poset (conjunto parcialmente ordenado) possua uma ordem *hierárquica*. Neste trabalho, estenderemos este resultado para as instâncias que ainda permanecem abertas, as métricas poset-block (e métricas de bloco como caso particular).

A organização do trabalho é esquematizada da seguinte maneira: No Capítulo 1 descrevemos alguns conceitos de conjuntos parcialmente ordenados necessários e posteriormente definimos as métricas poset-block efetuando uma descrição dos espaços munidos com tais métricas. No Capítulo 2, desenvolvemos a teoria de códigos com base nas métricas poset-block, apresentando os conceitos de distribuição de pesos e demonstrando a Identidade de MacWilliams clássica (para espaços de Hamming). No Capítulo 3, estabelecemos as condições necessárias e suficientes para que um poset-block admita uma identidade do tipo MacWilliams e em seguida explicitamos tais identidades. Para o desenvolvimento dos Capítulos 2 e 3, necessitamos da teoria de caracteres sobre corpos finitos e dos polinômios de Krawtchouk. Procurando tornar este texto mais auto-contido e ao mesmo tempo permitir uma fluência maior na leitura das demonstrações principais, optamos por apresentar uma breve resenha de definições e resultados relativos a estes assuntos nos Apêndices A e B.

Capítulo 1

Métricas Poset-Block

Neste capítulo, apresentaremos as noções básicas sobre conjuntos parcialmente ordenados, para posteriormente, definirmos as métricas poset-block, que serão os objetos principais deste trabalho. Todos os resultados aqui apresentados podem ser encontrados em [19].

1.1 Conjuntos Parcialmente Ordenados

Sejam X e Y conjuntos não vazios. Uma *relação binária* sobre X e Y é qualquer subconjunto R do produto cartesiano $X \times Y$. Se $(x, y) \in R$, ou seja, se x se relaciona com y, escrevemos xRy. Se R é uma relação binária em $X \times X$ dizemos simplesmente que R é uma relação binária em X. Uma *relação de ordem parcial* num conjunto X, é uma relação binária $\preccurlyeq$ que satisfaz para todo $x, y, z \in X$, as seguintes condições:

(i) $x \preccurlyeq x$ (Reflexiva);

(ii) Se $x \preccurlyeq y$ e $y \preccurlyeq x$, então $x = y$ (Anti-simétrica) e

(iii) Se $x \preccurlyeq y$ e $y \preccurlyeq z$, então $x \preccurlyeq z$. (Transitiva).

Uma relação de ordem parcial em X é dita *total* se $x \preccurlyeq y$ ou $y \preccurlyeq x$ para todo $x, y \in X$.

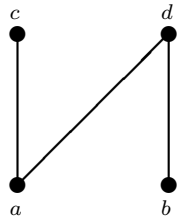
Definição 1. *Se $\preccurlyeq$ é uma relação de ordem parcial em X, chamaremos o par ordenado $P \triangleq (X, \preccurlyeq)$ de poset (do inglês, partially ordered set).*

Observação 1. *Eventualmente denotaremos a ordem do poset $P = (X, \preccurlyeq)$ por $\preccurlyeq_P$ e diremos que P é um poset em X, além disso, se $x \in X$, com um abuso de notação, diremos que $x \in P$, ou seja, representaremos o conjunto X pelo poset P.*

Se $x, y \in P$ são tais que $x \preccurlyeq_P y$ ou $y \preccurlyeq_P x$, dizemos que x e y são *comparáveis*, caso contrário, são ditos *incomparáveis*. Um poset P é dito *cadeia*, ou linear, se a relação de ordem $\preccurlyeq_P$ for total, ou seja, se quaisquer dois elementos de P forem comparáveis. Um poset é chamado de *anticadeia*, ou antilinear, se quaisquer dois elementos distintos forem incomparáveis.

Se M é um conjunto finito, o poset P em M é dito um *poset finito*. Caso não haja menção em relação a cardinalidade dos posets, estaremos assumindo serem posets finitos. Na literatura encontra-se diversas ferramentas para representação de posets, consulte [19], representaremos geometricamente um poset P através do *diagrama de Hasse*, neste diagrama, os elementos de M são representados por vértices e as relações entre dois elementos x e y de M são representadas por arestas, convencionando-se que x está abaixo de y se, e somente se, $x \neq y$, $x \preccurlyeq_P y$ e não existe um terceiro elemento $z \in M$ tal que $x \preccurlyeq_P z \preccurlyeq_P y$.

Exemplo 2. *Seja $M = \{a, b, c, d\}$ o conjunto com relação de ordem parcial dada por: $a \preccurlyeq_P c$, $a \preccurlyeq_P d$ e $b \preccurlyeq_P d$. Então, o diagrama abaixo é uma representação do poset P através do diagrama de Hasse.*



Definição 3. *Sejam P um poset em M e I um subconjunto de M. Se para todo $x \in I$ e $y \in M$ satisfazendo $y \preccurlyeq_P x$ têm-se que $y \in I$, então I é dito um ideal de P. Se A é um subconjunto de M, denotamos por $\langle A \rangle_P$ o menor ideal de P contendo A, que chamaremos de ideal gerado por A. Se $A = \{x_1, .., x_n\}$, o ideal gerado por A será denotado por $\langle x_1, .., x_n \rangle_P$ ao invés de $\langle \{x_1, .., x_n\} \rangle_P$.*

Proposição 4. *Se $\{A_1, ..., A_k\}$ é uma família finita não vazia de ideais de um poset P, então $\cap_{i=1}^{k} A_i$ é um ideal de P.*

Sendo P um poset finito, o conjunto $\Theta(P)$ de todos os ideais de P é também finito, logo, se A é um subconjunto de P, como a interseção finita de ideais é um ideal e P é um ideal contendo

A, então o ideal gerado por um conjunto sempre existe e

$$\langle A\rangle_P = \bigcap_{\substack{I\in\Theta(P)\\ A\subset I}} I,$$

ou seja, o menor ideal de P contendo o conjunto A é a interseção de todos os ideais de P contendo tal conjunto.

Proposição 5. *Se $\{A_1, ..., A_k\}$ é uma família finita não vazia de subconjuntos do poset P,*

$$\bigcup_{i=1}^{k}\langle A_i\rangle_P = \left\langle \bigcup_{i=1}^{k} A_i \right\rangle_P .$$

Definição 6. *Seja I um ideal de um poset P. Um elemento $x \in I$ é dito maximal em I se para todo $y \in I$ satisfazendo $x \preccurlyeq_P y$ tivermos que $x = y$, é dito minimal se para todo $y \in I$ satisfazendo $y \preccurlyeq_P x$ tivermos que $y = x$. Denotaremos por $Max(I)$ e $Min(I)$ os conjuntos dos elementos maximais e minimais de I respectivamente, isto é,*

$$Min(I) \triangleq \{x \in I : x \text{ é minimal em } I\} \quad e \quad Max(I) \triangleq \{x \in I : x \text{ é maximal em } I\}.$$

Seja P um poset em M, se N é um subconjunto de M, e Q é um poset em N tal que para todo $x, y \in N$ tem-se que $x \preccurlyeq_Q y$ se, e somente se, $x \preccurlyeq_P y$, diremos que a ordem de Q é uma *ordem induzida* do poset P. Se P e Q são posets tais que a ordem de Q é induzida pela ordem de P, diremos que Q é um *subposet* de P, sendo assim, Q será dito uma cadeia de P se Q for um poset do tipo cadeia, nesse caso, definimos o *comprimento* da cadeia Q como sendo a cardinalidade de N. O conjunto das cadeias de P será denotado por C_P. O *posto* de um elemento $x \in P$, denotado por $r_P(x)$, é o comprimento da maior cadeia de P contendo x como elemento maximal, ou seja,

$$r_P(x) \triangleq max\{|S| : S \subset \langle x\rangle_P \text{ e } S \in C_P\},$$

onde $|S|$ denota a cardinalidade do conjunto S, com isso, definimos a altura do poset P por

$$h(P) \triangleq max\{r_P(x) : x \in P\}.$$

Definição 7. *Sendo P um poset em M tal que $h(P) = t$. Dado $i \in \{1, \cdots, t\}$, o subconjunto de P contendo todos os elementos de posto i será denotado por*

$$\Gamma_P^i \triangleq \{x \in P : r_P(x) = i\},$$

e chamado de i-ésimo nível do poset. Definimos a estrutura de nível de P como sendo a t-upla

$$\Gamma_P \triangleq (|\Gamma_P^1|, |\Gamma_P^2|, \cdots, |\Gamma_P^t|).$$

Se P é um poset de altura t, é claro que Γ_P^1 coincide com o conjunto dos elementos minimais de P. Por outro lado, de modo geral, podemos apenas afirmar que os elementos de Γ_P^t são maximais em P, sem necessariamente conter todos estes elementos.

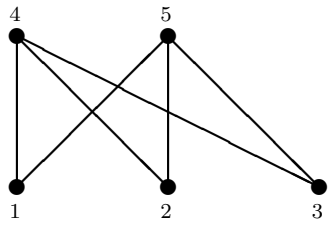
Exemplo 8. *No poset P do Exemplo 2, temos que a estrutura de nível de P é dada por $\Gamma_P = (2, 2)$, onde $\Gamma_P^1 = \{a, b\}$ e $\Gamma_P^2 = \{c, d\}$ são os níveis 1 e 2 do poset respectivamente.*

Se P e Q são dois posets tais que $M_1 \cap M_2 = \emptyset$. A *soma ordinária* entre P e Q, denotada por $P \oplus Q$ é uma relação binária em $M_1 \cup M_2$ definida da seguinte maneira:

$$x \preccurlyeq_{P\oplus Q} y \Leftrightarrow \begin{cases} x \preccurlyeq_P y, & \text{quando} \quad x, y \in M_1 \\ x \preccurlyeq_Q y, & \text{quando} \quad x, y \in M_2 \\ x \in P \text{ e } y \in Q. \end{cases}$$

É claro que $\preccurlyeq_{P\oplus Q}$ é uma ordem parcial em $M_1 \cup M_2$, logo $P \oplus Q$ é um poset em $M_1 \cup M_2$ e portanto a soma ordinária é uma operação associativa mas não comutativa e fechada no conjunto dos posets. A generalização da soma ordinária para n posets segue naturalmente somando-se dois a dois.

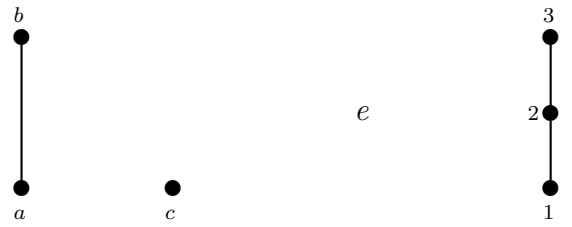
Exemplo 9. *Sejam $P = (\{1, 2, 3\}, \preccurlyeq)$ e $Q = (\{4, 5\}, \preccurlyeq)$ dois posets anticadeia. O diagrama de Hasse do poset $P \oplus Q$ é dado por:*



Definição 10. *Sejam P e Q dois posets. Dizemos que uma aplicação $f : P \to Q$ é um homomorfismo de ordem se, para todo $x, y \in P$ tais que $x \preccurlyeq_P y$ tivermos que $f(x) \preccurlyeq_Q f(y)$.*

Como consequência da Definição 10, qualquer função que possuir como domínio uma anticadeia será um homomorfismo de ordem. Se Q é um subposet de P, a aplicação de inclusão $i : Q \to P$ define um homomorfismo de ordem. Reciprocamente, se P e Q são dois posets tais que a aplicação de inclusão $i : Q \to P$ é um homomorfismo de ordem, então Q é um subposet de P.

Exemplo 11. *Sejam P e Q dois posets com diagramas de Hasse*



respectivamente. A aplicação $f : P \to Q$ definida por $f(a) = 1$, $f(b) = 3$ e $f(c) = 2$, é um homomorfismo de ordem.

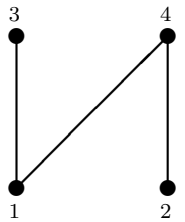
Pelo Exemplo 11, temos que $2 \preccurlyeq_Q 3$, porém $f^{-1}(2)$ e $f^{-1}(3)$ são incomparáveis. Portanto, se f for um homomorfismo de ordem bijetor, em geral não podemos afirmar que f^{-1} define um homomorfismo de ordem.

Definição 12. *Um homomorfismo de ordem é dito um isomorfismo de posets se for bijetor e sua inversa for um homomorfismo de ordem, neste caso, dizemos que os posets são isomorfos. Um isomorfismo de poset sobre si mesmo é dito um automorfismo.*

Definição 13. *Dados P um poset e B um conjunto não vazio. Se $g : P \to B$ é uma bijeção e Q é um poset em B tal que a aplicação $f : P \to Q$ definida por $f(x) = g(x)$ é um isomorfismo de ordem, diremos que $\preccurlyeq_Q$ é uma ordem parcial em B induzida pela aplicação g.*

Tomando por conveniência $m_0 = 0$, diremos que um poset P com estrutura de nível $(m_1, \cdots, m_t)$ possui um *rotulamento natural* se $\Gamma_P^i = \{m_0+m_1+\cdots+m_{i-1}+1, \cdots, m_1+\cdots+m_i\}$ para todo $i \in \{1, \cdots, t\}$.

Exemplo 14. *O poset $Q = (\{1, 2, 3, 4\}, \preccurlyeq_Q)$ com relação de ordem parcial determinada pelo diagrama de Hasse abaixo, é um poset com rotulamento natural e estrutura de nivel $(2, 2)$.*



Mostraremos que todo poset finito é isomorfo a um poset com rotulamento natural, desta forma, não perderemos em generalidade se trabalharmos apenas com posets rotulados naturalmente. Defina $[m] \triangleq \{1, \cdots, m\}$, temos então o seguinte teorema:

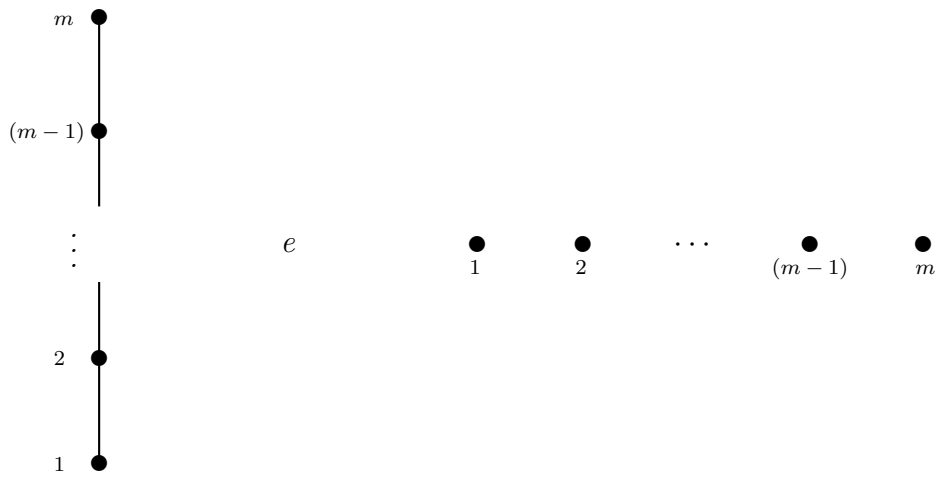
Teorema 15. *Seja P um poset finito em M com m elementos, então existe um poset Q em $[m]$ com rotulamento natural isomorfo a P.*

Demonstração. Suponha que $(m_1, \cdots, m_t)$ seja a estrutura de nível de P, defina $g : P \to [m]$ tal que para todo $i \in \{1, \cdots, t\}$, $\Gamma_P^i = \{g^{-1}(m_0 + m_1 + \cdots + m_{i-1} + 1), \cdots, g^{-1}(m_1 + \cdots + m_i)\}$. Seja $\preccurlyeq_Q$ a ordem em $[m]$ induzida pela aplicação g. Portanto, a aplicação $f : P \to Q$ definida por $f(x) = g(x)$ é um isomorfismo de ordem, além disso, por construção, Q está rotulado naturalmente. ■

Exemplo 16. *Sejam P e Q os posets dos Exemplos 2 e 14 respectivamente, a aplicação $f : P \to Q$ definida por $f(a) = 1$, $f(b) = 2$, $f(c) = 3$ e $f(d) = 4$ é um isomorfismo de posets.*

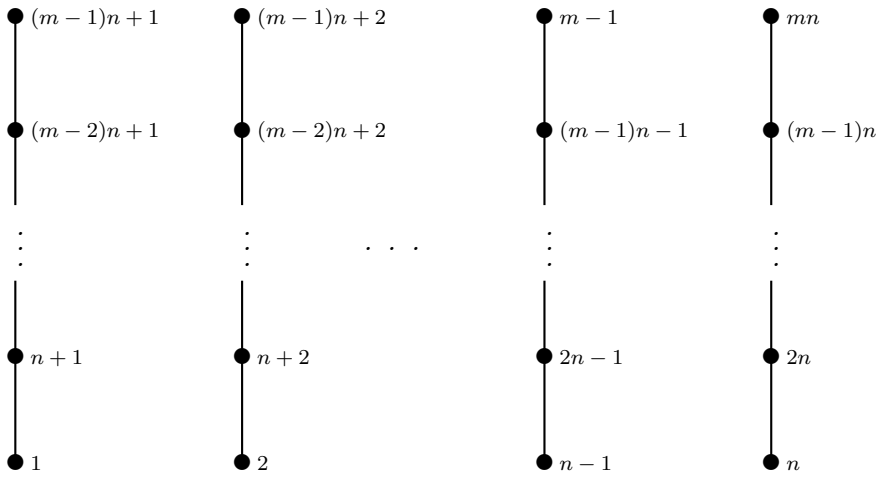
Apresentaremos agora famílias de posets que se destacam no contexto de códigos corretores de erros.

Exemplo 17. *(Cadeia e Anticadeia) Os posets cadeia denotados por $\mathcal{C}$ e anticadeia denotados por $\mathcal{A}$, possuem diagrama de Hasse*

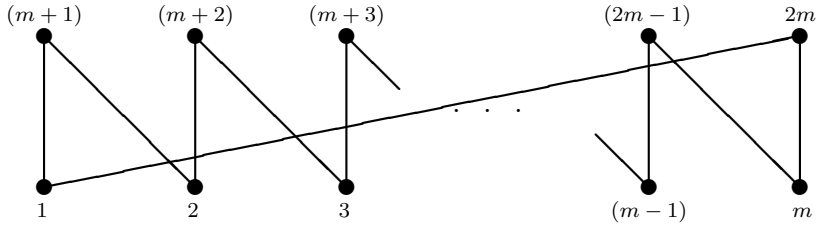


respectivamente.

Exemplo 18. *(Niederreiter-Rosembloom-Tsfasman $\mathcal{NRT}$) O poset $\mathcal{NRT}$ é obtido através da união finita e disjunta de cadeias de mesmo comprimento. Se $\mathcal{C}_i$ são cadeias de comprimento m em $\{i, n+i, 2n+i, \cdots, (m-1)n+i\}$ para todo $i \in \{1, \cdots, n\}$, então o poset $\mathcal{NRT}$ obtido pela união dessas cadeias é um poset sobre $[mn]$ dado pelo seguinte diagrama de Hasse:*



Exemplo 19. *(Coroa) Seja $\mathcal{CR}$ o poset em $[2m]$ definido da seguinte maneira: $1 \preccurlyeq m+1$, $1 \preccurlyeq 2m$, $i \preccurlyeq m+i$ e $i \preccurlyeq m+i-1$ para todo $i \in \{2,3,\cdots,m\}$. Tal poset é chamado de coroa e possui o seguinte diagrama de Hasse:*



Exemplo 20. *(Hierárquico) Para todo $i \in \{1,\cdots,t\}$, seja $\mathcal{A}^i$ um poset anticadeia tal que $|\mathcal{A}^i| = m_i$ e $\Gamma^1_{\mathcal{A}^i} = \{m_0+m_1+\cdots+m_{i-1}+1,\cdots,m_1+\cdots+m_i\}$. O poset $\mathcal{H}$ com estrutura de nível $(m_1,\cdots,m_t)$ definido por*

$$\mathcal{H} = \mathcal{A}^1 \oplus \mathcal{A}^2 \oplus \cdots \oplus \mathcal{A}^t,$$

é chamado de poset hierárquico. O poset do Exemplo 9 é um poset hierárquico com rotulamento natural e estrutura de nível $(3,2)$.

Note que as classes de posets apresentadas nos exemplos anteriores não são disjuntas. A classe de posets hierárquicos se destaca, pois contém as classes de posets cadeia e anticadeia, além disso, se intercepta com as classes dos poset coroa e $\mathcal{NRT}$.

Definição 21. *Sejam P e Q dois posets em $[m]$. Uma bijeção $f : P \to Q$ é dita um anti-isomorfismo se*

$$i \preccurlyeq_P j \iff f(j) \preccurlyeq_Q f(i).$$

para todo $i, j \in P$.

Definição 22. *Sendo P um poset em $[m]$, o poset $\overline{P}$ em $[m]$ com ordem parcial dada por*

$$i \preccurlyeq_{\overline{P}} j \iff j \preccurlyeq_P i,$$

será chamado de poset dual de P.

A ordem parcial em $[m]$ definida por $\overline{P}$ é a única que faz com que a aplicação identidade $id : P \to \overline{P}$ seja um anti-isomorfismo, portanto $\Gamma^1_{\overline{P}}$ coincide com os elementos maximais de P, ou seja, $Max(P) = Min(\overline{P})$.

1.2 Espaços com Métricas Poset-Block

Sendo $\mathbb{F}_q$ um corpo finito com q elementos, denote por $\mathbb{F}_q^n$ o espaço vetorial das n-uplas sobre $\mathbb{F}_q$. Construiremos uma família de métricas sobre $\mathbb{F}_q^n$ que posteriormente serão utilizadas no contexto de teoria de códigos. A métrica mais importante nesse contexto em termos de aplicações práticas é a de Hamming, definida em [5], tal métrica é utilizada geralmente em códigos e espaços vetoriais sobre o corpo com dois elementos $\mathbb{F}_2$. A métrica de Lee ([27] e [13]), definida na década de 50, também é uma métrica que desperta interesse em teoria de códigos, porém não a trataremos aqui, pois veremos que uma métrica poset-block, objeto principal de estudo desse trabalho, coincide com a métrica de Lee apenas em algumas situações clássicas (Hamming binário e ternário).

Sejam n e m dois inteiros positivos tais que $m \leqslant n$. Se P é um poset em $[m]$ e $\pi : [m] \to \mathbb{N}^*$ é uma aplicação tal que $\sum_{i=1}^{m} \pi(i) = n$, diremos que o par (P, π) é um *poset-block* em $[m]$. Denote $k_i = \pi(i)$, então

$$V \triangleq \mathbb{F}_q^{k_1} \times \mathbb{F}_q^{k_2} \times \cdots \times \mathbb{F}_q^{k_m}$$

é um $\mathbb{F}_q$-espaço vetorial isomorfo a $\mathbb{F}_q^n$. Portanto, dado $u \in \mathbb{F}_q^n$, existe uma única decomposição $u = (u_1, \cdots, u_m)$ de maneira que $u_i \in \mathbb{F}_q^{k_i}$ para todo $i \in [m]$, em virtude disso, chamaremos o conjunto $[m]$ de *π-coordenadas* de $\mathbb{F}_q^n$ e a aplicação π de *dimensionamento do poset P* (pois associa uma dimensão k_i a cada elemento $i \in P$).

Definição 23. *Dado $u \in \mathbb{F}_q^n$, o π-suporte de u é o conjunto das π-coordenadas de $\mathbb{F}_q^n$ para as quais $u_i \in \mathbb{F}_q^{k_i}$ é não nulo, ou seja,*

$$supp_\pi(u) \triangleq \{i \in [m] : u_i \neq 0 \in \mathbb{F}_q^{k_i}\}.$$

Quando $k_i = 1$ para todo $i \in \{1, \cdots, m\}$, o π-suporte de u será denotado por $supp(u)$ e chamado de suporte de u.

Definição 24. *O (P, π)-peso de um elemento $u \in \mathbb{F}_q^n$ é a cardinalidade do ideal de P gerado pelo π-suporte de u, ou seja,*

$$w_{(P,\pi)}(u) \triangleq |\langle supp_\pi(u)\rangle_P|.$$

Sejam u e v elementos de $\mathbb{F}_q^n$. A (P, π)-distância entre u e v é definida por

$$d_{(P,\pi)}(u, v) \triangleq w_{(P,\pi)}(u - v).$$

Teorema 25. *(Métricas poset-block,[1]) Se (P, π) é um poset-block em $[m]$ sobre $\mathbb{F}_q^n$, então a (P, π)-distância é uma métrica em $\mathbb{F}_q^n$.*

Demonstração. É claro que a (P, π)-distância é positiva e $d_{(P,\pi)}(u, v) = 0$ se, e somente se, $u = v$ para todo $u, v \in \mathbb{F}_q^n$. A propriedade de simetria também é evidente do fato de $supp_\pi(u - v) = supp_\pi(v - u)$ para todo $u, v \in \mathbb{F}_q^n$. Basta então mostrar que $d_{(P,\pi)}$ satisfaz a desigualdade triangular. Dados $u, v, w \in \mathbb{F}_q^n$, temos que

$$d_{(P,\pi)}(u, v) = w_{(P,\pi)}(u - v) = w_{(P,\pi)}(u - w + w - v).$$

Tomando $x = u - w$ e $y = w - v$, para concluirmos a prova resta verificar que $w_{(P,\pi)}(x + y) \leqslant w_{(P,\pi)}(x) + w_{(P,\pi)}(y)$. Para tanto, note que $supp_\pi(x + y) \subset supp_\pi(x) \cup supp_\pi(y)$, portanto

$$w_{(P,\pi)}(x + y) = |\langle supp_\pi(x + y)\rangle_P| \leqslant |\langle supp_\pi(x) \cup supp_\pi(y)\rangle_P|.$$

Pela Proposição 5 e como $|\langle supp_\pi(x) \cup supp_\pi(y)\rangle_P| \leqslant |\langle supp_\pi(x)\rangle_P| + |\langle supp_\pi(y)\rangle_P|$, segue que

$$\begin{aligned} |\langle supp_\pi(x) \cup supp_\pi(y)\rangle_P| &= |\langle supp_\pi(x)\rangle_P \cup \langle supp_\pi(y)\rangle_P| \\ &\leqslant |\langle supp_\pi(x)\rangle_P| + |\langle supp_\pi(y)\rangle_P| \\ &= w_{(P,\pi)}(x) + w_{(P,\pi)}(y). \end{aligned}$$

Portanto $d_{(P,\pi)}(u, v) \leqslant w_{(P,\pi)}(x) + w_{(P,\pi)}(y) = d_{(P,\pi)}(u, w) + d_{(P,\pi)}(w, v)$. ■

Chamaremos a métrica $d_{(P,\pi)}$ em $\mathbb{F}_q^n$ de *métrica poset-block* ou (P, π)-*métrica*, o par ordenado $(\mathbb{F}_q^n, d_{(P,\pi)})$ será chamado de *espaço poset-block* ou (P, π)-*espaço*.

Definição 26. *Seja (P, π) um poset-block em $[m]$, a estrutura $(\overline{P}, \pi)$ é dita poset-block dual de (P, π) se $\overline{P}$ for o poset dual de P.*

Observação 2. *Se (P,π) é um poset-block, com um abuso de notação, identificaremos os elementos do poset P como sendo elementos do poset-block (P,π), isto é, $i \in P$ se, e somente se, $i \in (P,\pi)$.*

Definição 27. *Uma aplicação $f : (P,\pi) \to (P_1,\pi_1)$ é um homomorfismo de poset-block se f for um homomorfismo de ordem entre os posets P e P_1, e $\pi_1(f(j)) = \pi(j)$ para todo $j \in P$.*

Definição 28. *Se $f : (P,\pi) \to (P_1,\pi_1)$ é um homomorfismo bijetor de poset-block, então f será dito um isomorfismo de poset-block se f^{-1} for um homomorfismo de poset-block, neste caso, diremos que (P,π) e (P_1,π_1) são isomorfos.*

Pela Definição 28, se P e P_1 forem isomorfos e $\pi_1(f(j)) = \pi(j)$, então (P,π) e (P_1,π_1) são isomorfos enquanto poset-block.

Definição 29. *Sejam (P,π) e (P_1,π_1) dois poset-block. Diremos que uma aplicação $f : (\mathbb{F}_q^n, d_{(P,\pi)}) \to (\mathbb{F}_q^n, d_{(P_1,\pi_1)})$ é uma isometria, se para todo $u, v \in \mathbb{F}_q^n$,*

$$d_{(P,\pi)}(u,v) = d_{(P_1,\pi_1)}(f(u), f(v)).$$

Neste caso, diremos que o (P,π)-espaço e o (P_1,π_1)-espaço são isométricos.

Definição 30. *Se (P,π) é um poset-block com t níveis, para todo $i \in \{1,\cdots,t\}$, defina*

$$b_i \triangleq \sum_{j \in \Gamma_P^i} k_j,$$

como sendo a soma da dimensão associada por π dos elementos do i-ésimo nível de P, que chamaremos de dimensão do i-ésimo nível de P.

Se (P,π) é um poset-block em $[m]$ sobre $\mathbb{F}_q^n$ tal que $(m_1,\cdots,m_t)$ é a estrutura de nível de P, então $n = b_1 + \cdots + b_t$ e $m = m_1 + \cdots + m_t$. Dado $i \in \{0,1,\cdots,t\}$, no decorrer desse trabalho usaremos as seguintes notações:

- $b_0 = 0$, $m_0 = 0$ e $k_0 = 0$;
- $\widehat{b_i} = n - (b_0 + b_1 + \cdots + b_i)$;
- $\widehat{m_i} = m - (m_0 + m_1 + \cdots + m_i)$ e

- Se $i \neq 0$, $r_i = m_0 + m_1 + \cdots + m_{i-1}$;

De maneira semelhante ao efetuado nos posets, mostraremos que, a menos de isomorfismo de poset-block, podemos admitir que o poset associado ao poset-block está rotulado naturalmente.

Teorema 31. *Se (P, π) é um poset-block com estrutura de nível $(m_1, \cdots, m_t)$, então existe um poset-block (P_1, π_1) em $[m]$ isomorfo a (P, π) tal que P_1 possui rotulamento natural.*

Demonstração. Pelo Teorema 15, existe um poset P_1 com rotulamento natural e um isomorfismo $g : P \to P_1$. Se π_1 é a aplicação de dimensionamento do poset P_1 definida por $\pi_1(j) = \pi(g^{-1}(j))$ para todo $j \in [m]$, ou seja, $\pi_1(g(j)) = \pi(j)$, então $f : (P, \pi) \to (P_1, \pi_1)$ definida por $f(j) = g(j)$ é por construção um isomorfismo de poset-block. ■

Corolário 32. *Se $(\mathbb{F}_q^n, d_{(P,\pi)})$ é um (P, π)-espaço, então existe um (P_1, π_1)-espaço $(\mathbb{F}_q^n, d_{(P_1,\pi_1)})$ isométrico ao (P, π)-espaço $(\mathbb{F}_q^n, d_{(P,\pi)})$ tal que o poset P_1 seja rotulado naturalmente.*

Demonstração. Pelo Teorema 31, existe um poset-block (P_1, π_1) e um isomorfismo $\sigma : (P, \pi) \to (P_1, \pi_1)$ onde P_1 é um poset rotulado naturalmente. Denote $\pi_1(j) = k'_j$ e $\pi(j) = k_j$, então o mapa

$$\begin{array}{rccc} g & : & (\mathbb{F}_q^{k_1} \times \cdots \times \mathbb{F}_q^{k_m}, d_{(P,\pi)}) & \longrightarrow & (\mathbb{F}_q^{k'_1} \times \cdots \times \mathbb{F}_q^{k'_m}, d_{(P_1,\pi_1)}) \\ & & (v_1, \cdots, v_m) & \longmapsto & (v_{\sigma(1)}, \cdots, v_{\sigma(m)}) \end{array}$$

é, por construção, uma isometria linear. ■

Pelo Corolário 32, segue que do ponto de vista métrico, o (P, π)-espaço e o (P_1, π_1)-espaço são essencialmente equivalentes. Além disso, se (P, π) é um poset-block tal que P é um poset com altura t rotulado naturalmente, então todo elemento u de $\mathbb{F}_q^n$ pode ser descrito da seguinte forma:

$$u = \sum_{i=1}^{h(P)} \sum_{j=1}^{m_i} \sum_{l=1}^{k_{(r_i+j)}} u_{r_i+j}^l e_{s(i,j,l)},$$

onde $u_{r_i+j}^l \in \mathbb{F}_q$ são escalares, $(m_1, \cdots, m_t)$ é a estrutura de nível de P e

$$\left\{ e_{s(i,j,l)} :, 1 \leqslant i \leqslant h(P), 1 \leqslant j \leqslant m_i, 1 \leqslant l \leqslant k_{(r_i+j)} \right\}$$

é a base canônica de $\mathbb{F}_q^n$ definida de forma que $s(i, j, l) = l + \sum_{t=0}^{r_i+j-1} k_t$.

Observação 3. *Por questão de conveniência, identificaremos as propriedades do poset como sendo também propriedades do poset-block, por exemplo, se P é hierárquico, diremos que o poset-block (P, π) é hierárquico.*

Se (P,π) é um poset-block com estrutura de nível $(m_1,\cdots,m_t)$, defina por

$$V \triangleq \mathbb{F}_q^{b_1} \times \cdots \times \mathbb{F}_q^{b_t}$$

o espaço vetorial sobre $\mathbb{F}_q$ isomorfo a $\mathbb{F}_q^n$. Dado $u \in \mathbb{F}_q^n$, existe uma única decomposição de u da forma $u = (u^1,\cdots,u^t)$ onde $u^i \in \mathbb{F}_q^{b_i}$, além disso, se (P,π) está rotulado naturalmente, então $u^i = (u_{r_i+1},\cdots,u_{r_i+m_i})$ é tal que $u_{r_i+j} \in \mathbb{F}_q^{k_{(r_i+j)}}$. Eventualmente usaremos a seguinte notação: $\widetilde{u^{i+1}} = (u^{i+1},\cdots,u^t) \in \mathbb{F}_q^{\widehat{b_i}}$.

Mostraremos agora o quão abrangente são as estruturas de poset-block que definimos. Seja (P,π) um poset-block em $[m]$, então:

- Se a estrutura de blocos é trivial, ou seja, $\pi(j) = 1$ para todo $j \in [m]$. Dados $u, v \in \mathbb{F}_q^n$ segue que

  $$d_{(P,\pi)}(u,v) = |\langle supp_\pi(u-v)\rangle_P| = |\langle supp(u-v)\rangle_P| = d_P(u,v),$$

  ou seja, a métrica poset-block $d_{(P,\pi)}$ coincide, neste caso, com a *métrica poset* d_P definida em [2];

- Se (P,π) é um poset-block em $[m]$ tal que $P = \mathcal{A}$, ou seja, P é anticadeia. Para todo $u, v \in \mathbb{F}_q^n$

  $$d_{(P,\pi)}(u,v) = |\langle supp_\pi(u-v)\rangle_P| = |supp_\pi(u-v)| = d_\pi(u,v),$$

  portanto, neste caso, a métrica poset-block $d_{(P,\pi)}$ coincide com a *métrica de bloco* d_π definida em [4], também conhecida como π-*distância*.

- Se (P,π) é um poset-block tal que $P = \mathcal{A}$ e a estrutura de blocos é trivial, segue que

  $$d_{(P,\pi)}(u,v) = |\langle supp_\pi(u-v)\rangle_P| = |supp_\pi(u-v)| = |supp(u-v)| = d_H(u,v),$$

  ou seja, a (P,π)-métrica $d_{(P,\pi)}$ coincide com a *métrica de Hamming* d_H.

Portanto, a família das métricas poset-block contém ambas as famílias das métricas poset e das métricas de bloco, e consequentemente contém a métrica de Hamming. Seja p um número primo, dados $u, v \in \mathbb{F}_p^n$, a *métrica de Lee* em $\mathbb{F}_p^n$ é definida por

$$d_L(u,v) \triangleq \sum_{i=1}^{n} |u_i - v_i|_L$$

para todo $u, v \in \mathbb{F}_p^n$ onde

$$|u_i - v_i|_L \triangleq min\{|u_i - v_i|, p - |u_i - v_i|\}$$

e $|.|$ denota o valor absoluto usual em $\mathbb{R}$. É claro que se $p \in \{2, 3\}$, $d_L = d_H$. A proposição a seguir mostra que exceto nos casos onde a métrica de Lee coincide com a métrica de Hamming, não existe um poset-block (P, π) tal que $d_L = d_{(P,\pi)}$.

Proposição 33. *Seja p um número primo maior que 3, então não existe uma (P, π)-métrica que coincida com a métrica de Lee em $\mathbb{F}_p^n$.*

Demonstração. Seja (P, π) um poset-block em $[m]$, podemos supor sem perca de generalidade que (P, π) está rotulado naturalmente. Tome $u \in \mathbb{F}_p^n$ tal que

$$u = \sum_{i=1}^{h(P)} \sum_{j=1}^{m_i} \left\lfloor \frac{p}{2} \right\rfloor e_{s(i,j,1)},$$

onde $\lfloor x \rfloor$ denota a parte inteira do número real x, logo $d_{(P,\pi)}(y, 0) = m$ e $d_L(y, 0) = m \left\lfloor \frac{p}{2} \right\rfloor$, ou seja, $d_{(P,\pi)} \neq d_L$. ■

Assim como em todo espaço métrico, podemos definir em $(\mathbb{F}_q^n, d_{(P,\pi)})$ os conceitos de bolas, esferas e raio de empacotamento. Seja $v \in \mathbb{F}_q^n$ e r um inteiro não negativo. A (P, π)-*bola* com centro em v e raio r é o conjunto

$$B_{(P,\pi)}(v, r) = \{u \in \mathbb{F}_q^n : d_{(P,\pi)}(u, v) \leqslant r\}$$

de todos os vetores em $\mathbb{F}_q^n$ que distam no máximo r (com a (P, π)-métrica) de v. A (P, π)-*esfera* com centro em v e raio r é o conjunto

$$S_{(P,\pi)}(v, r) = \{u \in \mathbb{F}_q^n : d_{(P,\pi)}(u, v) = r\}$$

dos vetores em $\mathbb{F}_q^n$ com (P, π)-distância a v igual a r.

Denote por

$$\Theta_j(i) \triangleq \{I \subset P : I \text{ é ideal }, \ |I| = i, \ |Max(I)| = j\}$$

o conjunto dos ideais de P com cardinalidade i e j elementos maximais, onde $Max(I)$ é o conjunto dos elementos maximais do ideal I.

Teorema 34. *Sejam $u \in \mathbb{F}_q^n$ e i um inteiro não negativo, então*

$$|S_{(P,\pi)}(u,i)| = \sum_{j=1}^{i} \sum_{I \in \Theta_j(i)} \prod_{m \in Max(I)} (q^{k_m} - 1) \prod_{m \in I \backslash Max(I)} q^{k_m}$$

se $i > 0$ e $|S_{(P,\pi)}(u,i)| = 1$ se $i = 0$.

Demonstração. Como $d_{(P,\pi)}(u,v) = w_{(P,\pi)}(u-v) = d_{(P,\pi)}(0,u-v)$ para todo $v \in \mathbb{F}_q^n$, a cardinalidade de uma (P,π)-esfera independe de seu centro, encontraremos então a cardinalidade de uma (P,π)-esfera centrada na origem. Se $i = 0$, então $S_{(P,\pi)}(0,0)$ contém apenas o vetor nulo, logo $|S_{(P,\pi)}(0,0)| = 1$. Suponha que $i \geqslant 1$, se $u \in S_{(P,\pi)}(0,i)$, então $w_{(P,\pi)}(u) = i$, ou seja, o ideal gerado pelo π-suporte de u possui i elementos. Portanto, sendo I um ideal de P tal que $|I| = i$, devemos encontrar quantos vetores $v \in \mathbb{F}_q^n$ satisfazem $\langle supp_\pi(v) \rangle_P = I$. Suponha que $|Max(I)| = j$, note que $1 \leqslant j \leqslant i$. Como $v = (v_1, \cdots, v_m)$, se v_s é tal que $s \in Max(I)$, segue que v_s não pode ser nulo, logo existem $q^{k_s} - 1$ possibilidades para v_s, e portanto existem $\prod_{m \in Max(I)} (q^{k_m} - 1)$ possíveis escolhas para os vetores das π-coordenadas de $\mathbb{F}_q^n$ pertencentes aos elementos maximais de I. Para os vetores das π-coordenadas de $\mathbb{F}_q^n$ pertencentes ao conjunto $I \backslash Max(I)$, uma vez que não há restrições para tais vetores, temos $\prod_{m \in I \backslash Max(I)} q^{k_m}$ maneiras de construí-los. Como os vetores das π-coordenadas de $\mathbb{F}_q^n$ pertencentes ao conjunto $[m] \backslash I$ são nulos e $[m] = Max(I) \sqcup I \backslash Max(I) \sqcup [m] \backslash I$, então existem

$$\prod_{m \in Max(I)} (q^{k_m} - 1) \prod_{m \in I \backslash Max(I)} q^{k_m}$$

vetores em $\mathbb{F}_q^n$ cujo ideal gerado por seu π-suporte é igual ao ideal I. Como I é um ideal qualquer com j elementos maximais, segue que existem

$$\sum_{I \in \Theta_j(i)} \prod_{m \in Max(I)} (q^{k_m} - 1) \prod_{m \in I \backslash Max(I)} q^{k_m}$$

vetores com peso i e j elementos maximais em seu π-suporte. Como $1 \leqslant j \leqslant i$, segue que

$$|S_{(P,\pi)}(0,i)| = \sum_{j=1}^{i} \sum_{I \in \Theta_j(i)} \prod_{m \in Max(I)} (q^{k_m} - 1) \prod_{m \in I \backslash Max(I)} q^{k_m}.$$

■

Corolário 35. *Sejam $u \in \mathbb{F}_q^n$ e r um inteiro não negativo, então*

$$|B_{(P,\pi)}(u,r)| = 1 + \sum_{i=1}^{r} \sum_{j=1}^{i} \sum_{I \in \Theta_j(i)} \prod_{m \in Max(I)} (q^{k_m} - 1) \prod_{m \in I \backslash Max(I)} q^{k_m}$$

se $r > 0$ e $|B_{(P,\pi)}(u,r)| = 1$ se $r = 0$.

Demonstração. Segue imediatamente do fato que

$$B_{(P,\pi)}(u,r) = \bigsqcup_{i=0}^{r} S_{(P,\pi)}(0,i)$$

sendo a união disjunta. ■

A partir da cardinalidade da (P,π)-bola é pode-se mostrar que o número de vetores em $(\mathbb{F}_q^n, d_H)$, $(\mathbb{F}_q^n, d_P)$ e $(\mathbb{F}_q^n, d_\pi)$ cuja distância a um vetor fixo $u \in \mathbb{F}_q^n$ é no máximo $r > 0$, respectivamente, é dado por

$$|B_H(u,r)| = \sum_{i=0}^{r} \binom{n}{i} (q-1)^i,$$

$$|B_P(u,r)| = 1 + \sum_{i=1}^{r} \sum_{j=1}^{i} (q-1)^j q^{i-j} \Theta_j(i)$$

e

$$|B_\pi(u,r)| = 1 + \sum_{i=1}^{r} \sum_{\substack{J \subset [n] \\ |J|=i}} \prod_{m \in J} (q^{k_m} - 1).$$

Além disso,

$$B_P(u,r) \subset B_H(u,r) \subset B_\pi(u,r) \tag{1.1}$$

para todo $u \in \mathbb{F}_q^n$.

Definição 36. *Sendo d uma métrica em $\mathbb{F}_q^n$, se U é um subespaço vetorial de $\mathbb{F}_q^n$, o raio de empacotamento de U é o maior número real $R_d(U)$ tal que as bolas de raio $R_d(U)$ e centro nos elementos de U são disjuntas, ou seja,*

$$R_d(U) = max\{r \in \mathbb{N} : B_d(v,r) \cap B_d(w,r) = \emptyset, \forall v, w \in U, v \neq w\}.$$

Pelas inclusões (1.1) segue que

$$R_{d_\pi}(U) \leqslant R_{d_H}(U) \leqslant R_{d_P}(U). \tag{1.2}$$

Veremos no próximo capítulo que é de suma importância em teoria de códigos encontrar o raio de empacotamento dos subespaços de $\mathbb{F}_q^n$, pois além de determinar a capacidade máxima de correção de erros, também permite descrever uma importante classe de códigos lineares, os chamados códigos perfeitos, porém em geral, encontrar o raio de empacotamento de um subespaço é uma tarefa complexa, e apenas algumas soluções para famílias particulares de métricas poset-block são conhecidas.

Capítulo 2

Códigos Lineares em Métricas Poset-Block

O principal objetivo deste capítulo é apresentar algumas definições básicas de códigos corretores de erros em espaços poset-block e introduzir as identidades de MacWilliams. Embora hajam poucos textos sobre códigos lineares em métricas poset-block, grande parte dos resultados desse capítulo são generalizações naturais para as métricas poset-block das definições encontradas em [28], [18], [7] e [6]. Os demais resultados foram obtidos através do estudo de artigos que serão citados no decorrer do capítulo.

2.1 Códigos Lineares

Seja A um conjunto finito, que chamaremos de *alfabeto*. Um *código corretor de erros*, ou simplesmente um *código*, é um subconjunto das palavras de comprimento n desse alfabeto, ou seja, é um subconjunto de A^n para algum número natural n, os elementos do código são chamados de *palavras-código*. Em teoria de códigos, do ponto de vista de implementação, é preferível trabalhar com códigos que possuem uma boa estrutura algébrica, por esse motivo, a classe de códigos mais utilizada na prática é a dos códigos lineares, na qual o alfabeto utilizado é um corpo finito e o código possui uma estrutura de espaço vetorial.

Definição 37. *Seja $\mathbb{F}_q^n$ o espaço vetorial das n-uplas sobre $\mathbb{F}_q$, $\mathscr{C}$ será dito um código linear*

se $\mathscr{C}$ for um subespaço vetorial de $\mathbb{F}_q^n$.

A estrutura de espaço vetorial não é uma estrutura suficiente para se mensurar ou corrigir erros, portanto a fim de desenvolvermos a teria de códigos, devemos estabelecer uma maneira de medir o quão distante um elemento está de um outro, ou seja, precisamos introduzir em $\mathbb{F}_q^n$ uma métrica. Neste trabalho, desenvolveremos a teoria dos códigos lineares com base nas (P,π)-métricas definidas no Capítulo 1, que já sabemos ser uma família de métricas contendo as métricas de bloco, as métricas poset e a clássica métrica de Hamming. Se $\mathbb{F}_q^n$ está munido com uma (P,π)-métrica, diremos que $\mathscr{C}$ é um (P,π)-*código linear*, eventualmente, usaremos a notação clássica e diremos que $\mathscr{C}$ é um código.

Definição 38. *(Distância Mínima) Sendo $\mathscr{C}$ um (P,π)-código linear, definimos a distância mínima de $\mathscr{C}$ como o menor (P,π)-peso das palavras-código não nulas de $\mathscr{C}$, ou seja,*

$$\delta_{(P,\pi)} \triangleq min\{w_{(P,\pi)}(v) : v \in \mathscr{C} \ e \ v \neq 0 \in \mathbb{F}_q^n\}.$$

Se $\mathscr{C}$ é um (P,π)-código linear em $\mathbb{F}_q^n$ de dimensão k e distância mínima $\delta_{(P,\pi)}$, denotaremos seus parâmetros por $[n,k,\delta_{(P,\pi)}]_q$. Sendo $\mathcal{H}$ um poset hierárquico, veremos que a distância mínima de um $(\mathcal{H},\pi)$-código linear determina seu raio de empacotamento, e portanto determina a quantidade máxima de erros que o vetor recebido pode conter e ainda ser corretamente decodificado.

Exemplo 39. *Seja $\mathcal{H}$ um poset hierárquico em $[3] = \{1,2,3\}$ com relação de ordem parcial: $1 \preccurlyeq_{\mathcal{H}} 2$ e $1 \preccurlyeq_{\mathcal{H}} 3$. Defina $\pi : [3] \to \mathbb{N}$ pondo $\pi(1) = 1$, $\pi(2) = 1$ e $\pi(3) = 2$. Logo, o código*

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

é um $(\mathcal{H},\pi)$-código linear com parâmetros $[4,1,2]_2$.

Se $\mathscr{C}$ é um (P,π)-código linear e $\lfloor\alpha\rfloor$ denota a parte inteira do número real α, de uma maneira geral, podemos estabelecer limitantes para o raio de empacotamento desse código, ou seja,

$$\left\lfloor \frac{\delta_{(P,\pi)} - 1}{2} \right\rfloor \leqslant R_{d_{(P,\pi)}}(\mathscr{C}) \leqslant \delta_{(P,\pi)} - 1.$$

Pela definição da distância mínima de $\mathscr{C}$, é claro que $R_{d_{(P,\pi)}}(\mathscr{C}) \leqslant \delta_{(P,\pi)} - 1$. Seja $t = \lfloor(\delta_{(P,\pi)} - 1)/2\rfloor$, dados $u, v \in \mathscr{C}$ distintos, para provarmos que $\lfloor(\delta_{(P,\pi)} - 1)/2\rfloor \leqslant R_{d_{(P,\pi)}}(\mathscr{C})$, basta mostrar

que $B_{(P,\pi)}(u,t)$ e $B_{(P,\pi)}(v,t)$ são disjuntas. Suponha que w pertença a interseção dessas, pela desigualdade triangular,

$$d_{(P,\pi)}(u,v) \leqslant d_{(P,\pi)}(u,w) + d_{(P,\pi)}(w,v) \leqslant 2t \leqslant d-1,$$

um absurdo, pois por definição $d \leqslant d_{(P,\pi)}(u,v)$.

Mostraremos que os limitantes obtidos para o raio de empacotamento são atingidos em certas classes de métricas poset-block, e portanto são os melhores limitantes quando não explicitamos o poset-block adotado. Em [21] e [3], foram encontrados os raios de empacotamento para métricas poset-block com P sendo um poset cadeia e para métricas poset hierárquicas, respectivamente. No teorema abaixo, estenderemos ambos os resultados encontrando o raio de empacotamento para códigos em métricas poset-block hierárquicas.

Teorema 40. *Se $(\mathcal{H},\pi)$ é um poset-block hierárquico em $[m]$ possuindo estrutura de nível $(m_1,\cdots,m_t)$ e $\mathscr{C}$ é um $(\mathcal{H},\pi)$-código linear com parâmetros $[n,k,\delta_{(\mathcal{H},\pi)}]$, sendo c uma palavra tal que $w_{(\mathcal{H},\pi)}(c) = \delta_{(\mathcal{H},\pi)}$ e $Max(\langle supp_\pi(c)\rangle_{\mathcal{H}}) \subset \Gamma^j_{\mathcal{H}}$, então*

$$R = R_{d_{(\mathcal{H},\pi)}}(\mathscr{C}) = r_j + \left\lfloor \frac{\delta_{(\mathcal{H},\pi)} - r_j - 1}{2} \right\rfloor,$$

é o raio de empacotamento de $\mathscr{C}$.

Demonstração. Dados $u,v \in \mathscr{C}$ distintos, como $\mathscr{C}$ é linear e a métrica $d_{(\mathcal{H},\pi)}$ é invariante por translações, provar que $B_{d_{(\mathcal{H},\pi)}}(u,R) \cap B_{d_{(\mathcal{H},\pi)}}(v,R) = \emptyset$, é equivalente a mostrar que $B_{d_{(\mathcal{H},\pi)}}(0,R) \cap B_{d_{(\mathcal{H},\pi)}}(u,R) = \emptyset$ para todo $u \in \mathscr{C}$ não nulo. Suponha que $z \in B_{d_{(\mathcal{H},\pi)}}(0,R) \cap B_{d_{(\mathcal{H},\pi)}}(u,R)$ para algum $u \in \mathscr{C}$, suponha ainda que $Max(\langle supp_\pi(u)\rangle_{\mathcal{H}}) \subset \Gamma^s_{\mathcal{H}}$, é claro que $s \geqslant j$, pois $u \in \mathscr{C}$ e $w_{(\mathcal{H},\pi)}(u) \geqslant w_{(\mathcal{H},\pi)}(c)$.

Note que $Max(\langle supp_\pi(z)\rangle_{\mathcal{H}}) \subset \Gamma^l_{\mathcal{H}}$ onde $l = s$, de fato, se $l < s$, como $|Max(\langle supp_\pi(c)\rangle_{\mathcal{H}})| = \delta_{(\mathcal{H},\pi)} - r_j$ e $\delta_{(\mathcal{H},\pi)} = w_{(\mathcal{H},\pi)}(c)$, então $w_{(\mathcal{H},\pi)}(z-u) = w_{(\mathcal{H},\pi)}(u) \geqslant \delta_{(\mathcal{H},\pi)} > R$, ou seja, $z \notin B_{d_{(\mathcal{H},\pi)}}(u,R)$, o que é um absurdo. Se $l > s$, então $w_{(\mathcal{H},\pi)}(z-u) = w_{(P,\pi)}(z) > r_{j+1} > R$ pois $r_{j+1} = r_j + m_j$ e $m_j > \lfloor(\delta_{(\mathcal{H},\pi)} - r_j - 1)/2\rfloor$, logo $z \notin B_{d_{(\mathcal{H},\pi)}}(0,R)$, novamente um absurdo. Portanto $Max(\langle supp_\pi(z)\rangle_{\mathcal{H}}) \subset \Gamma^s_{\mathcal{H}}$.

Se $s > j$, como $Max(\langle supp_\pi(z)\rangle_{\mathcal{H}}) \subset \Gamma^s_{\mathcal{H}}$, então $w_{(\mathcal{H},\pi)}(z) > R$, um absurdo pois $z \in B_{d_{(\mathcal{H},\pi)}}(0,R)$. Portanto $s = j$, ou seja, $Max(\langle supp_\pi(u)\rangle_{\mathcal{H}}) \subset \Gamma^j_{\mathcal{H}}$ e $Max(\langle supp_\pi(z)\rangle_{\mathcal{H}}) \subset \Gamma^j_{\mathcal{H}}$.

Se $|Max(\langle supp_\pi(z)\rangle_{\mathcal{H}})| > \lfloor(\delta_{(\mathcal{H},\pi)} - r_j - 1)/2\rfloor$, então $w_{(\mathcal{H},\pi)}(z) > R$, ou seja, $z \notin B_{d_{(\mathcal{H},\pi)}}(0,R)$. Suponha então que $|Max(\langle supp_\pi(z)\rangle_{\mathcal{H}})| \leqslant \lfloor(\delta_{(\mathcal{H},\pi)} - r_j - 1)/2\rfloor < (\delta_{(\mathcal{H},\pi)} - r_j)/2$, logo $z \in$

$B_{d_{(\mathcal{H},\pi)}}(0,R)$ porém, como $|Max(\langle supp_\pi(u)\rangle_\mathcal{H})| \geqslant \delta_{(\mathcal{H},\pi)} - r_j = |Max(\langle supp_\pi(c)\rangle_\mathcal{H})|$ e ambos $Max(\langle supp_\pi(z)\rangle_\mathcal{H})$ e $Max(\langle supp_\pi(u)\rangle_\mathcal{H})$ pertencem ao mesmo nível de $\mathcal{H}$, segue que

$$\begin{aligned} d_{(\mathcal{H},\pi)}(u,z) = w_{(\mathcal{H},\pi)}(u-z) &= r_j + |Max(\langle supp_\pi(u-z)\rangle_\mathcal{H})| \\ &\geqslant r_j + \frac{\delta_{(\mathcal{H},\pi)} - r_j}{2} \\ &> r_j + \left\lfloor \frac{\delta_{(\mathcal{H},\pi)} - r_j - 1}{2} \right\rfloor. \end{aligned}$$

Note que $w_{(\mathcal{H},\pi)}(u) \neq w_{(\mathcal{H},\pi)}(z)$, pois caso contrário $u \in B_{d_{(\mathcal{H},\pi)}}(0,R)$, o que é um absurdo. Portanto $z \notin B_{d_{(\mathcal{H},\pi)}}(u,R)$.

Mostraremos agora que existe $u \in \mathscr{C}$ tal que $B_{d_{(\mathcal{H},\pi)}}(0,R+1) \cap B_{d_{(\mathcal{H},\pi)}}(u,R+1) \neq \emptyset$, de fato, tome $u = c$, sabemos que $\delta_{(\mathcal{H},\pi)} - r_j = |Max(\langle supp_\pi(c)\rangle_\mathcal{H})| = 2l + \varepsilon$ para algum $l \in \mathbb{N}$ tal que $\varepsilon \in \{0,1\}$, então $l + \varepsilon = \lfloor(\delta_{(\mathcal{H},\pi)} - r_j - 1)/2\rfloor + 1$. Note que c possui exatamente $2l+\varepsilon$ blocos não nulos associados aos elementos maximais de $\langle supp_\pi(c)\rangle_\mathcal{H}$, suponha que as π-coordenadas desses blocos sejam os elementos do conjunto $I \sqcup J \sqcup \{l_\varepsilon\}$ de maneira que

$$I = \{i_1, \cdots, i_l\}, \quad J = \{j_1, \cdots, j_l\}$$

e $\{l_\varepsilon\} = \emptyset$ se $\varepsilon = 0$. Seja $x = (x_1, \cdots, x_m)$ o vetor definido por

$$x_i = \begin{cases} c_i & \text{se} \quad i \in J \\ 0 & \text{se} \quad i \notin J \end{cases}$$

onde $x_i \in \mathbb{F}_q^{k_i}$ e $c = (c_1, \cdots, c_m)$. Temos então que

$$d(x,c) = r_j + |I \cup \{l_\varepsilon\}| = r_j + l + \varepsilon$$

e

$$d(x,0) = r_j + |J| = r_j + l.$$

Donde segue que $x \in B_{d_{(\mathcal{H},\pi)}}(0, r_j + l + \varepsilon) \cap B_{d_{(\mathcal{H},\pi)}}(c, r_j + l + \varepsilon)$, ou seja, $x \in B_{d_{(\mathcal{H},\pi)}}(0,R+1) \cap B_{d_{(\mathcal{H},\pi)}}(c,R+1)$, e portanto $R = \lfloor(\delta_{(\mathcal{H},\pi)} - r_j - 1)/2\rfloor$ é o raio de empacotamento do (P,π)-código linear $\mathscr{C}$. ■

Corolário 41. *Seja $(\mathcal{A},\pi)$ uma estrutura de poset-block anticadeia. Se $\mathscr{C}$ é um código em $\mathbb{F}_q^n$ com parâmetros $[n,k,\delta_{(\mathcal{A},\pi)}]_q$, então*

$$R_{d_{(\mathcal{A},\pi)}}(\mathscr{C}) = \left\lfloor \frac{\delta_{(\mathcal{A},\pi)} - 1}{2} \right\rfloor.$$

Se tomarmos no Corolário 41 a aplicação de dimensionamento trivial, obtemos o raio de empacotamento para os espaços de Hamming: $R_{d_H}(\mathscr{C}) = \lfloor(\delta-1)/2\rfloor$.

Corolário 42. *([21]) Seja (P,π) um poset-block tal que $P = \mathcal{C}$, ou seja, P é um poset cadeia. Se $\mathscr{C}$ é um código com parâmetros $[n,k,\delta_{(\mathcal{C},\pi)}]_q$, então*

$$R_{d_{(\mathcal{C},\pi)}}(\mathscr{C}) = \delta_{(\mathcal{C},\pi)} - 1.$$

Definição 43. *(Códigos Perfeitos) Seja $\mathscr{C}$ um (P,π)-código linear em $\mathbb{F}_q^n$, diremos que $\mathscr{C}$ é um código perfeito se*

$$\mathbb{F}_q^n = \bigcup_{v\in\mathscr{C}} B_{(P,\pi)}(v, R_{d_{(P,\pi)}}(\mathscr{C})),$$

ou seja, se for possível cobrir o (P,π)-espaço com bolas disjuntas e de mesmo raio centradas nos elementos do código.

A distância mínima de um (P,π)-código linear pode ser vista como uma medida de qualidade desse código, desta forma podemos definir o seguinte problema clássico da teoria de códigos:

Problema 44. *Se (P,π) é uma estrutura de poset-block, para um dado comprimento e um número de palavras-códigos fixo, um problema fundamental é construir um (P,π)-código com esses parâmetros possuindo a maior distância mínima possível, de outro modo, dado n e $\delta_{(P,\pi)}$, o problema agora se torna encontrar um código no (P,π)-espaço de comprimento n e distância mínima $\delta_{(P,\pi)}$ possuindo a maior quantidade de palavras-código possível.*

Se $\mathscr{C}$ é um (P,π)-código linear de dimensão k em $\mathbb{F}_q^n$, como a cardinalidade das bolas são invariantes por translação no (P,π)-espaço, e como as bolas de raio $R_{d_{(P,\pi)}}(\mathscr{C})$ centradas em palavras-códigos são duas a duas disjuntas, então

$$|\mathscr{C}| = q^k \leqslant \frac{q^n}{1+\sum_{i=1}^{R_{d_{(P,\pi)}}(\mathscr{C})}\sum_{j=1}^{i}\sum_{I\in\Theta_j(i)}\prod_{m\in Max(I)}(q^{k_m}-1)\prod_{m\in I\setminus Max(I)}q^{k_m}}. \tag{2.1}$$

O limitante para o número de palavras-código (2.1) é chamado de *limitante do empacotamento de esferas*, quando a métrica poset-block coincide com a métrica de Hamming, é chamado de *limitante de Hamming*. Considere a seguinte função:

$$A(n,\delta_{(P,\pi)}) = max\{q^k : \text{ existe um } (P,\pi)\text{-código linear com parâmetros } [n,k,\delta_{(P,\pi)}]_q \text{ em } \mathbb{F}_q^n\}$$

onde q é um número fixo. Pelo limitante do empacotamento de esferas,

$$A(n,\delta_{(P,\pi)}) \leqslant \frac{q^n}{1+\sum_{i=1}^{R_{d_{(P,\pi)}}(\mathscr{C})}\sum_{j=1}^{i}\sum_{I\in\Theta_j(i)}\prod_{m\in Max(I)}(q^{k_m}-1)\prod_{m\in I\setminus Max(I)}q^{k_m}}.$$

Definição 45. *Um (P,π)-código linear $\mathscr{C}$ com parâmetros $[n,k,\delta_{(P,\pi)}]_q$ será chamado de código ótimo se $|\mathscr{C}| = A(n,\delta_{(P,\pi)})$.*

Pela Definição 45, um (P,π)-código linear é dito perfeito se, e somente se, o limitante do empacotamento de esferas é atingido, o que é equivalente a dizer que todo código perfeito é um código ótimo, portanto, os códigos perfeitos são soluções para casos particulares do problema 44. Por esse motivo, a busca por códigos perfeitos é um campo de pesquisa de grande interesse em teoria de códigos. Em 1973, a classificação dos códigos lineares perfeitos em espaços de Hamming foi estabelecida, veja [26]. As desigualdades (1.2) implicam que existe uma liberdade maior para construirmos estruturas de poset-block que tornam um determinado código perfeito, ou seja, é de se esperar que existam mais códigos perfeitos (com relação as métricas poset-block) além dos já classificados na métrica de Hamming. Exemplos que justificam essa afirmação, são as classificações dos posets que tornam perfeitos o código binário de Golay estendido e o código binário de Hamming estendido dados em [9] e [8] respectivamente, e a prova da existência de determinados códigos perfeitos em métricas de bloco dada em [4].

Dados $u, v \in \mathbb{F}_q^n$, seja $u \cdot v$ o produto interno usual formal em $\mathbb{F}_q$ entre u e v, isto é,

$$u \cdot v = u_1 v_1 + \cdots + u_n v_n$$

onde $u = (u_1, \cdots, u_n)$, $v = (v_1, \cdots, v_n)$ e $u_i, v_i \in \mathbb{F}_q$ para todo $i \in \{1, \cdots, n\}$.

Definição 46. *Seja $\mathscr{C}$ um (P,π)-código com parâmetros $[n,k,\delta_{(P,\pi)}]_q$. O $(\overline{P},\pi)$-código linear definido por*

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

é chamado de código dual de $\mathscr{C}$.

Para um dado (P,π)-código linear $\mathscr{C}$, seu código dual é claramente um subespaço linear de $\mathbb{F}_q^n$. Como a dimensão de $\mathscr{C}^{\perp}$ independe da métrica empregada, segue que $(\mathscr{C}^{\perp})^{\perp} = \mathscr{C}$ e $\mathscr{C}^{\perp}$ é um subespaço $(n-k)$-dimensional de $\mathbb{F}_q^n$ assim como no caso clássico da métrica de Hamming, portanto $\mathscr{C}^{\perp}$ é um $(\overline{P},\pi)$-código linear com parâmetros $[n, n-k, \delta_{(\overline{P},\pi)}]_q$. Note que em (P,π)-espaços a métrica em $\mathscr{C}^{\perp}$ é diferente da métrica em $\mathscr{C}$, tal mudança é motivada pela definição de código dual em espaços posets apresentada em [12], dessa maneira, quando tomarmos a estrutura de blocos trivial, nossa definição coincidirá com a efetuada nas métricas poset. A notação $\mathscr{C}^{\perp}$ é uma notação formal para o código dual, não podemos confundi-la

com o complemento ortogonal de espaços vetoriais sobre $\mathbb{R}$, pois no caso de corpos finitos os subespaços $\mathscr{C}$ e $\mathscr{C}^{\perp}$ eventualmente possuem intersecção não trivial, em certas circunstâncias, $\mathscr{C} = \mathscr{C}^{\perp}$, e nesse caso, dizemos que $\mathscr{C}$ é um código *auto-dual*.

Exemplo 47. *Seja $(\mathcal{H}, \pi)$ o poset-block do Exemplo 39. O código dual de*

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

é o $(\overline{\mathcal{H}}, \pi)$-código linear com parâmetros $[4,3,1]_2$ dado por

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

2.2 Distribuição de Pesos

Sejam $\mathbb{F}_q^n$ um (P,π)-espaço e $\mathscr{C}$ um (P,π)-código linear, denote por $A_{i,(P,\pi)}(\mathscr{C})$ o número de palavras-código de $\mathscr{C}$ com (P,π)-peso igual a i, ou seja,

$$A_{i,(P,\pi)}(\mathscr{C}) \triangleq |\{v \in \mathscr{C} : w_{(P,\pi)}(v) = i\}|.$$

Se (P,π) é um poset block em $[m]$, a distribuição de (P,π)-pesos de um código (também chamada de (P,π)-espectro do código) é a sequência ordenada finita

$$Spec(\mathscr{C}) \triangleq (A_{0,(P,\pi)}(\mathscr{C}), A_{1,(P,\pi)}(\mathscr{C}), \cdots, A_{m,(P,\pi)}(\mathscr{C})).$$

Não havendo possibilidade de confusão, usaremos uma notação simplificada para os elementos do (P,π)-espectro: $A_{i,(P,\pi)}(\mathscr{C}) = A_i$ e $A_{i,(\overline{P},\pi)}(\mathscr{C}^{\perp}) = A_i^{\perp}$. Uma importante linha de pesquisa em teoria de códigos é voltada para o cálculo da distribuição de pesos de códigos específicos ou famílias de códigos. Mesmo que em geral o espectro não determina unicamente um código, ele é um invariante de relevante importância pois nos dá informações tanto de natureza prática quanto teórica do código, por exemplo, permite determinar a probabilidade de erro na transmissão associada ao código, [18].

Se P é um poset em $[m]$ e se $\mathscr{C}$ é um (P,π)-código linear com parâmetros $[n,k,\delta_{(P,\pi)}]_q$, é claro que $A_0 + A_1 + \cdots + A_m = q^k$ e $A_0 = 1$, além disso, pela definição de distância mínima segue que $A_1 = \cdots = A_{\delta_{(P,\pi)}-1} = 0$.

Exemplo 48. *Seja $(\mathcal{H}, \pi)$ o poset-block do Exemplo 39. O código*

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

é um $(\mathcal{H}, \pi)$-código linear com parâmetros $[4,1,2]_2$ e (P,π)-espectro $(1,0,1,0)$, ou seja, $A_0 = 1$, $A_1 = 0$, $A_2 = 1$ e $A_3 = 0$. Além disso, como

$$\mathscr{C}_2^{\perp} = \{(0,0,0,0),(1,0,0,0),(0,0,1,0),(0,0,0,1),(1,0,1,0),(1,0,0,1)(0,0,1,1)(1,0,1,1)\},$$

então $A_0^{\perp} = 1$, $A_1^{\perp} = 3$, $A_2^{\perp} = 0$ e $A_3^{\perp} = 4$, ou seja, o $(\overline{P},\pi)$-espectro de $\mathscr{C}_2^{\perp}$ é dado por $(1,3,0,4)$.

Uma forma de expressar o (P,π)-espectro de um código, que proporciona uma forma mais algébrica para desenvolvermos nosso objetivo, é através de polinômios, os chamados (P,π)-polinômios de distribuição de (P,π)-pesos de $\mathscr{C}$, ou simplesmente, polinômio enumerador de $\mathscr{C}$.

Definição 49. *Dados P um poset em $[m]$ e um (P,π)-código linear $\mathscr{C}$, o polinômio enumerador de $\mathscr{C}$ é o polinômio*

$$W_{\mathscr{C},(P,\pi)}(x) \triangleq \sum_{u\in\mathscr{C}} x^{w_{(P,\pi)}(u)} = \sum_{i=0}^{m} A_{i,(P,\pi)}(\mathscr{C})x^i.$$

Em espaços de Hamming, um dos mais importantes resultados sobre distribuição de pesos é o conjunto de relações estabelecidas entre a distribuição de pesos de um código $\mathscr{C}$ e a distribuição de pesos do seu dual, das quais implica, em particular, que a distribuição de pesos do código $\mathscr{C}$ é unicamente determinada pela distribuição de pesos de $\mathscr{C}^{\perp}$, e vice-versa. Para a demonstração dessas relações, necessitamos de ferramentas (polinômios de Krawtchowk e caracteres aditivos em $\mathbb{F}_q$) que são apresentadas nos Apêndices A e B.

Lema 50. *Seja π uma aplicação de dimensionamento de um poset P em $[m]$ tal que $n = \sum_{j\in[m]} k_j$. Se V é um espaço vetorial sobre os complexos e $\{f_j : \mathbb{F}_q^{k_j} \to V\}_{j\in[m]}$ é uma família finita de funções, então*

$$\sum_{v\in\mathbb{F}_q^n}\prod_{j=1}^{m} f_j(v_j) = \prod_{j=1}^{m}\left(\sum_{v_j\in\mathbb{F}_q^{k_j}} f_j(v_j)\right).$$

Demonstração. Se $m = 1$, o lema é verdadeiro pois nesse caso $n = 1$. Assuma que o lema seja verdadeiro para $m-1$. Para todo $w \in \mathbb{F}_q^{k_m}$, defina

$$\mathbb{F}_{q,w}^n \triangleq \{v \in \mathbb{F}_q^n : w = v_m\}.$$

É claro que $\{\mathbb{F}_{q,w}^{k_m}\}_{w\in\mathbb{F}_q^{k_m}}$ é uma partição de $\mathbb{F}_q^n$, logo

$$\begin{aligned}\sum_{v\in\mathbb{F}_q^n}\prod_{j=1}^{m} f_j(v_j) &= \sum_{w\in\mathbb{F}_q^{k_m}}\sum_{v\in\mathbb{F}_{q,w}^n} f_m(w)\prod_{j=1}^{m-1} f_j(v_j)\\ &= \sum_{w\in\mathbb{F}_q^{k_m}}\sum_{(v_1,\cdots,v_{m-1})\in\mathbb{F}_q^{n-k_m}} f_m(w)\prod_{j=1}^{m-1} f_j(v_j)\\ &= \sum_{w\in\mathbb{F}_q^{k_m}} f_m(w)\sum_{(v_1,\cdots,v_{m-1})\in\mathbb{F}_q^{n-k_m}}\prod_{j=1}^{m-1} f_j(v_j). \qquad (2.2)\end{aligned}$$

Por hipótese de indução temos que

$$\sum_{(v_1,\cdots,v_{m-1})\in\mathbb{F}_q^{n-k_m}}\prod_{j=1}^{m-1} f_j(v_j) = \prod_{j=1}^{m-1}\sum_{v_j\in\mathbb{F}_q^{k_j}} f_j(v_j). \qquad (2.3)$$

Portanto de (2.2) e (2.3) o resultado segue. ■

Definição 51. *Dado $s\in\mathbb{N}$, seja $\delta_s:\mathbb{F}_q^s\to\{0,1\}$ a função delta de Kroneker definida por*

$$\delta_s(v)\triangleq\begin{cases}1, & se\ v\neq 0\in\mathbb{F}_q^s\\ 0, & se\ v=0\in\mathbb{F}_q^s\end{cases}.$$

Faremos agora uma breve descrição dos resultados sobre caracteres necessários para o desenvolvimento deste trabalho, para uma descrição mais detalhada contendo as demonstrações que aqui forem omitidas, consulte o Apêndice A.

Um *caracter não trivial* χ do grupo aditivo $\mathbb{F}_q$ é um homomorfismo de $\mathbb{F}_q$ no grupo multiplicativo dos números complexos tal que $\chi(a)\neq 1$ para algum $a\in\mathbb{F}_q$. Sendo χ um caracter não trivial de $\mathbb{F}_q$, se $\mathscr{C}$ é um código linear em $\mathbb{F}_q^n$ e f é uma função complexa também em $\mathbb{F}_q^n$, a *fórmula da soma discreta de Poisson* é dada por

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

onde $\widehat{f}(u)\triangleq\sum_{v\in\mathbb{F}_q^n}\chi(u\cdot v)f(v)$ é a *transformada de Hadamard* de f.

Teorema 52. *(Identidades de MacWilliams em espaços de Hamming) Seja $\mathbb{F}_q^n$ um espaço de Hamming, se $\mathscr{C}$ é um código linear sobre $\mathbb{F}_q$ com parâmetros $[n,k,\delta]_q$, então*

$$W_{\mathscr{C}^\perp}(x) = \frac{1}{|\mathscr{C}|}(1+(q-1)x)^n W_{\mathscr{C}}\left(\frac{1-x}{1+(q-1)x}\right). \qquad (2.4)$$

Demonstração. Sejam χ um caracter aditivo não trivial de $\mathbb{F}_q$ e $f : \mathbb{F}_q^n \to \mathbb{C}[x]$ a função definida por $f(u) = x^{w_H(u)}$, onde $w_H(u)$ denota o peso de Hamming do vetor u, isto é, $w_H(u) = d_H(u, 0)$. A transformada de Hadamard de f é dada por

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

Como $v = (v_1, \cdots, v_n)$ é tal que $v_i \in \mathbb{F}_q$ para todo $i \in \{1, \cdots, n\}$, então $w_H(v) = \delta_1(v_1) + \cdots + \delta_1(v_n)$, portanto

$$\begin{aligned}\widehat{f}(u) &= \sum_{(v_1,\cdots,v_n) \in \mathbb{F}_q^n} \chi(u_1 v_1 + \cdots + u_n v_n) x^{\delta_1(v_1)+\cdots+\delta_1(v_n)} \\ &= \sum_{(v_1,\cdots,v_n) \in \mathbb{F}_q^n} \prod_{j=1}^{n} \chi(u_j v_j) x^{\delta_1(v_j)}.\end{aligned}$$

Sejam $f_j(v) = \chi(u_j v_j) x^{\delta_1(v_j)}$ para todo $j \in \{1, \cdots, n\}$ e π uma aplicação de dimensionamento trivial em $[n]$, tomando $m = n$, do Lema 50 segue que

$$\widehat{f}(u) = \prod_{j=1}^{n} \sum_{\alpha \in \mathbb{F}_q} \chi(u_j \alpha) x^{\delta_1(\alpha)}. \tag{2.5}$$

Dado $u \in \mathbb{F}_q^n$,

- se $u_j = 0$ para algum $j \in \{1, \cdots, n\}$, então

$$\sum_{\alpha \in \mathbb{F}_q} \chi(u_j \cdot \alpha) x^{\delta_1(\alpha)} = \sum_{\alpha \in \mathbb{F}_q} \chi(0) x^{\delta_1(\alpha)} = \sum_{\alpha \in \mathbb{F}_q} x^{\delta_1(\alpha)} = 1 + (q-1)x. \tag{2.6}$$

- se $u_j \neq 0$, então

$$\sum_{\alpha \in \mathbb{F}_q} \chi(u_j \alpha) x^{\delta_1(\alpha)} = 1 + \sum_{\alpha \in \mathbb{F}_q \setminus \{0\}} \chi(u_j \alpha) x.$$

  Pelo Lema 82, $\sum_{\alpha \in \mathbb{F}_q} \chi(u_j \alpha) = 0$, como $\chi(0) = 1$, então $\sum_{\alpha \in \mathbb{F}_q \setminus \{0\}} \chi(u_j \alpha) = -1$. Logo, se $u_j \neq 0$,

$$\sum_{\alpha \in \mathbb{F}_q} \chi(u_j \alpha) x^{\delta_1(\alpha)} = 1 - x. \tag{2.7}$$

Se $w_H(u) = k$, então existem k coordenadas não nulas de u e portanto $n - k$ nulas, logo de (2.5), (2.6) e (2.7) segue que

$$\widehat{f}(u) = (1-x)^{w_H(u)} (1 + (q-1)x)^{n - w_H(u)}.$$

Pela fórmula da soma discreta de Poisson (Lema 85),

$$W_{\mathscr{C}^\perp}(x) = \sum_{u\in\mathscr{C}^\perp} x^{w_H(u)} = \frac{1}{|\mathscr{C}|}\sum_{u\in\mathscr{C}}(1-x)^{w_H(u)}(1+(q-1)x)^{n-w_H(u)} \tag{2.8}$$
$$= \frac{1}{|\mathscr{C}|}(1+(q-1)x)^n \sum_{u\in\mathscr{C}}\left(\frac{1-x}{(1+(q-1)x)}\right)^{w_H(u)}$$
$$= \frac{1}{|\mathscr{C}|}(1+(q-1)x)^n W_{\mathscr{C}}\left(\frac{1-x}{(1+(q-1)x)}\right).$$

■

Como $\mathscr{C} = (\mathscr{C}^\perp)^\perp$ são dois (P,π)-códigos lineares, a Equação (2.4) é simétrica em relação ao código e seu dual, ou seja,

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

Corolário 53. *(Relação entre A_i e $A_i^\perp$) Seja $\mathscr{C}$ um código linear sobre $\mathbb{F}_q$ com parâmetros $[n,k,\delta]_q$, então para todo $i \in \{1,\cdots,n\}$*

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

além disso, $A_0^\perp = A_0$.

Demonstração. Sendo $\gamma = q-1$, pela Definição 86 (polinômio de Krawtchouk) encontrada no Apêndice B, segue que

$$(1-x)^{w_H(u)}(1+\gamma x)^{n-w_H(u)} = \sum_{i=0}^{n} P_i(w_H(u):n)x^i.$$

Portanto da Identidade (2.8),

$$W_{\mathscr{C}^\perp}(x) = \sum_{i=0}^{n} A_i^\perp x^i = \frac{1}{|\mathscr{C}|}\sum_{u\in\mathscr{C}}\sum_{i=0}^{n} P_i(w_H(u):n)x^i$$
$$= \sum_{i=0}^{n}\sum_{u\in\mathscr{C}}\frac{1}{|\mathscr{C}|}P_i(w_H(u):n)x^i. \tag{2.9}$$

A família $\{B_j\}_{j\in\{0,\cdots,n\}}$ definida por $B_j = \{v\in\mathscr{C} : w_H(v) = j\}$, determina uma partição do conjunto $\mathscr{C}$, então

$$\sum_{u\in\mathscr{C}}\frac{1}{|\mathscr{C}|}P_i(w_H(u):n) = \sum_{j=0}^{n}\sum_{\substack{u\in\mathscr{C}\\ w_H(u)=j}}\frac{1}{|\mathscr{C}|}P_i(j:n)$$
$$= \sum_{j=0}^{n}\frac{A_j}{|\mathscr{C}|}P_i(j:n), \tag{2.10}$$

ou seja,

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

Usando definição de igualdade entre polinômios, segue que

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

■

A Equação (2.4) que relaciona os polinômios de distribuição de pesos de um código e de seu dual, é conhecida como *Identidade de MacWilliams* pois foi apresentada por F. J. MacWilliams em [17] e [16]. Identidades do tipo MacWilliams se destacam em teoria de códigos pois estabelecem uma relação entre invariantes de códigos possuindo alta taxa de informação e códigos com baixa dimensão. Devido a esse resultado, em espaços de Hamming, o espectro de um código está unicamente determinado pelo espectro de seu dual, porém como veremos no exemplo a seguir, em geral não podemos fazer tal afirmação.

Exemplo 54. *Sejam $(\mathcal{H}, \pi)$ o poset-block hierárquico e $\mathscr{C}_1$ o código do Exemplo 39. Se $\mathscr{C}_2$ é o código do Exemplo 48, então*

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

É um simples exercício mostrar que

$$W_{\mathscr{C}_1^{\perp},(\overline{\mathcal{H}},\pi)}(x) = 1 + 2x + x^2 + 4x^3,$$

além disso, sabemos pelo Exemplo 48 que

$$W_{\mathscr{C}_2^{\perp},(\overline{\mathcal{H}},\pi)}(x) = 1 + 3x + 4x^3.$$

Portanto, o espectro de $\mathscr{C}_1$ não determina unicamente o espectro de $\mathscr{C}_1^{\perp}$.

Nosso principal objetivo é classificar os poset-block para os quais é possível determinar relações entre a distribuição de pesos de códigos e seus duais, ou seja, que satisfazem algum tipo de identidade de MacWilliams. Para isso, necessitamos da seguinte definição:

Definição 55. *Dizemos que um poset-block (P, π) admite a identidade de MacWilliams se, e somente se, para quaisquer código $\mathscr{C}$, o polinômio de distribuição de (P, π)-pesos de $\mathscr{C}$ for*

unicamente determinado pelo polinômio de distribuição de $(\overline{P},\pi)$*-pesos de* $\mathscr{C}^{\perp}$*, ou seja, se* $\mathscr{C}_1$ *e* $\mathscr{C}_2$ *são dois códigos quaisquer satisfazendo* $W_{\mathscr{C}_1,(P,\pi)}(x) = W_{\mathscr{C}_2,(P,\pi)}(x)$*, então* $W_{\mathscr{C}_1^{\perp},(\overline{P},\pi)}(x) = W_{\mathscr{C}_2^{\perp},(\overline{P},\pi)}(x)$*.*

Se (P,π) é uma estrutura de poset-block com π sendo a aplicação de dimensionamento trivial, em [12] foi mostrado que (P,π) admite uma identidade de MacWilliams se, e somente se, P for um poset hierárquico. Porém, se π é não trivial e $(\mathcal{H},\pi)$ é um poset-block hierárquico, não é verdade em geral que $(\mathcal{H},\pi)$ admite uma identidade de MacWilliams, veja o Exemplo 54.

Definição 56. *Seja* (P,π) *um poset-block com* t *níveis. O* (P,π)*-polinômio de distribuição de pesos por níveis de um* (P,π)*-código linear* $\mathscr{C}$ *é a expressão formal*

$$W_{\mathscr{C},(P,\pi)}(x;y_0,\cdots,y_t) \triangleq \sum_{u\in\mathscr{C}} x^{w_{(P,\pi)}(u)} y_{s_P(u)},$$

onde $s_P(u) \triangleq max\{i : u^i \in \mathbb{F}_q^{b_i}\backslash\{0\}\}$*,* $s_P(0) = 0$ *e* b_i *é a dimensão do* i*-ésimo nível do poset-block* (P,π)*.*

A Definição 56 é similar a utilizada em [12] na classificação dos espaços posets que admitem a identidade de MacWilliams, ou seja, no caso em que a estrutura de blocos é trivial. É claro que $W_{\mathscr{C},(P,\pi)}(x) = W_{\mathscr{C},(P,\pi)}(x;1,\cdots,1)$. Tomando $j \in \{1,\cdots,t\}$, o coeficiente do termo $x^i y_j$ representa o número de palavras-código de (P,π)-peso i possuindo o nível j do poset como sendo o maior nível contendo elementos do suporte dessa palavra-código

2.3 Estruturas de Poset-Block Hierárquico Regular por Nível

Dentre as estruturas de poset-block existentes, estamos interessados nas que admitem a identidade de MacWilliams, por esse motivo, passaremos a trabalhar com estruturas de poset-block possuindo determinadas características, que serão o objeto principal de interesse no decorrer deste trabalho.

Definição 57. *Seja* $(\mathcal{H},\pi)$ *um poset-block hierárquico com estrutura de níveis* $(m_1,\cdots,m_t)$*. Para todo* $i \in \{1,\cdots,t\}$ *e* $j \in \{1,\cdots,m_i\}$*, suponha* $\pi(r_i + j) = d_i$*, ou seja, quaisquer dois elementos pertencentes ao mesmo nível de* $\mathcal{H}$ *possuem mesma imagem pela aplicação* π*. Nestas condições, diremos que* $(\mathcal{H},\pi)$ *é um poset-block hierárquico regular por nível.*

Seja $(\mathcal{H},\pi)$ um poset-block hierárquico regular por nível com t níveis, se $\mathscr{C}$ é um $(\mathcal{H},\pi)$-código linear, pela definição do polinômio de distribuição de $(\mathcal{H},\pi)$-pesos por níveis de $\mathscr{C}$, segue que

$$W_{\mathscr{C}^\perp,(\overline{P},\pi)}(x;z_0,\cdots,z_t)=\sum_{u\in\mathscr{C}^\perp}x^{w_{(\overline{P},\pi)}(u)}z_{s_{\overline{P}}(u)}, \tag{2.11}$$

onde $s_{\overline{P}}(u)=max\{i:u^i\in\mathbb{F}_q^{\overline{b_i}}\backslash\{0\}\}$, $s_{\overline{P}}(0)=0$ e $\overline{b_i}$ denota a dimensão do i-ésimo nível de $\overline{P}$. Como $\Gamma^i_P=\Gamma^{(t+1)-i}_{\overline{P}}$, podemos escrever o polinômio de distribuição de $(\mathcal{H},\pi)$-pesos por níveis de $\mathscr{C}$ com base na dimensão dos níveis do poset P. Defina $s'_{\overline{P}}(u)=min\{i:u^i\in\mathbb{F}_q^{b_i}\backslash\{0\}\}$ e $s'_{\overline{P}}(0)=t+1$, ou seja, $s'_{\overline{P}}(u)=(t+1)-s_{\overline{P}}(u)$. Logo, ao definirmos

$$W_{\mathscr{C}^\perp,(\overline{P},\pi)}(x;y_{t+1},\cdots,y_1)\triangleq\sum_{u\in\mathscr{C}^\perp}x^{w_{(\overline{P},\pi)}(u)}y_{s'_{\overline{P}}(u)}, \tag{2.12}$$

então os coeficientes de z_i em (2.11) coincidem com os coeficientes de $y_{(t+1)-i}$ em (2.12). Portanto se $z_i=y_{(t+1)-i}$ para todo $i\in\{0,\cdots,t\}$,

$$W_{\mathscr{C}^\perp,(\overline{P},\pi)}(x;z_0,\cdots,z_t)=W_{\mathscr{C}^\perp,(\overline{P},\pi)}(x;y_{t+1},\cdots,y_1).$$

A dimensão do i-ésimo nível de $(\mathcal{H},\pi)$ é dada por

$$b_i=\sum_{j=1}^{m_i}\pi(r_i+j)=m_id_i.$$

Se $\mathscr{C}$ é um $(\mathcal{H},\pi)$-código linear, o conjunto

$$\mathscr{C}_i\triangleq\{u\in\mathscr{C}:\widetilde{u^{i+1}}=0\in\mathbb{F}_q^{\widehat{b_i}}\} \tag{2.13}$$

é um sub-código de $\mathscr{C}$ que pode ser escrito como $\mathscr{C}_i=\mathscr{C}_i^0\sqcup\mathscr{C}_i^1$ onde

$$\mathscr{C}_i^0\triangleq\{u\in\mathscr{C}_i:u^i=0\in\mathbb{F}_q^{b_i}\} \tag{2.14}$$

e

$$\mathscr{C}_i^1\triangleq\{u\in\mathscr{C}_i:u^i\neq0\in\mathbb{F}_q^{b_i}\}. \tag{2.15}$$

Como $(\mathcal{H},\pi)$ é um poset-block hierárquico regular por nível, se u,v são elementos de $\mathscr{C}$ satisfazendo $w_{(\mathcal{H},\pi)}(u)=w_{(\mathcal{H},\pi)}(v)$, então $s_{\mathcal{H}}(u)=s_{\mathcal{H}}(v)$. Logo o $(\mathcal{H},\pi)$-polinômio de distribuição de pesos por níveis de $\mathscr{C}$ é dado por

$$\begin{aligned}W_{\mathscr{C}}(x;y_0,\cdots,y_t)=A_0y_0+(A_1x+\cdots+A_{m_1}x^{m_1})y_1\\+(A_{m_1+1}x^{m_1+1}+\cdots+A_{m_1+m_2}x^{m_1+m_2})y_2\\+\cdots\\+(A_{m_1+\cdots+m_{t-1}+1}x^{m_1+\cdots+m_{t-1}+1}+\cdots+A_{m_1+\cdots+m_t}x^{m_1+\cdots+m_t})y_t,\end{aligned}$$

além disso, do fato de $m - \widehat{m_i} = m_0 + m_1 + \cdots + m_i$ e $m_0 = 0$, segue que

$$\begin{aligned} W_{\mathscr{C}}(x; y_0, \cdots, y_t) &= A_0 y_0 + (A_{m-\widehat{m_0}+1} x^{m-\widehat{m_0}+1} + \cdots + A_{m-\widehat{m_1}} x^{m-\widehat{m_1}}) y_1 \\ &\quad + (A_{m-\widehat{m_1}+1} x^{m-\widehat{m_1}+1} + \cdots + A_{m-\widehat{m_2}} x^{m-\widehat{m_2}}) y_2 \\ &\quad + \cdots \\ &\quad + (A_{m-\widehat{m_{t-1}}+1} x^{m-\widehat{m_{t-1}}+1} + \cdots + A_{m-\widehat{m_t}} x^{m-\widehat{m_t}}) y_t \\ &= A_0 y_0 + \sum_{i=1}^{t} (A_{m-\widehat{m_{i-1}}+1} x^{m-\widehat{m_{i-1}}+1} + \cdots + A_{m-\widehat{m_i}} x^{m-\widehat{m_i}}) y_i \\ &= A_0 y_0 + \sum_{i=1}^{t} \left(\sum_{j=1}^{m_i} A_{m-\widehat{m_{i-1}}+j} x^{m-\widehat{m_{i-1}}+j} \right) y_i \\ &= A_0 y_0 + \sum_{i=1}^{t} \left(\sum_{j=1}^{m_i} A_{r_i+j} x^{r_i+j} \right) y_i. \end{aligned} \tag{2.16}$$

Para $i \in \{1, \cdots, t\}$, defina o polinômio enumerador do i-ésimo nível do poset-block por

$$LW^{(i)}_{\mathscr{C},(\mathcal{H},\pi)}(x) \triangleq \sum_{j=1}^{m_i} A_{r_i+j} x^{r_i+j}. \tag{2.17}$$

Os coeficientes desse polinômio representam a distribuição de pesos das palavras-código de $\mathscr{C}$ cujo π-suporte contém elementos do i-ésimo nível de $\mathcal{H}$ e não contém elementos acima desse nível. Tome $LW^{(0)}_{\mathscr{C}}(x) = A_0$, portanto de (2.16) e (2.17),

$$W_{\mathscr{C},(\mathcal{H},\pi)}(x; y_0, y_1, \cdots, y_t) = \sum_{i=0}^{t} LW^{(i)}_{\mathscr{C},(\mathcal{H},\pi)}(x) y_i. \tag{2.18}$$

É claro que se $y_j = 1$ para todo $j \in \{0, \cdots, i\}$ onde $i \in \{1, \cdots, t\}$ e $y_k = 0$ para todo $k > i$, então o $(\mathcal{H}, \pi)$-polinômio enumerador de pesos por níveis de $\mathscr{C}$ se torna o $(\mathcal{H}, \pi)$-polinômio enumerador de pesos do subespaço $\mathscr{C}_i$, além disso, pelas definições de $\mathscr{C}_i$ e $\mathscr{C}_i^1$ segue que

$$W_{\mathscr{C}_i,(\mathcal{H},\pi)}(x) - W_{\mathscr{C}_{i-1},(\mathcal{H},\pi)}(x) = LW^{(i)}_{\mathscr{C},(\mathcal{H},\pi)}(x) = \sum_{u \in \mathscr{C}_i^1} x^{w_{(\mathcal{H},\pi)}(u)}. \tag{2.19}$$

Sabemos que se tomarmos $y_j = 1$ para todo $j \in \{0, \cdots, t\}$, então o polinômio enumerador de pesos por níveis de $\mathscr{C}$ se torna o $(\mathcal{H}, \pi)$-polinômio enumerador de pesos usual, como aqui o poset-block é hierárquico regular por nível, segue que

$$W_{\mathscr{C},(\mathcal{H},\pi)}(x; 1, 1, \cdots, 1) = W_{\mathscr{C},(\mathcal{H},\pi)}(x) = \sum_{i=0}^{t} LW^{(i)}_{\mathscr{C},(\mathcal{H},\pi)}(x).$$

Definição 58. *Seja $(\mathcal{H}, \pi)$ um poset-block hierárquico regular por nível em $[m]$. Se $u, v \in \mathbb{F}_q^n$, para todo $i \in \{1, \cdots, t\}$, a π_i-distância entre u^i e v^i é definida por*

$$d_{\pi_i}(u^i, v^i) = |\{r_i + j : u_{r_i+j} \neq u_{r_i+j} \ e \ 1 \leqslant j \leqslant m_i\}|.$$

O conjunto $\{r_i + 1, \cdots, r_i + m_i\}$ será chamado de π_i-coordenadas de $\mathbb{F}_q^{b_i}$, além disso, o π_i-peso de u é o número inteiro $w_{\pi_i}(u^i) = d_{\pi_i}(u^i, 0)$. O π_i-suporte de u é o subconjunto dos elementos $r_i + j$ pertencentes as π_i-coordenadas de $\mathbb{F}_q^{b_i}$ tais que $u_{r_i+j} = 0 \in \mathbb{F}_q^{k_{r_i+j}}$, portanto

$$d_{\pi_i}(u^i, v^i) = |supp_{\pi_i}(u - v)|.$$

Capítulo 3

Espaços Poset-Block que Admitem a Identidade de MacWilliams

Como o título já sugere, neste capítulo apresentaremos a classificação dos poset-block que admitem a identidade de MacWilliams. Como consequência, assim como feito para os espaços de Hamming no Capítulo 2, explicitaremos as relações existentes entre os polinômios enumeradores de um código e seu dual.

3.1 Condição Necessária

Nesta seção encontraremos condições necessárias para que uma estrutura de poset-block admita a identidade de MacWilliams. Posteriormente, veremos que tais condições não serão apenas necessárias mas também condições suficientes para que a estrutura de poset-block admita a identidade de MacWilliams.

Os quatro lemas abaixo são os equivalentes para o caso poset-block dos Lemas (2.1), (2.2), (2.3) e (2.4) de [12]. Apesar de suas provas serem mais delicadas do que no caso poset (onde os blocos são triviais), elas seguem de maneira similar.

Para os lemas abaixo, seja (P, π) um poset-block com estrutura de nível $(m_1, \cdots, m_t)$.

Lema 59. *Dado $u \in \mathbb{F}_q^n$, então*

$$w_{(\overline{P},\pi)}(u) = m \Longleftrightarrow supp_\pi(u) \supset \Gamma_P^1.$$

Demonstração. Note que $w_{(\overline{P},\pi)}(u) = m$ se, e somente se, $Max(\overline{P}) \subset supp_\pi(u)$, ou seja, se e somente se, $\Gamma_P^1 \subset supp_\pi(u)$, pois como já vimos no Capítulo 1, $Max(\overline{P}) = \Gamma_P^1$. ■

Lema 60. *Se $u \in \mathbb{F}_q^n$ é tal que $supp_\pi(u) \subset \Gamma_P^1$, então*

$$q^{n-b_1} \mid |\{v \in \mathbb{F}_q^n : u \cdot v = 0 \text{ e } w_{(\overline{P},\pi)}(v) = m\}|$$

onde $a \mid b$ denota que a divide b e b_1 é a dimensão do nível 1 de P.

Demonstração. Seja $u \in \mathbb{F}_q^n$ tal que $supp_\pi(u) \subset \Gamma_P^1$. Podemos supor sem perda de generalidade que P está rotulado naturalmente, ou seja, $\Gamma_P^1 = \{1, 2, \cdots, m_1\}$. Além disso tal rotulamento em Γ_P^1 pode ser tomado de forma que $u = (u_1, \cdots, u_i, 0, \cdots, 0)$ onde $i \leqslant m_1$ e $u_j \in \mathbb{F}_q^{k_j} \setminus \{0\}$ para todo $j \in \{1, \cdots, i\}$. Sejam

$$A \triangleq \{(v_1, \cdots, v_i) \in \mathbb{F}_q^{k_1+\cdots+k_i} : v_j \in \mathbb{F}_q^{k_j} \setminus \{0\} \ \forall\ 1 \leqslant j \leqslant i \text{ e } u_1 \cdot v_1 + \cdots + u_i \cdot v_i = 0\}$$

e

$$B \triangleq \{(v_1, \cdots, v_{m_1}) \in \mathbb{F}_q^{b_1} : v_j \in \mathbb{F}_q^{k_j} \setminus \{0\} \ \forall\ 1 \leqslant j \leqslant m_1 \text{ e } u_1 \cdot v_1 + \cdots + u_i \cdot v_i = 0\}.$$

Como cada espaço $\mathbb{F}_q^{k_j}$ possui $q^{k_j} - 1$ vetores não nulos, existem $\prod_{j=i+1}^{m_1}(q^{k_j} - 1)$ possibilidades de entradas não nulas nos vetores das π-coordenadas de $\mathbb{F}_q^n$ referentes ao conjunto $\{i+1, \cdots, m_1\}$, logo

$$|B| = |A| \prod_{j=i+1}^{m_1} (q^{k_j} - 1). \tag{3.1}$$

Se

$$C \triangleq \{v \in \mathbb{F}_q^n : u \cdot v = 0 \text{ e } w_{(\overline{P},\pi)}(v) = m\},$$

pelo Lema 59 obtemos que

$$C = \{v \in \mathbb{F}_q^n : u \cdot v = 0 \text{ e } supp_\pi(v) \supset \Gamma_P^1\}.$$

Note que se $v = (v_1, \cdots, v_{m_1}, \cdots, v_m) \in C$ então $(v_1, \cdots, v_{m_1}) \in B$. Como não impomos restrição nos $m - m_1$ blocos restantes de $v \in C$, ou seja, nos vetores v_i possuindo π-coordenada

pertencente ao conjunto $\{m_1+1,\cdots,m\}$, segue que $|C| = |B|q^{k_{m_1+1}+\cdots+k_m} = |B|q^{n-b_1}$, o que é equivalente por (3.1) a

$$|C| = q^{n-b_1}|A|\prod_{j=i+1}^{m_1}(q^{k_j}-1)$$

e portanto $q^{n-b_1} \mid |C|$, ou seja,

$$q^{n-b_1} \mid |\{v \in \mathbb{F}_q^n : u_1\cdot v_1+\cdots+u_i\cdot v_i = 0 \text{ e } supp_\pi(v) \supset \Gamma_P^1\}|.$$

■

Lema 61. *Se um poset-block (P,π) admite a identidade de MacWilliams, então $j \preceq_P i$ para todo $i \in \Gamma_P^2$ e $j \in \Gamma_P^1$.*

Demonstração. Assumindo que $\Gamma_P^2 \neq \emptyset$, segue que $m > m_1$. Suponha que existam $i \in \Gamma_P^2$ e $j \in \Gamma_P^1$ tais que i e j não são comparáveis. Então, $|\langle i\rangle_P| < 1+|\Gamma_P^1|$, de modo que existem $u,v \in \mathbb{F}_q^n$ tais que $supp_\pi(u) = \{i\}$, $supp_\pi(v) \subset \Gamma_P^1$ e $w_{(P,\pi)}(u) = w_{(P,\pi)}(v)$. Sem perda de generalidade podemos assumir que $u = e_{s(2,1,1)}$. Sejam $\mathscr{C}_u$ e $\mathscr{C}_v$ dois (P,π)-códigos lineares gerados por u e v respectivamente (gerados no sentido de espaço vetorial). Como $\mathscr{C}_u$ e $\mathscr{C}_v$ são espaços vetoriais unidimensionais e $w_{(P,\pi)}(u) = w_{(P,\pi)}(v)$, $\mathscr{C}_u$ e $\mathscr{C}_v$ possuem o mesmo (P,π)-polinômio enumerador. Por hipótese (P,π) admite a identidade de MacWilliams, então os $(\overline{P},\pi)$-códigos lineares $\mathscr{C}_u^\perp$ e $\mathscr{C}_v^\perp$ possuem o mesmo $(\overline{P},\pi)$-polinômio enumerador, em particular $A_{m,(\overline{P},\pi)}(\mathscr{C}_u^\perp) = A_{m,(\overline{P},\pi)}(\mathscr{C}_v^\perp)$, ou seja,

$$|\{x \in \mathscr{C}_u^\perp : w_{(\overline{P},\pi)}(x) = m\}| = |\{x \in \mathscr{C}_v^\perp : w_{(\overline{P},\pi)}(x) = m\}|. \tag{3.2}$$

Pelo Lema 59,

$$|\{x \in \mathscr{C}_u^\perp : w_{(\overline{P},\pi)}(x) = m\}| = |\{x \in \mathscr{C}_u^\perp : \Gamma_P^1 \subset supp_\pi(x)\}|. \tag{3.3}$$

Da definição de código dual, $x \in \mathscr{C}_u^\perp$ se, e somente se, $x\cdot u' = 0$ para todo $u' \in \mathscr{C}_u$. Logo se $x \in \mathscr{C}_u^\perp$ então $x\cdot u = 0$ e como $u = e_{s(2,1,1)}$, então $x \in \mathscr{C}_u^\perp$ se, e somente se, $x \in \mathbb{F}_q^n$ e $x_{r_2+1}^1 = 0 \in \mathbb{F}_q$, ou seja,

$$|\{x \in \mathscr{C}_u^\perp : \Gamma_P^1 \subset supp_\pi(x)\}| = |\{x \in \mathbb{F}_q^n : x_{r_2+1}^1 = 0 \text{ e } \Gamma_P^1 \subset supp_\pi(x)\}|. \tag{3.4}$$

Portanto de (3.3) e (3.4) segue que

$$|\{x \in \mathscr{C}_u^\perp : w_{(\overline{P},\pi)}(x) = m\}| = |\{x \in \mathbb{F}_q^n : x_{r_2+1}^1 = 0 \text{ e } \Gamma_P^1 \subset supp_\pi(x)\}|. \tag{3.5}$$

Sejam

$$A \triangleq \{x_i \in \mathbb{F}_q^{k_i} : x_{r_2+1}^1 = 0\}$$

e

$$B \triangleq \{(x_1, \cdots, x_i, \cdots, x_m) : x_j \neq 0 \in \mathbb{F}_q^{k_j} \backslash \{0\} \ \forall \ j \in \Gamma_P^1 = \{1, \cdots, m_1\} \ \text{ e } x_i = 0 \in \mathbb{F}_q^{k_i}\}.$$

Note que B está bem definido pois $i \in \Gamma_P^2$. Se $x = (x_1, \cdots, x_i, \cdots, x_m) \in B$ e $y_i \in A$, substituindo x_i por y_i em x obtemos um vetor que denotaremos por x'. Por construção $\Gamma_P^1 \subset supp_\pi(x)$, como $x_i = 0$ implica que $x_{r_2+1}^1 = 0$ pois esta é uma das coordenadas de x_i, então por (3.5) segue que $x' \in \mathscr{C}_u^\perp$. Desta maneira, para cada $x \in B$ temos $|A| = q^{k_i - 1}$ possibilidades de construir x', além disso todos os elementos de $\mathscr{C}_u^\perp$ com $(\overline{P}, \pi)$-peso igual a m podem ser construídos dessa forma. Como

$$|B| = q^{n-b_1-k_i} \prod_{j=1}^{m_1} (q^{k_j} - 1),$$

segue que

$$|\{x \in \mathscr{C}_u^\perp : w_{(\overline{P},\pi)}(x) = m\}| = |B||A| = q^{n-b_1-1} \prod_{j=1}^{m_1} (q^{k_j} - 1). \tag{3.6}$$

Por outro lado, se $x \in \mathbb{F}_q^n$ é tal que $x \cdot v = 0$, como $\mathscr{C}_v$ é um subespaço unidimensional de $\mathbb{F}_q^n$, então $x \in \mathscr{C}_v^\perp$, logo

$$\{x \in \mathscr{C}_v^\perp : w_{(\overline{P},\pi)}(x) = m\} = \{x \in \mathbb{F}_q^n : x \cdot v = 0 \text{ e } w_{(\overline{P},\pi)}(x) = m\}. \tag{3.7}$$

Usando o Lema 60 na Igualdade (3.7), pelas Equações (3.2) e (3.6) segue que

$$q^{n-b_1} \big| q^{n-b_1-1} \prod_{j=1}^{m_1} (q^{k_j} - 1),$$

portanto

$$q \big| \prod_{j=1}^{m_1} (q^{k_j} - 1).$$

Como q é potência de primo, suponha $q = p^r$, então $p \big| (q^{k_j} - 1)$ para algum $j \in \{1, \cdots, m_1\}$, o que é um absurdo pois $p \big| q^{k_j}$ para todo $j \in \{1, \cdots, m_1\}$ e p é um número primo. Portanto $|\langle i \rangle_P| = 1 + |\Gamma_P^1|$, ou seja, $j \preceq_P i$ para todo $j \in \Gamma_P^1$. ■

Seja $P^j = P \backslash \cup_{i=1}^j \Gamma_P^i$. Considere em P^j a ordem induzida por P e seja $\pi^j = \pi|_{[m]\backslash \cup_{i=1}^j \Gamma_P^i}$ a restrição da aplicação π ao conjunto $[m] \backslash \cup_{i=1}^j \Gamma_P^i$. Podemos então enunciar o seguinte Lema:

Lema 62. *Se um poset-block (P,π) admite a identidade de MacWilliams, então o poset-block (P^1,π^1) também admite.*

Demonstração. Se $m = m_1$ temos que $[m]\backslash\Gamma_P^1 = \emptyset$, suponha então $m > m_1$. Sejam $\mathscr{C}_1'$ e $\mathscr{C}_2'$ códigos lineares de comprimento $n - b_1$ e mesmo (P^1,π^1)-polinômio enumerador. Sejam

$$\mathscr{C}_1 = \mathbb{F}_q^{b_1} \oplus \mathscr{C}_1' \triangleq \{(u,v) : u \in \mathbb{F}_q^{b_1} \text{ e } v \in \mathscr{C}_1'\}$$

e

$$\mathscr{C}_2 = \mathbb{F}_q^{b_1} \oplus \mathscr{C}_2' \triangleq \{(u,v) : u \in \mathbb{F}_q^{b_1} \text{ e } v \in \mathscr{C}_2'\}$$

dois (P,π)-códigos lineares de comprimento $b_1 + (n - b_1) = n$ obtidos através da extensão de $\mathscr{C}_1'$ e $\mathscr{C}_2'$ respectivamente. Pelo Lema 61, a relação entre os dois últimos níveis de (P,π) é hierárquica, como se $(u,v) \in \mathscr{C}_i$ então $supp_\pi((u,0)) \subset \Gamma_P^1$ e por hipótese (P,π) admite a identidade de MacWilliams, então $\mathscr{C}_1^\perp$ e $\mathscr{C}_2^\perp$ possuem o mesmo $(\overline{P},\pi)$-polinômio enumerador. Note que

$$\mathscr{C}_i^\perp = \{(u,v) \in \mathbb{F}_q^n : (u,v)\cdot(a,b) = 0 \ \forall\ a \in \mathbb{F}_q^{b_1} \text{ e } b \in \mathscr{C}_i'\},$$

além disso, como $(u,v)\cdot(a,b) = 0$ se, e somente se, $u\cdot a + v\cdot b = 0$, tomando $b = 0 \in \mathscr{C}_i'$ temos que $u\cdot a = 0$ para todo $a \in \mathbb{F}_q^{b_1}$, ou seja, $u = 0 \in \mathbb{F}_q^{b_1}$. Logo

$$\mathscr{C}_i^\perp = \{(u,v) : u = 0 \in \mathbb{F}_q^{b_1} \text{ e } v\cdot b = 0 \ \forall\ b \in \mathscr{C}_i'\},$$

sendo assim,

$$\mathscr{C}_i^\perp = \{(u,v) : u = 0 \in \mathbb{F}_q^{b_1} \text{ e } v \in \mathscr{C}_i'^\perp\}.$$

Pelo Lema 61, $w_{(P,\pi)}(0,v) = w_{(P_1,\pi_1)}(v) + |\Gamma_P^1|$, portanto $\mathscr{C}_1'^\perp$ e $\mathscr{C}_2'^\perp$ possuem o mesmo $(\overline{P^1},\pi^1)$-polinômio enumerador, logo o poset-block (P^1,π^1) admite a identidade de MacWilliams. ■

Por indução, usando os Lemas 61 e 62 temos a seguinte condição necessária para um poset-block (P,π) admitir a identidade de MacWilliams.

Proposição 63. *Se um poset-block (P,π) admite a identidade de MacWilliams, então P é um poset hierárquico.*

Pelo Exemplo 54 podemos concluir que a condição anterior não é suficiente para assegurar a existência da identidade de MacWilliams, a seguinte condição é também necessária:

Proposição 64. *Suponha que o poset-block (P,π) admite a identidade de MacWilliams. Então, $\pi(j_1)=\pi(j_2)$ para todo $j_1,j_2\in\Gamma_P^i$ e todo $1\leqslant i\leqslant h(P)$, ou seja, blocos pertencentes ao mesmo nível possuem mesma dimensão.*

Demonstração. Suponha que para algum $i\in\{1,\cdots,h(P)\}$ existam dois elementos $j_1,j_2\in\Gamma_P^i$ tais que $\pi(j_1)\leqslant\pi(j_2)$. Sejam $\mathscr{C}_u$ e $\mathscr{C}_v$ dois (P,π)-códigos lineares unidimensionais de comprimento n gerados por $u=e_{s(i,j_1-r_i,1)}$ e $v=e_{s(i,j_2-r_i,1)}$ respectivamente. Pela Proposição 63 o poset P é hierárquico, como existem

$$(q^{k_{j_1}-1}-1)+\sum_{\substack{j\in\Gamma_P^i\\ j\neq j_1}}(q^{k_j}-1)$$

elementos em $\mathscr{C}_u^\perp$ com suporte em um único bloco no i-ésimo nível de P, então

$$A_{m_{i+1}+\cdots+m_t+1,(\overline{P},\pi)}(\mathscr{C}_u^\perp)=(q^{k_{j_1}-1}-1)\prod_{\substack{j\in\Gamma_P^l\\ i<l\leqslant t}}q^{k_j}+\sum_{\substack{j\in\Gamma_P^i\\ j\neq j_1}}(q^{k_j}-1)\prod_{\substack{j\in\Gamma_P^l\\ i<l\leqslant t}}q^{k_j}$$

pois considerando o poset dual $\overline{P}$ não existem restrições nas coordenadas dos blocos pertencentes aos níveis maiores (em P) do que i. De uma maneira similar podemos mostrar que

$$A_{m_{i+1}+\cdots+m_t+1,(\overline{P},\pi)}(\mathscr{C}_v^\perp)=(q^{k_{j_2}-1}-1)\prod_{\substack{j\in\Gamma_P^l\\ i<l\leqslant t}}q^{k_j}+\sum_{\substack{j\in\Gamma_P^i\\ j\neq j_2}}(q^{k_j}-1)\prod_{\substack{j\in\Gamma_P^l\\ i<l\leqslant t}}q^{k_j}.$$

Assumindo que o poset-block (P,π) admite a identidade de MacWilliams, segue que

$$A_{m_{i+1}+\cdots+m_t+1,(\overline{P},\pi)}(\mathscr{C}_u^\perp)=A_{m_{i+1}+\cdots+m_t+1,(\overline{P},\pi)}(\mathscr{C}_v^\perp),$$

ou seja, $\pi(j_1)=\pi(j_2)$. ■

Das Proposições 63 e 64 segue o teorema abaixo:

Teorema 65. *Se um poset-block (P,π) admite a identidade de MacWilliams então (P,π) é um poset-block hierárquico regular por nível.*

3.2 Condição Suficiente

O objetivo principal desta seção é mostrar que a condição necessária para que um poset-block admita a identidade de MacWilliams obtida na seção anterior, é também suficiente. Para

atingirmos tal objetivo, faremos uma demonstração construtiva utilizando caracteres aditivos sobre corpos finitos. Os conceitos relacionados com caracteres aditivos que utilizaremos estão descritos no Apêndice A, tais conceitos foram utilizados de forma similar inicialmente por F. J. MacWilliams em [17], e posteriormente em [10], [12] e [11] para as demonstrações das identidades de MacWilliams em espaços de Hamming e em espaços poset, respectivamente. Sejam

- $(\mathcal{H}, \pi)$ um poset-block hierárquico regular por nível em $[m]$ possuindo estrutura de nível $(m_1, \cdots, m_t)$ tal que $n = \sum_{j\in[m]} \pi(j)$;
- χ um caracter aditivo não trivial em $\mathbb{F}_q$ e
- $\mathscr{C}$ um $(\mathcal{H}, \pi)$-código linear em $\mathbb{F}_q^n$.

Como visto no Teorema 52, identidades de MacWilliams em espaços de Hamming são obtidas aplicando a fórmula discreta de Poisson na função $f(u) = x^{w_H(u)}$. Em espaços poset, as identidades de MacWilliams foram obtidas em [12] aplicando a fórmula discreta de Poisson na função $f(u) = x^{w_P(u)} z_{s'_{\overline{P}}(u)}$ onde P é um poset dado. Como por (2.12),

$$W_{\mathscr{C},(\overline{\mathcal{H}},\pi)}(x; z_{t+1}, \cdots, z_1) = \sum_{u\in\mathscr{C}^\perp} x^{w_{(\overline{\mathcal{H}},\pi)}(u)} z_{s'_{\overline{\mathcal{H}}}(u)},$$

seja $f : \mathbb{F}_q^n \to \mathbb{C}[x, z_1, \cdots, z_{t+1}]$ a função definida por $f(u) = x^{w_{(\overline{\mathcal{H}},\pi)}(u)} z_{s'_{\overline{\mathcal{H}}}(u)}$. Nosso trabalho agora é escrever $\sum_{u\in\mathscr{C}^\perp} f(u)$ em função do $(\mathcal{H}, \pi)$-polinômio enumerador de $\mathscr{C}$.

Sejam $B_0 = \{(u^1, \cdots, u^t) \in \mathbb{F}_q^n : u^1 \neq 0 \in \mathbb{F}_q^{b_1}\}$ e $B_t = \{0\} \subset \mathbb{F}_q^n$. Para $i \in \{1, \cdots, t-1\}$, definimos

$$B_i \triangleq \{(u^1, \cdots, u^t) \in \mathbb{F}_q^n : u^j = 0 \in \mathbb{F}_q^{b_j} \ \forall\ j \in \{1, \cdots, i\} \text{ e } u^{i+1} \neq 0 \in \mathbb{F}_q^{b_{(i+1)}}\}.$$

Dessa forma, a família $\{B_i\}_{i\in\{0,\cdots,t\}}$ determina uma partição de $\mathbb{F}_q^n$, isto é, $\mathbb{F}_q^n = \sqcup_{i=0}^t B_i$. Portanto, a transformada de Hadamard de f pode ser expressa da seguinte forma:

$$\begin{aligned}\widehat{f}(u) = \sum_{v\in\mathbb{F}_q^n} \chi(u\cdot v) f(v) &= \sum_{i=0}^{t} \sum_{v\in B_i} \chi(u\cdot v) f(v) \\ &= \sum_{i=0}^{t} \sum_{v\in B_i} \chi(u\cdot v) x^{w_{(\overline{\mathcal{H}},\pi)}(v)} z_{s'_{\overline{\mathcal{H}}}(v)}.\end{aligned}$$

Denote $S_i(u) = \sum_{v \in B_i} \chi(u \cdot v) x^{w_{(\overline{\mathcal{H}},\pi)}(v)} z_{s'_{\overline{\mathcal{H}}}(v)}$. Como $B_t = \{0\}$ e $s'_{\overline{\mathcal{H}}}(0) = t+1$, então

$$\widehat{f}(u) = \sum_{i=0}^{t} S_i(u) = S_t(u) + \sum_{i=0}^{t-1} S_i(u) = z_{t+1} + \sum_{i=0}^{t-1} S_i(u) = z_{t+1} + \sum_{i=1}^{t} S_{i-1}(u). \tag{3.8}$$

Pela fórmula da soma discreta de Poisson,

$$|\mathscr{C}| \sum_{v \in \mathscr{C}^\perp} f(v) = \sum_{u \in \mathscr{C}} \widehat{f}(u),$$

portanto reduzimos o problema de escrever $\sum_{u \in \mathscr{C}^\perp} f(u)$ em função do $(\overline{\mathcal{H}}, \pi)$-polinômio enumerador de $\mathscr{C}$ ao problema de escrever $\sum_{u \in \mathscr{C}} \widehat{f}(u)$ em função desse polinômio.

Como $(\overline{\mathcal{H}}, \pi)$ é um poset-block hierárquico regular por nível em $[m]$ com t níveis, para todo $i \in \{1, \cdots, t\}$, podemos assumir que:

- $r_i = m_0 + m_1 + \cdots + m_{i-1}$ onde $m_0 = 0$;
- $\Gamma^i_{\mathcal{H}} = \{r_i + 1, \cdots, r_i + m_i\}$ ($\mathcal{H}$ está rotulado naturalmente);
- $d_i = \pi(r_i + j) = k_{(r_i+j)}$ para todo $j \in \{1, \cdots, m_i\}$;
- $b_i = m_i d_i$ é tal que $\sum_{i=1}^{t} b_i = n$ e
- $\gamma_i = (q^{d_i} - 1)$.

Além disso, para todo $i \in \{1, \cdots, t\}$, defina

$$Q_i(x) \triangleq \left(\frac{1-x}{1+\gamma_i x}\right), \tag{3.9}$$

$$a_i(x) \triangleq q^{\widehat{b_i}} \left(\frac{1+\gamma_i x}{x}\right)^{m - \widehat{m_i}} (1-x)^{\widehat{m_{i-1}}} \quad \text{e} \tag{3.10}$$

$$c_i(x) \triangleq x^{\widehat{m_i}} q^{\widehat{b_i}} \left(\frac{1-x}{Q_i(x)}\right)^{m_i}. \tag{3.11}$$

Sejam também g_j e h_j definidos da seguinte maneira:

$$g_j \triangleq \begin{cases} \sum_{i=j+1}^{t} c_i(x) z_i, & \text{se } 0 \leqslant j \leqslant t-1 \\ 0, & \text{se } j = t \end{cases} \quad \text{e} \tag{3.12}$$

$$h_j \triangleq \begin{cases} \sum_{i=j}^{t} z_i x^{\widehat{m_i}} q^{\widehat{b_i}}, & \text{se } 1 \leqslant j \leqslant t \\ \sum_{i=1}^{t} z_i x^{\widehat{m_i}} q^{\widehat{b_i}}, & \text{se } j = 0 \end{cases}. \tag{3.13}$$

Proposição 66. *Com as condições e definições acima estabelecidas, temos que*

$$W_{\mathscr{C}^\perp,(\overline{\mathcal{H}},\pi)}(x;z_{t+1},\cdots,z_1) = z_{t+1} + \frac{1}{|\mathscr{C}|}\left(\frac{x}{1-x}\right)^m \sum_{i=1}^{t} a_i(x) z_i LW^{(i)}_{\mathscr{C},(\mathcal{H},\pi)}(Q_i(x)) + \frac{1}{|\mathscr{C}|}W_{\mathscr{C},(\mathcal{H},\pi)}(1;g_0,\cdots,g_t) - \frac{1}{|\mathscr{C}|}W_{\mathscr{C},(\mathcal{H},\pi)}(1;h_0,\cdots,h_t).$$

Demonstração. Como a demonstração dessa proposição é um tanto longa, será dividida em 5 passos, cada um necessário para a demonstração do subsequente. A hipótese de (P,π) ser um poset-block hierárquico regular por níveis é utilizada já no primeiro destes passos.

Passo 1. *Mostraremos inicialmente que para todo $u \in \mathbb{F}_q^n$ e $i \in \{1,\cdots,t\}$,*

$$S_{i-1}(u) = z_i x^{\widehat{m_i}} q^{\widehat{b_i}}[(1-x)^{w_{\pi_i}(u^i)}(1+\gamma_i x)^{m_i - w_{\pi_i}(u^i)} - 1]$$

se $\widetilde{u^{i+1}} = 0 \in \mathbb{F}_q^{\widehat{b_i}}$ e

$$S_{i-1}(u) = 0$$

se $\widetilde{u^{i+1}} \neq 0 \in \mathbb{F}_q^{\widehat{b_i}}$.

De fato, como $\mathcal{H}$ é hierárquico, se $v \in B_{i-1}$ para algum $i \in \{1,\cdots,t\}$,

$$w_{(\overline{\mathcal{H}},\pi)}(v) = m_{i+1} + \cdots + m_t + w_{\pi_i}(v^i) = \widehat{m_i} + w_{\pi_i}(v^i)$$

onde $w_{\pi_i}(v^i)$ é o π_i-peso de v obtido a partir da Definição 58. Se $v \in B_{i-1}$, então $s'_{\overline{\mathcal{H}}}(v) = i$, logo

$$\begin{aligned} S_{i-1}(u) &= \sum_{v\in B_{i-1}} \chi(u\cdot v) x^{w_{(\overline{\mathcal{H}},\pi)}(v)} z_{s'_{\overline{\mathcal{H}}}(v)} \\ &= \sum_{v\in B_{i-1}} \chi(u\cdot v) x^{\widehat{m_i}+w_{\pi_i}(v^i)} z_i \\ &= z_i x^{\widehat{m_i}} \sum_{v\in B_{i-1}} \chi(u\cdot v) x^{w_{\pi_i}(v^i)}. \end{aligned} \tag{3.14}$$

Dado $v \in \mathbb{F}_q^n$, podemos denotar $v = (v^1,\cdots,v^i,\widetilde{v^{i+1}})$ e assim sendo, para todo $u \in \mathbb{F}_q^n$ e $v \in B_{i-1}$, o produto interno entre u e v é dado por $u\cdot v = u^i\cdot v^i + \widetilde{u^{i+1}}\cdot\widetilde{v^{i+1}}$. Como χ é um

caracter aditivo não trivial de $\mathbb{F}_q$, então

$$\begin{aligned} z_i x^{\widehat{m_i}} \sum_{v\in B_{i-1}} \chi(u\cdot v) x^{w_{\pi_i}(v^i)} &= z_i x^{\widehat{m_i}} \sum_{v\in B_{i-1}} \chi(u^i\cdot v^i)\chi(\widetilde{u^{i+1}}\cdot\widetilde{v^{i+1}}) x^{w_{\pi_i}(v^i)} \\ &= z_i x^{\widehat{m_i}} \sum_{\substack{v^i\in\mathbb{F}_q^{b_i}\setminus\{0\} \\ \widetilde{v^{i+1}}\in\mathbb{F}_q^{\widehat{b_i}}}} \chi(u^i\cdot v^i)\chi(\widetilde{u^{i+1}}\cdot\widetilde{v^{i+1}}) x^{w_{\pi_i}(v^i)} \\ &= z_i x^{\widehat{m_i}} \sum_{\widetilde{v^{i+1}}\in\mathbb{F}_q^{\widehat{b_i}}} \chi(\widetilde{u^{i+1}}\cdot\widetilde{v^{i+1}}) \sum_{v^i\in\mathbb{F}_q^{b_i}\setminus\{0\}} \chi(u^i\cdot v^i) x^{w_{\pi_i}(v^i)}. \end{aligned} \tag{3.15}$$

Portanto, de (3.14) e (3.15) segue que

$$S_{i-1}(u) = z_i x^{\widehat{m_i}} \sum_{\widetilde{v^{i+1}}\in\mathbb{F}_q^{\widehat{b_i}}} \chi(\widetilde{u^{i+1}}\cdot\widetilde{v^{i+1}}) \sum_{v^i\in\mathbb{F}_q^{b_i}\setminus\{0\}} \chi(u^i\cdot v^i) x^{w_{\pi_i}(v^i)}.$$

Para todo $i\in\{1,\cdots,t\}$, temos que $|\mathbb{F}_q^{\widehat{b_i}}| = q^{\widehat{b_i}}$, portanto do Lema 82,

$$\sum_{\widetilde{v^{i+1}}\in\mathbb{F}_q^{\widehat{b_i}}} \chi(\widetilde{u^{i+1}}\cdot\widetilde{v^{i+1}}) = \begin{cases} q^{\widehat{b_i}}, & \text{se } \widetilde{u^{i+1}} = 0\in\mathbb{F}_q^{\widehat{b_i}} \\ 0, & \text{se } \widetilde{u^{i+1}} \neq 0\in\mathbb{F}_q^{\widehat{b_i}} \end{cases},$$

ou seja,

$$S_{i-1}(u) = \begin{cases} z_i x^{\widehat{m_i}} q^{\widehat{b_i}} \displaystyle\sum_{v^i\in\mathbb{F}_q^{b_i}\setminus\{0\}} \chi(u^i\cdot v^i) x^{w_{\pi_i}(v^i)}, & \text{se } \widetilde{u^{i+1}} = 0\in\mathbb{F}_q^{\widehat{b_i}} \\ 0, & \text{se } \widetilde{u^{i+1}} \neq 0\in\mathbb{F}_q^{\widehat{b_i}} \end{cases}. \tag{3.16}$$

Como $\chi(0)=1$, então

$$\sum_{v^i\in\mathbb{F}_q^{b_i}} \chi(u^i\cdot v^i) x^{w_{\pi_i}(v^i)} = 1 + \sum_{v^i\in\mathbb{F}_q^{b_i}\setminus\{0\}} \chi(u^i\cdot v^i) x^{w_{\pi_i}(v^i)}. \tag{3.17}$$

Sabemos que u^i pode ser decomposto da seguinte maneira: $u^i = (u_{r_i+1},\cdots,u_{r_i+m_i})$ onde $u_{r_i+j}\in\mathbb{F}_q^{k_{r_i+j}}$ para todo $j\in\{1,\cdots,m_i\}$, logo como χ é um caracter aditivo, $\chi(u^i\cdot v^i) = \sum_{j=1}^{m_i}\chi(u_{r_i+j}\cdot v_{r_i+j})$. Sendo δ_s a função delta de Kroneker dada pela Definição 51, então $w_{\pi_i}(v^i) = \delta_{k_{(r_i+1)}}(v_{r_i+1}) + \cdots + \delta_{k_{(r_i+m_i)}}(v_{r_i+m_i})$ e portanto

$$\sum_{v^i\in\mathbb{F}_q^{b_i}} \chi(u^i\cdot v^i) x^{w_{\pi_i}(v^i)} = \sum_{v^i\in\mathbb{F}_q^{b_i}} \prod_{j=1}^{m_i} \chi(u_{r_i+j}\cdot v_{r_i+j}) x^{\delta_{k_{(r_i+j)}}(v_{r_i+j})}.$$

Pelo Lema 50,

$$\sum_{v^i\in\mathbb{F}_q^{b_i}} \chi(u^i\cdot v^i) x^{w_{\pi_i}(v^i)} = \prod_{j=1}^{m_i} \sum_{v_{r_i+j}\in\mathbb{F}_q^{k_{r_i+j}}} \chi(u_{r_i+j}\cdot v_{r_i+j}) x^{\delta_{k_{(r_i+j)}}(v_{r_i+j})}. \tag{3.18}$$

Note agora que:

- Se $r_i + j$ não pertence ao π_i-suporte de u, então

$$\sum_{v_{r_i+j} \in \mathbb{F}_q^{k_{r_i+j}}} \chi(u_{r_i+j} \cdot v_{r_i+j}) x^{\delta_{k_{(r_i+j)}}(v_{r_i+j})} = \sum_{v_{r_i+j} \in \mathbb{F}_q^{k_{r_i+j}}} x^{\delta_{k_{r_i+j}}(v_{r_i+j})} = 1 + (q^{k_{r_i+j}} - 1)x.$$

  Como $(\mathcal{H}, \pi)$ é um poset-block hierárquico regular por nível, dado $i \in \{1, \cdots, t\}$ então $k_{r_i+j_1} = k_{r_i+j_2}$ para todo $j_1, j_2 \in \{1, \cdots, m_i\}$. Definindo $d_i = k_{r_i+j}$ para todo $j \in \{1, \cdots, m_i\}$, segue que

$$\sum_{v_{r_i+j} \in \mathbb{F}_q^{k_{r_i+j}}} \chi(u_{r_i+j} \cdot v_{r_i+j}) x^{\delta_{k_{(r_i+j)}}(v_{r_i+j})} = 1 + (q^{d_i} - 1)x = 1 + \gamma_i x. \tag{3.19}$$

- Se $r_i + j$ pertence ao π_i-suporte de u, então $u_{r_i+j} \neq 0$. Pelo Lema 83, $\sum_{v_{r_i+j} \in \mathbb{F}_q^{k_{r_i+j}}} \chi(u_{r_i+j} \cdot v_{r_i+j}) = 0$, ou seja,

$$\sum_{v_{r_i+j} \in \mathbb{F}_q^{k_{r_i+j}} \setminus \{0\}} \chi(u_{r_i+j} \cdot v_{r_i+j}) = -1.$$

  Como $x^{\delta_{k_{(r_i+j)}}(0)} = 1$ e $x^{\delta_{k_{(r_i+j)}}(v_{r_i+j})} = x$ para todo v_{r_i+j} não nulo, então

$$\sum_{v_{r_i+j} \in \mathbb{F}_q^{k_{r_i+j}}} \chi(u_{r_i+j} \cdot v_{r_i+j}) x^{\delta_{k_{(r_i+j)}}(v_{r_i+j})} = 1 + x \sum_{v_{r_i+j} \in \mathbb{F}_q^{k_{r_i+j}} \setminus \{0\}} \chi(u_{r_i+j} \cdot v_{r_i+j}) = 1 - x. \tag{3.20}$$

Por definição, $w_{\pi_i}(u^i) = |supp_{\pi_i}(u)|$, então de (3.17), (3.18), (3.19) e (3.20),

$$\sum_{v^i \in \mathbb{F}_q^{b_i} \setminus \{0\}} \chi(u^i \cdot v^i) x^{w_{\pi_i}(u^i)} = (1-x)^{w_{\pi_i}(u^i)} (1 + \gamma_i x)^{m_i - w_{\pi_i}(u^i)} - 1.$$

Portanto, substituindo a igualdade acima em (3.16), para todo $i \in \{1, \cdots, t\}$ tem-se que

$$S_{i-1}(u) = \begin{cases} z_i x^{\widehat{m_i}} q^{\widehat{b_i}} [(1-x)^{w_{\pi_i}(u^i)} (1 + \gamma_i x)^{m_i - w_{\pi_i}(u^i)} - 1], & \text{se } \widetilde{u^{i+1}} = 0 \in \mathbb{F}_q^{\widehat{b_i}} \\ 0, & \text{se } \widetilde{u^{i+1}} \neq 0 \in \mathbb{F}_q^{\widehat{b_i}} \end{cases}.$$

Passo 2.

$$\begin{aligned} \sum_{u \in \mathscr{C}} \widehat{f}(u) =& |\mathscr{C}| z_{t+1} + \left(\frac{x}{1-x}\right)^m \sum_{i=1}^{t} a_i(x) z_i LW^{(i)}_{\mathscr{C},(\mathcal{H},\pi)}(Q_i(x)) + \sum_{i=1}^{t} z_i c_i(x) |\mathscr{C}_{i-1}| \\ & - \sum_{i=1}^{t} z_i x^{\widehat{m_i}} q^{\widehat{b_i}} |\mathscr{C}_i|. \end{aligned}$$

Como $\widetilde{u^{i+1}} = 0 \in \mathbb{F}_q^{\widehat{b_i}}$ para todo $u \in \mathscr{C}_i$, do Passo 1 segue que

$$\begin{aligned}\sum_{u\in\mathscr{C}_i} S_{i-1}(u) &= z_i x^{\widehat{m_i}} q^{\widehat{b_i}} \sum_{u\in\mathscr{C}_i} \left[(1-x)^{w_{\pi_i}(u^i)}(1+\gamma_i x)^{m_i - w_{\pi_i}(u^i)} - 1\right] \\ &= z_i x^{\widehat{m_i}} q^{\widehat{b_i}} \left[\left(\sum_{u\in\mathscr{C}_i} \left(\frac{1-x}{1+\gamma_i x}\right)^{w_{\pi_i}(u^i)} (1+\gamma_i x)^{m_i}\right) - |\mathscr{C}_i|\right].\end{aligned}$$

Pela Definição 2.13, se $u \in \mathscr{C}$, então $u \in \mathscr{C}_i$ se, e somente se, $\widetilde{u^{i+1}} = 0 \in \mathbb{F}_q^{\widehat{b_i}}$, ou seja, se $u \notin \mathscr{C}_i$ então $\widetilde{u^{i+1}} \neq 0 \in \mathbb{F}_q^{\widehat{b_i}}$, o que pelo Passo 1 implica $S_{i-1}(u) = 0$, logo

$$\sum_{u\in\mathscr{C}} S_{i-1}(u) = \sum_{u\in\mathscr{C}_i} S_{i-1}(u),$$

e portanto

$$\sum_{u\in\mathscr{C}} S_{i-1}(u) = z_i x^{\widehat{m_i}} q^{\widehat{b_i}} \left[(1+\gamma_i x)^{m_i} \left(\sum_{u\in\mathscr{C}_i} Q_i(x)^{w_{\pi_i}(u^i)}\right) - |\mathscr{C}_i|\right]. \tag{3.21}$$

Pelas características dos conjuntos $\mathscr{C}_i^0$ e $\mathscr{C}_i^1$ descritos respectivamente em (2.14) e (2.15), segue que

$$\sum_{u\in\mathscr{C}_i} Q_i(x)^{w_{\pi_i}(u^i)} = \sum_{u\in\mathscr{C}_i^1} Q_i(x)^{w_{\pi_i}(u^i)} + \sum_{u\in\mathscr{C}_i^0} Q_i(x)^{w_{\pi_i}(u^i)}. \tag{3.22}$$

Se $u \in \mathscr{C}_i^1$, então o π_i-suporte de u é não vazio, como $\widetilde{u^{i+1}} = 0 \in \mathbb{F}_q^{\widehat{b_i}}$ e o poset-block $(\mathcal{H}, \pi)$ é hierárquico,

$$w_{(\mathcal{H},\pi)}(u) = w_{\pi_i}(u^i) + r_i = w_{\pi_i}(u^i) + (m - \widehat{m_{i-1}}),$$

logo $Q_i(x)^{w_{\pi_i}(u^i)} = (1/Q_i(x)^{m-\widehat{m_{i-1}}}) Q_i(x)^{w_{(\mathcal{H},\pi)}(u)}$. Se $u \in \mathscr{C}_i^0$ então o π_i-suporte de u é vazio, logo $w_{\pi_i}(u^i) = 0$, ou seja, $\sum_{u\in\mathscr{C}_i^0} Q_i(x)^{w_{\pi_i}(u^i)} = |\mathscr{C}_i^0|$. Como $|\mathscr{C}_{i-1}| = |\mathscr{C}_i^0|$ pois $\mathscr{C}_{i-1} = \mathscr{C}_i^0$, de (3.22) segue que

$$\begin{aligned}\sum_{u\in\mathscr{C}_i} Q_i(x)^{w_{\pi_i}(u^i)} &= \sum_{u\in\mathscr{C}_i^1} Q_i(x)^{w_{\pi_i}(u^i)} + |\mathscr{C}_i^0| \\ &= \frac{1}{Q_i(x)^{m-\widehat{m_{i-1}}}} \sum_{u\in\mathscr{C}_i^1} Q_i(x)^{w_{(\mathcal{H},\pi)}(u)} + |\mathscr{C}_{i-1}|. \end{aligned}\tag{3.23}$$

Como $1 + \gamma_i x = [(1-x)/Q_i(x)]^{m_i}$, substituindo (3.23) em (3.21) obtemos uma nova expressão para $\sum_{u\in\mathscr{C}} S_{i-1}(u)$, isto é,

$$\begin{aligned}\sum_{u\in\mathscr{C}} S_{i-1}(u) &= x^{\widehat{m_i}}(1+\gamma_i x)^{m_i} \left(\frac{1+\gamma_i x}{1-x}\right)^{m-\widehat{m_{i-1}}} q^{\widehat{b_i}} z_i \sum_{u\in\mathscr{C}_i^1} Q_i(x)^{w_{(\mathcal{H},\pi)}(u)} \\ &\quad + z_i x^{\widehat{m_i}} q^{\widehat{b_i}} \left[\left(\frac{1-x}{Q_i(x)}\right)^{m_i} |\mathscr{C}_{i-1}| - |\mathscr{C}_i|\right]. \end{aligned}\tag{3.24}$$

Note que

$$x^{\widehat{m_i}}(1+\gamma_i x)^{m_i}\left(\frac{1+\gamma_i x}{1-x}\right)^{m-\widehat{m_{i-1}}} = \frac{x^m}{x^{m-\widehat{m_i}}}(1+\gamma_i x)^{m_i}\frac{(1+\gamma_i x)^{m-\widehat{m_{i-1}}}}{(1-x)^m}(1-x)^{\widehat{m_{i-1}}}$$
$$= \left(\frac{x}{1-x}\right)^m\left(\frac{1+\gamma_i x}{x}\right)^{m-\widehat{m_i}}(1-x)^{\widehat{m_{i-1}}}, \qquad (3.25)$$

pois $m-\widehat{m_{i-1}}+m_i = m-\widehat{m_i}$. Pelas igualdades dadas em (2.19), $\sum_{u\in\mathscr{C}_i^1} Q_i(x)^{w_{(\mathcal{H},\pi)}(u)} = LW^{(i)}_{\mathscr{C};(\mathcal{H},\pi)}(Q_i(x))$, portanto de (3.24) e (3.25) segue que

$$\sum_{u\in\mathscr{C}} S_{i-1}(u) = \left(\frac{x}{1-x}\right)^m q^{\widehat{b_i}}\left(\frac{1+\gamma_i x}{x}\right)^{m-\widehat{m_i}}(1-x)^{\widehat{m_{i-1}}} z_i LW^{(i)}_{\mathscr{C},(\mathcal{H},\pi)}(Q_i(x))$$
$$+z_i x^{\widehat{m_i}} q^{\widehat{b_i}}\left[\left(\frac{1-x}{Q_i(x)}\right)^{m_i}|\mathscr{C}_{i-1}| - |\mathscr{C}_i|\right]. \qquad (3.26)$$

Por (3.8), $\sum_{u\in\mathscr{C}}\widehat{f}(u) = |\mathscr{C}|z_{t+1} + \sum_{i=1}^t\sum_{u\in\mathscr{C}} S_{i-1}(u)$, substituindo (3.26) nessa igualdade, obtemos o resultado desejado, isto é,

$$\sum_{u\in\mathscr{C}}\widehat{f}(u) = |\mathscr{C}|z_{t+1} + \sum_{i=1}^t\left(\frac{x}{1-x}\right)^m q^{\widehat{b_i}}\left(\frac{1+\gamma_i x}{x}\right)^{m-\widehat{m_i}}(1-x)^{\widehat{m_{i-1}}} z_i LW^i_{\mathscr{C},(\mathcal{H},\pi)}(Q_i(x))$$
$$+\sum_{i=1}^t z_i x^{\widehat{m_i}} q^{\widehat{b_i}}\left(\frac{1-x}{Q_i(x)}\right)^{m_i}|\mathscr{C}_{i-1}| - \sum_{i=1}^t z_i x^{\widehat{m_i}} q^{\widehat{b_i}}|\mathscr{C}_i| \qquad (3.27)$$

Passo 3.

$$\sum_{i=1}^t z_i c_i(x)|\mathscr{C}_{i-1}| = W_{\mathscr{C},(\mathcal{H},\pi)}(1; g_0, \cdots, g_t).$$

Denotando $A_{i,(\mathcal{H},\pi)}(\mathscr{C}) = A_i$, pela definição de $\mathscr{C}_i$ segue que $|\mathscr{C}_0| = 0$ e

$$|\mathscr{C}_i| = A_0 + \sum_{j=1}^{m_1} A_j + \sum_{j=1}^{m_2} A_{m_1+j} + \cdots + \sum_{j=1}^{m_i} A_{r_i+j} = A_0 + \sum_{k=1}^{i}\sum_{j=1}^{m_k} A_{r_k+j} \qquad (3.28)$$

para todo $i \in \{1, \cdots, t\}$, então

$$\sum_{i=1}^t z_i c_i(x)|\mathscr{C}_{i-1}| = z_1 c_1(x)|\mathscr{C}_0| + z_2 c_2(x)|\mathscr{C}_1| + \cdots + z_t c_t(x)|\mathscr{C}_{t-1}|$$
$$= z_1 c_1(x) A_0 + z_2 c_2(x)\left(A_0 + \sum_{j=1}^{m_1} A_j\right) + \cdots + z_t c_t(x)\left(A_0 + \sum_{k=1}^{t-1}\sum_{j=1}^{m_k} A_{r_k+j}\right)$$
$$= A_0\sum_{j=1}^t c_j(x) z_j + \sum_{k=1}^{m_1} A_k \sum_{j=2}^t c_j(x) z_j + \cdots + \sum_{k=1}^{m_{t-1}} A_{r_{t-1}+k} c_t(x) z_t.$$

Como $LW^{(i)}_{\mathscr{C},(\mathcal{H},\pi)}(1) = \sum_{j=1}^{m_i} A_{r_i+j}$ e $LW^{(0)}_{\mathscr{C},(\mathcal{H},\pi)}(1) = A_0$, então

$$\sum_{i=1}^{t} z_i c_i(x)|\mathscr{C}_{i-1}| = A_0 \sum_{j=1}^{t} c_j(x)z_j + LW^{(1)}_{\mathscr{C},(\mathcal{H},\pi)}(1) \sum_{j=2}^{t} c_j(x)z_j + \cdots + LW^{(t-1)}_{\mathscr{C},(\mathcal{H},\pi)}(1)c_t(x)z_t$$
$$= \sum_{i=0}^{t-1} LW^{(i)}_{\mathscr{C},(\mathcal{H},\pi)}(1) \sum_{j=i+1}^{t} c_j(x)z_j. \tag{3.29}$$

Defina $g_i = \sum_{j=i+1}^{t} c_j(x)z_j$ se $i \in \{0, \cdots, t-1\}$ e $g_t = 0$, pela Identidade (2.18) e por (3.29) segue que

$$\sum_{i=1}^{t} z_i c_i(x)|\mathscr{C}_{i-1}| = W_{\mathscr{C},(\mathcal{H},\pi)}(1; g_0, \cdots, g_t).$$

Passo 4.

$$\sum_{i=1}^{t} z_i x^{\widehat{m_i}} q^{\widehat{b_i}} |\mathscr{C}_i| = W_{\mathscr{C},(\mathcal{H},\pi)}(1; h_0, ..., h_t).$$

Denote $A_{i,(\mathcal{H},\pi)}(\mathscr{C}) = A_i$. A demonstração segue de maneira análoga a demonstração do Passo 3, de fato, usando (3.28) segue que

$$\sum_{i=1}^{t} z_i x^{\widehat{m_i}} q^{\widehat{b_i}} |\mathscr{C}_i| = z_1 x^{\widehat{m_1}} q^{\widehat{b_1}} |\mathscr{C}_1| + \cdots + z_t x^{\widehat{m_t}} q^{\widehat{b_t}} |\mathscr{C}_t|$$
$$= z_1 x^{\widehat{m_1}} q^{\widehat{b_1}} \left(A_0 + \sum_{j=1}^{m_1} A_j \right) + \cdots + z_t x^{\widehat{m_t}} q^{\widehat{b_t}} \left(A_0 + \sum_{j=1}^{m_1} A_j + \cdots + \sum_{j=1}^{m_t} A_{r_t+j} \right).$$
$$= A_0 \sum_{i=1}^{t} z_i x^{\widehat{m_i}} q^{\widehat{b_i}} + \sum_{j=1}^{t} \left(\sum_{k=1}^{m_j} A_{r_j+k} \sum_{i=j}^{t} z_i x^{\widehat{m_i}} q^{\widehat{b_i}} \right)$$

Defina $h_j = \sum_{i=j}^{t} z_i x^{\widehat{m_i}} q^{\widehat{b_i}}$ se $j \in \{1, \cdots, t\}$ e $h_j = \sum_{i=1}^{t} z_i x^{\widehat{m_i}} q^{\widehat{b_i}}$ se $j = 0$, portanto

$$\sum_{i=1}^{t} z_i x^{\widehat{m_i}} q^{\widehat{b_i}} |\mathscr{C}_{i+1}| = \sum_{i=0}^{t} LW^{(i)}_{\mathscr{C},(\mathcal{H},\pi)}(1) h_i = W_{\mathscr{C},(\mathcal{H},\pi)}(1; h_0, \cdots, h_t).$$

Passo 5. *(Final)*

De (2.12) e (A.7) segue que

$$W_{\mathscr{C},(\overline{\mathcal{H}},\pi)}(x; z_{t+1}, \cdots, z_1) = \sum_{u \in \mathscr{C}^\perp} x^{w_{(\overline{\mathcal{H}},\pi)}(u)} z_{s'_{\overline{\mathcal{H}}}(u)} = \sum_{u \in \mathscr{C}^\perp} f(u) = \frac{1}{|\mathscr{C}|} \sum_{u \in \mathscr{C}} \widehat{f}(u). \tag{3.30}$$

Substituindo as equações dos Passos 3 e 4 na equação do Passo 2,

$$\frac{1}{|\mathscr{C}|}\sum_{u\in\mathscr{C}}\widehat{f}(u) = z_{t+1} + \frac{1}{|\mathscr{C}|}\left(\frac{x}{1-x}\right)^m \sum_{i=1}^{t} a_i(x) z_i LW^{(i)}_{\mathscr{C},(\mathcal{H},\pi)}(Q_i(x)) + \frac{1}{|\mathscr{C}|}W_{\mathscr{C},(\mathcal{H},\pi)}(1; g_0, \cdots, g_t) - \frac{1}{|\mathscr{C}|}W_{\mathscr{C},(\mathcal{H},\pi)}(1; h_0, ..., h_t). \tag{3.31}$$

Pelas Igualdades (3.30) e (3.31) o resultado segue.

■

Teorema 67. *Se $(\mathcal{H},\pi)$ é um poset-block hierárquico regular por nível, então $(\mathcal{H},\pi)$ admite a identidade de MacWilliams.*

Demonstração. Seja $\mathscr{C}$ um $(\mathcal{H},\pi)$-código linear, aplicando a Identidade (2.18) na Proposição 66 obtemos que

$$\begin{aligned} W_{\mathscr{C}^\perp,(\overline{\mathcal{H}},\pi)}(x; z_{t+1}, \cdots, z_1) = {} & z_{t+1} + \frac{1}{|\mathscr{C}|}\left(\frac{x}{1-x}\right)^m W_{\mathscr{C},(\mathcal{H},\pi)}(Q_1(x); 0, a_1(x)z_1, 0, 0, \cdots, 0) \\ & + \frac{1}{|\mathscr{C}|}\left(\frac{x}{1-x}\right)^m W_{\mathscr{C},(\mathcal{H},\pi)}(Q_2(x); 0, 0, a_2(x)z_2, 0, \cdots, 0) \\ & + \cdots + \frac{1}{|\mathscr{C}|}\left(\frac{x}{1-x}\right)^m W_{\mathscr{C},(\mathcal{H},\pi)}(Q_t(x); 0, 0, 0, \cdots, a_t(x)z_t) \\ & + \frac{1}{|\mathscr{C}|}W_{\mathscr{C},(\mathcal{H},\pi)}(1; g_0, \cdots, g_t) - \frac{1}{|\mathscr{C}|}W_{\mathscr{C},(\mathcal{H},\pi)}(1; h_0, \cdots, h_t). \end{aligned} \tag{3.32}$$

Se $\mathscr{C}_1$ é um $(\mathcal{H},\pi)$-código linear possuindo o mesmo $(\mathcal{H},\pi)$-polinômio enumerador do código $\mathscr{C}$, ao trocarmos $\mathscr{C}$ por $\mathscr{C}_1$ em (3.32), o lado direito não mudará pois $|\mathscr{C}| = |\mathscr{C}_1|$ e além disso, $\mathscr{C}$ e $\mathscr{C}_1$ possuem o mesmo $(\mathcal{H},\pi)$-polinômio enumerador. Portanto

$$W_{\mathscr{C}_1^\perp,(\overline{\mathcal{H}},\pi)}(x; 1, \cdots, 1) = W_{\mathscr{C}^\perp,(\overline{\mathcal{H}},\pi)}(x; 1, \cdots, 1),$$

ou seja, o $(\overline{\mathcal{H}},\pi)$-polinômio enumerador de $\mathscr{C}^\perp$ está unicamente determinado pelo $(\mathcal{H},\pi)$-polinômio enumerador de $\mathscr{C}$ para todo código $\mathscr{C}$, logo o poset-block $(\mathcal{H},\pi)$ admite a identidade de MacWilliams. ■

Portanto dos teoremas 65 e 67 temos a seguinte classificação:

Teorema 68. *Um poset-block (P,π) admite uma identidade do tipo MacWilliams se, e somente se, o poset-block é hierárquico regular por níveis.*

3.3 Relação Entre A_i e $A_i^{\perp}$

Daremos agora uma descrição explícita das relações existentes entre os coeficientes A_i e $A_i^{\perp}$ dos polinômios enumeradores dos códigos em questão. Sejam $(\mathcal{H},\pi)$ um poset-block hierárquico regular por nível e $\mathscr{C}$ um $(\mathcal{H},\pi)$-código linear em $\mathbb{F}_q^n$, usaremos aqui as definições e notações estabelecidas na seção anterior. Defina

$$E_1(x) \triangleq \sum_{i=1}^{t} q^{\widehat{b_i}} \left(\frac{1+\gamma_i x}{x}\right)^{m-\widehat{m_i}} (1-x)^{\widehat{m_{i-1}}} LW^{(i)}_{\mathscr{C},(\mathcal{H},\pi)}(Q_i(x))$$

e

$$E_2(x) \triangleq \sum_{i=1}^{t} x^{\widehat{m_i}} q^{\widehat{b_i}} \left(\left(\frac{1-x}{Q_i(x)}\right)^{m_i} |\mathscr{C}_{i-1}| - |\mathscr{C}_i| \right).$$

Pondo $z_1 = \cdots = z_{t+1} = 1$, de (3.27) e (2.12) segue que

$$W_{\mathscr{C}^{\perp},(\overline{\mathcal{H}},\pi)}(x) = \ 1 + \frac{1}{|\mathscr{C}|}\left(\frac{x}{1-x}\right)^{m} E_1(x) + \frac{1}{|\mathscr{C}|}E_2(x). \tag{3.33}$$

Como $Q_i(x) = (1-x)/(1+(q^{d_i}-1)x)$ e

$$LW^{(i)}_{\mathscr{C},(\mathcal{H},\pi)}(Q_i(x)) = \sum_{j=1}^{m_i} A_{r_i+j} Q_i(x)^{r_i+j},$$

então

$$\begin{aligned}
E_1(x) &= \sum_{i=1}^{t} q^{\widehat{b_i}} \left(\frac{1+\gamma_i x}{x}\right)^{m-\widehat{m_i}} (1-x)^{\widehat{m_{i-1}}} \sum_{j=1}^{m_i} A_{r_i+j} \left(\frac{1-x}{1+\gamma_i x}\right)^{m-\widehat{m_{i-1}}+j} \\
&= \sum_{i=1}^{t} \frac{q^{\widehat{b_i}}}{x^{m-\widehat{m_i}}} (1-x)^{\widehat{m_{i-1}}} \sum_{j=1}^{m_i} A_{r_i+j} (1+\gamma_i x)^{m_i-j} (1-x)^{m-\widehat{m_{i-1}}+j} \\
&= \sum_{i=1}^{t} \frac{q^{\widehat{b_i}}}{x^{m-\widehat{m_i}}} \sum_{j=1}^{m_i} A_{r_i+j} (1+\gamma_i x)^{m_i-j} (1-x)^{m+j}.
\end{aligned}$$

Como $\gamma_i = (q^{d_i}-1)$, então $(1+\gamma_i x)^{m_i-j}(1-x)^j$ é a função geradora dos polinômios de Krawtchowk

$$P_k^{\gamma_i}(j:m_i) = \sum_{l=0}^{k} (-1)^l \gamma_i^{k-l} \binom{j}{l} \binom{m_i-j}{k-l}$$

para todo $k \in \{0, \cdots, m_i\}$, (consulte Definição 87 do Apêndice B), então

$$\begin{aligned}\frac{1}{|\mathscr{C}|}\left(\frac{x}{1-x}\right)^m E_1(x) &= \frac{1}{|\mathscr{C}|}\sum_{i=1}^{t} q^{\widehat{b_i}} x^{\widehat{m_i}} \sum_{j=1}^{m_i} A_{r_i+j}(1+\gamma_i x)^{m_i-j}(1-x)^j \\ &= \frac{1}{|\mathscr{C}|}\sum_{i=1}^{t} q^{\widehat{b_i}} x^{\widehat{m_i}} \sum_{j=1}^{m_i} A_{r_i+j} \sum_{k=0}^{m_i} P_k^{\gamma_i}(j:m_i)x^k \\ &= \frac{1}{|\mathscr{C}|}\sum_{i=1}^{t} q^{\widehat{b_i}} x^{\widehat{m_i}} \sum_{k=0}^{m_i} \left(\sum_{j=1}^{m_i} A_{r_i+j} P_k^{\gamma_i}(j:m_i)\right) x^k.\end{aligned}$$

Defina agora

$$a_k(j:m_i) = \sum_{j=1}^{m_i} A_{r_i+j} P_k^{\gamma_i}(j:m_i),$$

note que $P_0^{\gamma_i}(j:m_i) = 1$ para todo $j \in \{1, \cdots, m_i\}$, então por (3.28) segue que

$$a_0(j:m_i) = \sum_{j=1}^{m_i} A_{r_i+j} = |\mathscr{C}_i| - |\mathscr{C}_{i-1}|.$$

Portanto

$$\frac{1}{|\mathscr{C}|}\left(\frac{x}{1-x}\right)^m E_1(x) = \frac{1}{|\mathscr{C}|}\sum_{i=1}^{t} q^{\widehat{b_i}} x^{\widehat{m_i}} \left(|\mathscr{C}_i| - |\mathscr{C}_{i-1}| + \sum_{k=1}^{m_i} a_k(j:m_i)x^k\right). \tag{3.34}$$

Do binômio de Newton temos que

$$(1+\gamma_i x)^{m_i} = \sum_{k=0}^{m_i}\binom{m_i}{k}(\gamma_i x)^k = 1 + \sum_{k=1}^{m_i}\binom{m_i}{k}\gamma_i^k x^k,$$

como $(1-x)/Q_i(x) = (1+\gamma_i x)$, da definição de $E_2(x)$ e da igualdade acima obtemos que

$$\begin{aligned}\frac{1}{|\mathscr{C}|}E_2(x) =& \frac{1}{|\mathscr{C}|}\sum_{i=1}^{t} x^{\widehat{m_i}} q^{\widehat{b_i}} \left[\left(1 + \sum_{k=1}^{m_i}\binom{m_i}{k}\gamma_i^k x^k\right)|\mathscr{C}_{i-1}| - |\mathscr{C}_i|\right] \\ =& \frac{1}{|\mathscr{C}|}\sum_{i=1}^{t} x^{\widehat{m_i}} q^{\widehat{b_i}} \left(|\mathscr{C}_{i-1}| - |\mathscr{C}_i| + \sum_{k=1}^{m_i}\binom{m_i}{k}\gamma_i^k |\mathscr{C}_{i-1}| x^k\right),\end{aligned} \tag{3.35}$$

portanto, substituindo (3.34) e (3.35) em (3.33) segue que

$$\begin{aligned}W_{\mathscr{C}^{\perp},(\overline{\mathcal{H}},\pi)}(x) =& 1 + \frac{1}{|\mathscr{C}|}\sum_{i=1}^{t} q^{\widehat{b_i}} x^{\widehat{m_i}} \left(|\mathscr{C}_i| - |\mathscr{C}_{i-1}| + \sum_{k=1}^{m_i} a_k(j:m_i)x^k\right) \\ &+ \frac{1}{|\mathscr{C}|}\sum_{i=1}^{t} x^{\widehat{m_i}} q^{\widehat{b_i}} \left(|\mathscr{C}_{i-1}| - |\mathscr{C}_i| + \sum_{k=1}^{m_i}\binom{m_i}{k}\gamma_i^k |\mathscr{C}_{i-1}| x^k\right) \\ =& 1 + \frac{1}{|\mathscr{C}|}\sum_{i=1}^{t} q^{\widehat{b_i}} x^{\widehat{m_i}} \left[\sum_{k=1}^{m_i}\left(a_k(j:m_i)\binom{m_i}{k}\gamma_i^k |\mathscr{C}_{i-1}|\right) x^k\right].\end{aligned} \tag{3.36}$$

Por outro lado, sabemos que

$$\begin{aligned} W_{\mathscr{C}^{\perp},(\overline{\mathcal{H}},\pi)}(x) =& A_0^{\perp} + (A_1^{\perp}x + \cdots + A_{m_t}^{\perp}x^{m_t}) \\ &+ (A_{m_t+1}^{\perp}x + \cdots + A_{m_t+m_{t-1}}^{\perp}x^{m_{t-1}})x^{m_t} \\ &+ \cdots + \\ &+ (A_{m_t+\cdots+m_2+1}^{\perp}x + \cdots + A_{m_t+\cdots+m_1}^{\perp}x^{m_1})x^{m_t+\cdots+m_2} \\ =& 1 + \sum_{i=1}^{t} x^{\widehat{m_i}} \sum_{k=1}^{m_i} A_{\widehat{m_i}+k}^{\perp}x^k. \end{aligned} \tag{3.37}$$

Portanto igualando (3.36) e (3.37) e fixando i e k, da igualdade entre tais polinômios segue que

$$A_{\widehat{m_i}+k,(\overline{\mathcal{H}},\pi)}^{\perp} = \frac{q^{\widehat{b_i}}}{|\mathscr{C}|}a_k(j:m_i) + \frac{q^{\widehat{b_i}}}{|\mathscr{C}|}\binom{m_i}{k}\gamma_i^k|\mathscr{C}_{i-1}|.$$

Temos então o seguinte teorema:

Teorema 69. *(Relação entre $A_{i,(\overline{\mathcal{H}},\pi)}^{\perp}$ e $A_{i,(\mathcal{H},\pi)}$) Se $(\mathcal{H},\pi)$ é um poset-block hierárquico regular por nível e $\mathscr{C}$ é um $(\mathcal{H},\pi)$-código linear, então*

$$A_{\widehat{m_i}+k,(\overline{\mathcal{H}},\pi)}^{\perp} = \frac{q^{\widehat{b_i}}}{|\mathscr{C}|}\sum_{j=1}^{m_i}(A_{r_i+j}P_k(j:m_i)) + \frac{q^{\widehat{b_i}}}{|\mathscr{C}|}\binom{m_i}{k}\gamma_i^k\sum_{j=0}^{r_i}A_j.$$

Se tomarmos a estrutura trivial de blocos, $b_j = m_j$ e $d_j = 1$ para todo $j \in \{1,\cdots,t\}$, então temos o resultado obtido no Teorema 4.4 de [12]. Por outro lado, se tomarmos o poset $\mathcal{H}$ como sendo anticadeia, isto é, nenhum de seus elementos são comparáveis, então $t = 1$ e $m = m_1$, portanto dado $k \in \{1,\cdots,m_1\}$ segue que

$$A_k^{\perp} = \frac{1}{|\mathscr{C}|}\left(\sum_{j=1}^{m}A_jP_k^{\gamma_1}(j:m) + \binom{m}{k}\gamma_1^k\right) = \frac{1}{|\mathscr{C}|}\sum_{j=0}^{m}A_jP_k^{\gamma_1}(j:m).$$

Apêndice A

Caracteres

A teoria de caracteres de grupos finitos foi uma ferramenta utilizada por F. J. MacWilliams em teoria de códigos para expressar a identidade de MacWilliams para códigos definidos em espaços com a métrica de Hamming (apresentada no Capítulo 2), posteriormente, tem sido utilizada por vários autores para expressar a identidade de MacWilliams nas métricas poset e poset-block. No desenvolvimento dos Capítulos 2 e 3 usamos dois lemas que são obtidos através das relações de ortogonalidade existentes entre caracteres. Nosso objetivo é portanto demonstrar tais lemas, assim como a fórmula da soma discreta de Poisson. Descreveremos aqui todos os caracteres de um grupo abeliano cíclico finito, obtendo assim todos os caracteres aditivos sobre $\mathbb{F}_q$. De uma forma geral, todos os resultados sobre caracteres que aqui estão demonstrados podem ser encontrados em [14], além disso, [18] descreve a teoria de caracteres tendo como foco a teoria de códigos. No que segue, G será um grupo abeliano finito de ordem k (para o qual utilizaremos a notação multiplicativa) com elemento neutro 1_G.

Definição 70. *Um caracter χ do grupo G é um homomorfismo de G no grupo multiplicativo dos números complexos $\mathbb{C}^* = \mathbb{C}\backslash\{0\}$. Equivalentemente, dizemos que $\chi : G \to \mathbb{C}^*$ é um caracter de G se $\chi(g_1g_2) = \chi(g_1)\chi(g_2)$ para quaisquer $g_1, g_2 \in G$. Um caracter é dito trivial se $\chi(g) = 1$ para todo $g \in G$, neste caso denotaremos o caracter por χ_0.*

Note que $\chi(1_G) = \chi(1_G)\chi(1_G)$, como $\chi(1_G) \neq 0$, então $\chi(1_G) = 1$, além disso, dado $g \in G$, $g^k = 1_G$, portanto

$$\chi(g)^k = \chi(g^k) = \chi(1_G) = 1,$$

ou seja, χ assume apenas valores que são k-ésimas raízes da unidade, logo $|\chi(g)| = 1$ para todo $g \in G$ (onde $|.|$ denota a norma do número complexo $\chi(g)$), portanto $\chi(g)^{-1} = \overline{\chi(g)}$. Como $\chi(g)\chi(g^{-1}) = \chi(gg^{-1}) = \chi(1_G) = 1$, segue que

$$\chi(g^{-1}) = \chi(g)^{-1} = \overline{\chi(g)}.$$

Definição 71. *Seja χ um caracter sobre G e defina $\overline{\chi}(g) = \overline{\chi(g)}$ para todo $g \in G$. É claro que $\overline{\chi}$ é um caracter sobre G. Dizemos que $\overline{\chi}$ é o caracter conjugado de χ.*

Definição 72. *Dados $\chi_1, \chi_2, \cdots, \chi_{n-1}$ e χ_n caracteres de G, definimos o produto de caracteres por*

$$\chi_1 \cdots \chi_n(g) = \chi_1(g) \cdots \chi_n(g)$$

para todo $g \in G$.

Proposição 73. *Seja $\widetilde{G}$ o conjunto de todos os caracteres de G, então $\widetilde{G}$ é um grupo abeliano finito com a operação de produto de caracteres.*

Demonstração. O produto de caracteres ainda é um caracter, além disso, as propriedades associativa e comutativa são facilmente verificáveis. Note também que χ_0 é o elemento neutro de $\widetilde{G}$. Sejam $\chi \in \widetilde{G}$ e $\overline{\chi}$ o caracter conjugado de χ. Como $|\chi(g)| = 1$ para todo $g \in G$, então $\chi\overline{\chi}(g) = \chi(g)\overline{\chi}(g) = \chi(g)\overline{\chi(g)} = 1$ para todo $g \in G$ e portanto $\overline{\chi} = \chi^{-1}$. Sendo assim, temos que $\widetilde{G}$ é grupo abeliano com o produto de caracteres. Como $\chi \in \widetilde{G}$ assume apenas valores que são k-ésimas raízes da unidade, então $\widetilde{G}$ é finito. ■

Proposição 74. *(Caracterização dos caracteres de um grupo finito cíclico) Seja G um grupo finito cíclico de ordem k, então $\widetilde{G}$ possui k caracteres χ_j tais que para $j \in \{0, \cdots, k-1\}$ fixo, define-se para todo $m \in \{1, \cdots, k-1\}$,*

$$\chi_j(g^m) = \xi^{jm},$$

onde $\xi = e^{2\pi i/k}$ é uma k-ésima raiz primitiva da unidade.

Demonstração. É claro que para j fixo, a função χ_j define um caracter de G. Além disso, se χ é um caracter qualquer de G, então $\chi(g)$ é uma k-ésima raiz da unidade para todo $g \in G$, ou seja, $\chi(g) = \xi^j$ e daí $\chi(g^m) = \xi^{jm}$ para algum $j \in \{0, \cdots, k-1\}$, logo $\chi = \chi_j$ e portanto todo caracter de G é da forma χ_j para algum $j \in \{0, \cdots, k-1\}$. ■

Teorema 75. *Sejam H um subgrupo de G e ψ um caracter de H. Então ψ pode ser estendida a um caracter de G, isto é, existe um caracter χ de G tal que $\chi(h) = \psi(h)$ para todo $h \in H$.*

Corolário 76. *Dados g_1 e g_2 elementos distintos de G, então existe um caracter χ de G tal que $\chi(g_1) \neq \chi(g_2)$.*

Demonstração. Seja $h = g_1 g_2^{-1}$, note que $h \neq 1_G$ pois $g_1 \neq g_2$. Como $\chi(h) = \chi(g_1)\chi(g_2^{-1}) = \chi(g_1)\chi(g_2)^{-1}$ para todo $\chi \in \widetilde{G}$, basta mostrar que existe $\chi \in \widetilde{G}$ tal que $\chi(h) \neq 1$ e portanto $\chi(g_1) \neq \chi(g_2)$. Seja H o subgrupo cíclico de G de ordem k_1 gerado por h, pela Proposição 74, $\psi(h^m) = e^{2\pi i m/k_1}$ define um caracter sobre H. Além disso, $\psi(h) \neq 1$ pois $k_1 \neq 1$, logo pelo Teorema 75 segue que o caracter χ extensão de ψ é o caracter procurado. ■

Teorema 77. *Se χ é um caracter não trivial de um grupo abeliano finito G, então*

$$\sum_{g \in G} \chi(g) = 0. \tag{A.1}$$

Se $g \in G$ com $g \neq 1_G$, então

$$\sum_{\chi \in \widetilde{G}} \chi(g) = 0. \tag{A.2}$$

Demonstração. Como χ é não trivial, existe $h \in G$ tal que $\chi(h) \neq 1$. Então

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

pois como g percorre por todos os elementos do grupo G então hg também percorre. Logo temos que $(\chi(h) - 1) \sum_{g \in G} \chi(g) = 0$, e como $\chi(h) \neq 1$, segue que $\sum_{g \in G} \chi(g) = 0$. Para a segunda identidade, defina $\widetilde{g} : \widetilde{G} \to \mathbb{C}^*$ pondo $\widetilde{g}(\chi) = \chi(g)$, note que $\widetilde{g}$ é um caracter de $\widetilde{G}$, ou seja, $\widetilde{g} \in \widetilde{\widetilde{G}}$, além disso, é um caracter não trivial pois pelo Corolário 76 existe $\chi \in \widetilde{G}$ com $\chi(g) \neq \chi(1_G) = 1$. Portanto, aplicando a primeira identidade no grupo $\widetilde{G}$ temos que

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

■

Teorema 78. *O número de caracteres de um grupo finito abeliano G é igual a $|G| = k$.*

Demonstração. Usando as Identidades (A.1) e (A.2) segue que

$$|\widetilde{G}| = \sum_{g\in G}\sum_{\chi\in\widetilde{G}}\chi(g) = \sum_{\chi\in\widetilde{G}}\sum_{g\in G}\chi(g) = |G|.$$

■

Teorema 79. *(Relações de ortogonalidade) Dados χ e ψ caracteres de G, então*

$$\sum_{g\in G}\chi(g)\overline{\psi}(g) = \begin{cases} 0 & se \quad \chi \neq \psi \\ |G| & se \quad \chi = \psi \end{cases}. \tag{A.3}$$

Além disso, se $g, h \in G$ então

$$\sum_{\chi\in\widetilde{G}}\chi(g)\overline{\chi}(h) = \begin{cases} 0 & se \quad g \neq h \\ |G| & se \quad g = h \end{cases} \tag{A.4}$$

Demonstração. É claro que se $\chi = \psi$, então $\chi(g)\overline{\psi}(g) = \chi(g)\overline{\chi}(g) = 1$ para todo $g \in G$, logo $\sum_{g\in G}\chi(g)\overline{\psi}(g) = |G|$. Suponha que $\chi \neq \psi$, então como $\chi(g)\overline{\psi}(g) = \chi\overline{\psi}(g)$ e o caracter $\chi\overline{\psi}$ é não trivial, pelo Teorema 77, $\sum_{g\in G}\chi\overline{\psi}(g) = 0$. Sejam agora g e h elementos de G, se $g \neq h$, tomando $gh^{-1} \in G$, pelo Teorema 77 e do fato de $gh^{-1} \neq 1_G$, seque que

$$0 = \sum_{\chi\in\widetilde{G}}\chi(gh^{-1}) = \sum_{\chi\in\widetilde{G}}\chi(g)\overline{\chi}(h).$$

Supondo $g = h$, como $\chi(g)\overline{\chi}(h) = 1$, pelo Teorema 78 o resultado segue. ■

Seja $\mathbb{F}_q$ um corpo finito onde $q = p^m$ com p primo. Em relação a adição $\mathbb{F}_q^n$ naturalmente é um grupo finito abeliano. Como $\mathbb{F}_p$ é isomorfo a um subcorpo de $\mathbb{F}_q$, além disso todas as soluções $\alpha \in \mathbb{F}_q$ de $\alpha^p = \alpha$ são exatamente os elemento de $\mathbb{F}_p$ e

$$\left(\sum_{i=0}^{m-1}\alpha^{p^i}\right)^p = \sum_{i=0}^{m-1}(\alpha^{p^i})^p = \sum_{i=0}^{m-1}\alpha^{p^i},$$

então $\sum_{i=0}^{m-1}\alpha^{p^i} \in \mathbb{F}_p$, logo podemos definir a seguinte função:

Definição 80. *Seja $\alpha \in \mathbb{F}_q$ onde $q = p^m$, o traço de α sobre $\mathbb{F}_p$ é definido por*

$$Tr(\alpha) = \alpha + \alpha^p + \cdots + \alpha^{p^{m-1}}.$$

A função traço é não nula pois caso contrário todo elemento de $\mathbb{F}_q$ seria raiz do polinômio $x + x^p + \cdots + x^{p^{m-1}}$, o que é um absurdo pois tal polinômio possui no máximo p^{m-1} raízes e $\mathbb{F}_q$ possui p^m elementos. Como a função traço é uma aplicação $\mathbb{F}_p$-linear não nula com imagem em $\mathbb{F}_p$, então ela é sobrejetora. Seja $Tr : \mathbb{F}_q \to \mathbb{F}_p$ a função traço sobre $\mathbb{F}_p$, defina

$$\chi_1(c) = e^{2\pi i Tr(c)/p} \text{ para todo } c \in \mathbb{F}_q,$$

então χ_1 é um caracter do grupo aditivo $\mathbb{F}_q$, que chamaremos de *caracter aditivo*.

Teorema 81. *Dado $b \in \mathbb{F}_q$, a função χ_b definida por $\chi_b(c) = \chi_1(bc)$ para todo $c \in \mathbb{F}_q$ é um caracter aditivo de $\mathbb{F}_q$ e além disso, todo caracter aditivo de $\mathbb{F}_q$ é obtido desta maneira.*

Demonstração. Tome $b \in \mathbb{F}_q$, então χ_b é um caracter aditivo, de fato, sejam $c_1, c_2 \in \mathbb{F}_q$, então

$$\chi_b(c_1 + c_2) = \chi_1(bc_1 + bc_2) = \chi_1(bc_1)\chi_1(bc_2) = \chi_b(c_1)\chi_b(c_2).$$

Como Tr é uma aplicação sobrejetora de $\mathbb{F}_q$ em $\mathbb{F}_p$, χ_1 é um caracter não trivial. Portanto, se $a, b \in \mathbb{F}_q$ com $a \neq b$, então

$$\frac{\chi_a(c)}{\chi_b(c)} = \frac{\chi_1(ac)}{\chi_1(bc)} = \chi_1((a-b)c) \neq 1$$

para $c \in \mathbb{F}_q$ conveniente, ou seja, se $m \not\equiv 0(p)$, então tome $c = 1/(a-b)$, caso contrário, como a função traço é sobrejetora, existe $\alpha \in \mathbb{F}_q$ tal que $Tr(\alpha) = 1$, logo basta tomar $c = \alpha/(a-b)$. Sendo assim, χ_a e χ_b são distintos. Portanto temos q caracteres aditivos, pelo Teorema 78 segue que tais caracteres são os únicos possíveis. ■

Lema 82. *Seja χ um caracter aditivo não trivial de $\mathbb{F}_q$, α um elemento fixo de $\mathbb{F}_q$ e m um inteiro não negativo. Então*

$$\sum_{\beta \in \mathbb{F}_q^m} \chi(\alpha \cdot \beta) = \begin{cases} q^m, & se \quad \alpha = 0 \\ 0, & se \quad \alpha \neq 0 \end{cases} \tag{A.5}$$

Demonstração. Pelo Lema 50 do Capítulo 2, segue que

$$\sum_{\beta \in \mathbb{F}_q^m} \chi(\alpha \cdot \beta) = \prod_{i=1}^{m} \sum_{\beta_i \in \mathbb{F}_q} \chi_{\alpha_i}(\beta_i).$$

Pela caracterização dos caracteres aditivos sobre $\mathbb{F}_q$ segue que dados $a, b \in \mathbb{F}_q$ então $\chi_a = \chi_b$ se, e somente se, $a = b$. Logo, tomando $b = 0$, pelo Teorema 79 segue o resultado. ■

Lema 83. *Seja χ um caracter aditivo não trivial de $\mathbb{F}_q$. Então, para qualquer código linear $\mathscr{C}$ sobre $\mathbb{F}_q$*

$$\sum_{v\in\mathscr{C}}\chi(u\cdot v)=\begin{cases}0, & se \quad u\notin\mathscr{C}^{\perp}\\ |\mathscr{C}|, & se \quad u\in\mathscr{C}^{\perp}\end{cases} \tag{A.6}$$

Demonstração. O caso em que $u\in\mathscr{C}^{\perp}$ é trivial pois $\chi(u\cdot v)=\chi(0)=1$ para todo $v\in\mathscr{C}$. Supondo então que $u\notin\mathscr{C}^{\perp}$ temos a seguinte igualdade

$$\sum_{v\in\mathscr{C}}\chi(u\cdot v)=\sum_{c\in\mathbb{F}_q}\sum_{v\in\mathscr{C},u\cdot v=c}\chi(c).$$

Podemos agora considerar $\mathscr{C}$ como grupo aditivo. Seja

$$S_u(0)=\{v\in\mathscr{C}:u\cdot v=0\}.$$

Claramente $S_u(0)$ é subgrupo de $\mathscr{C}$ pois se $a,b\in S_u(0)$, então $a-b\in S_u(0)$. Considere então o quociente $\mathscr{C}/S_u(0)$. Como $u\notin\mathscr{C}^{\perp}$ então existe $w\in\mathscr{C}$ tal que $w\cdot u=k\neq 0$. Mostraremos que

$$|\{v\in\mathscr{C}:u\cdot v=0\}|=|\{v\in\mathscr{C}:u\cdot v=k\}|.$$

De fato, note que $w+S_u(0)\in\mathscr{C}/S_u(0)$ e portanto $|w+S_u(0)|=|S_u(0)|$. Basta então mostrar que $w+S_u(0)=\{v\in\mathscr{C}:u\cdot v=k\}$, de fato, tome $w_1\in w+S_u(0)$, então $w_1=w+x$ com $x\in S_u(0)$, logo $w_1\cdot u=(w+x)\cdot u=k$, daí $w_1\in\{v\in\mathscr{C}:u\cdot v=k\}$. Reciprocamente, se $w_1\in\{v\in\mathscr{C}:u\cdot v=k\}$, podemos escrever $w_1=v+(w-v)\in v+S_u(0)$, portanto temos a igualdade desejada. Note agora que para todo $c\in\mathbb{F}_q$, existe $v\in\mathscr{C}$ tal que $u\cdot v=c$, portanto temos que

$$|\{v\in\mathscr{C}:u\cdot v=k_1\}|=|\{v\in\mathscr{C}:u\cdot v=k_2\}|$$

para todo $k_1,k_2\in\mathbb{F}_q$. Como $|\mathscr{C}/S_u(0)|=q$ segue que $|\{v\in\mathscr{C}:u\cdot v=c\}|=|\mathscr{C}|/q$, portanto

$$\sum_{c\in\mathbb{F}_q}\sum_{v\in\mathscr{C},u\cdot v=c}\chi(c)=\frac{|\mathscr{C}|}{q}\sum_{c\in\mathbb{F}_q}\chi(c)$$

pelo Lema 82, tomando $m=\alpha=1$ tem-se que $\sum_{c\in\mathbb{F}_q}\chi(c)=0$, portanto

$$\sum_{v\in\mathscr{C}}\chi(u\cdot v)=0.$$

■

Definição 84. *(Transformada de Hadamard) A transformada de Hadamard de f é a função complexa com domínio em $\mathbb{F}_q^n$ definida por*

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

Lema 85. *(Fórmula da soma discreta de Poisson) Seja $\mathscr{C}$ um código linear de comprimento n sobre $\mathbb{F}_q$ e f uma função em $\mathbb{F}_q^n$, então*

$$\sum_{v \in \mathscr{C}^\perp} f(v) = \frac{1}{|\mathscr{C}|} \sum_{u \in \mathscr{C}} \widehat{f}(u). \tag{A.7}$$

Demonstração. Pela Definição 84 segue que

$$\begin{aligned}
\frac{1}{|\mathscr{C}|} \sum_{u \in \mathscr{C}} \widehat{f}(u) &= \frac{1}{|\mathscr{C}|} \sum_{u \in \mathscr{C}} \sum_{v \in \mathbb{F}_q^n} \chi(u \cdot v) f(v) \\
&= \frac{1}{|\mathscr{C}|} \sum_{v \in \mathbb{F}_q^n} \sum_{u \in \mathscr{C}} \chi(u \cdot v) f(v) \\
&= \frac{1}{|\mathscr{C}|} \sum_{v \in \mathbb{F}_q^n} \left(f(v) \sum_{u \in \mathscr{C}} \chi(u \cdot v) \right).
\end{aligned}$$

Se $v \in \mathbb{F}_q^n$ então $v \in \mathscr{C}^\perp$ ou $v \notin \mathscr{C}^\perp$, logo do Lema 83,

$$\begin{aligned}
\frac{1}{|\mathscr{C}|} \sum_{v \in \mathbb{F}_q^n} \left(f(v) \sum_{u \in \mathscr{C}} \chi(u \cdot v) \right) &= \frac{1}{|\mathscr{C}|} \sum_{v \in \mathscr{C}^\perp} f(v) |\mathscr{C}| \\
&= \sum_{v \in \mathscr{C}^\perp} f(v).
\end{aligned}$$

■

Apêndice B

Polinômios de Krawtchouk

Os polinômios de Krawtchouk, introduzidos pelo ucraniano Mikhail Krawtchouk em 1929, constituem uma importante ferramenta combinatorial, para maiores detalhes, consulte [18]. Para definirmos os polinômios de Krawtchouk, necessitamos de algumas definições e propriedades de coeficientes binomiais. Dado $x \in \mathbb{R}$, o coeficiente binomial $\binom{x}{m}$ (leia-se x tomados m a m) é definido por:

$$\binom{x}{m} = \begin{cases} \frac{x(x-1)\cdots(x-m+1)}{m!}, & \text{se } m \text{ é um inteiro positivo.} \\ 1, & \text{se } m = 0. \\ 0, & \text{caso contrário.} \end{cases}$$

Serão apresentados abaixo algumas propriedades desses coeficientes, para mais detalhes consulte [18] e [24].

(a) O caso em que $x = n$ é um inteiro não negativo e $n \geqslant m \geqslant 0$, o coeficiente binomial $\binom{n}{m}$ pode ser interpretado como sendo o número de possíveis combinações de n elementos tomados m a m.

(b) Séries binomiais:

$$(a+b)^n = \sum_{m=0}^{n} \binom{n}{m} a^{n-m} b^m, \text{ se } n \text{ é um inteiro não negativo,} \tag{B.1}$$

$$(1+b)^x = \sum_{m=0}^{+\infty} \binom{x}{m} b^m, \text{ para } |b| < 1 \text{ e } x \in \mathbb{R}. \tag{B.2}$$

(c) Sejam n e m inteiros não negativos e x um número real, então:

$$\binom{n}{m} = \binom{n}{n-m}, \tag{B.3}$$

$$\binom{n}{m} = 0 \text{ para } m > n \geq 0, \tag{B.4}$$

$$\binom{n}{m} + \binom{n}{m-1} = \binom{n+1}{m} \text{ e} \tag{B.5}$$

$$(-1)^m \binom{-x}{m} = \binom{x+m-1}{m}. \tag{B.6}$$

No desenvolvimento das equações subsequentes usaremos expansões em séries binomiais, porém não nos preocuparemos em garantir que a série converge, ou seja, trabalharemos com séries formais, portanto sendo $\sum a_n x^n$ e $\sum b_n x^n$ duas séries de potência formais, definiremos o produto entre essas séries como sendo a série $\sum c_n x^n$ onde

$$c_n = a_0 b_n + a_1 b_{n-1} + \cdots + a_{n-1} b_1 + a_n b_0.$$

Definição 86. *Para todo inteiro positivo n e $q = p^r$ com p primo, define-se o polinômio de Krawtchouk como*

$$P_k(x; n) = P_k(x) = \sum_{j=0}^{k} (-1)^j \gamma^{k-j} \binom{x}{j} \binom{n-x}{k-j}, \quad k = 0, 1, \cdots, n, \tag{B.7}$$

onde $\gamma = q - 1$.

Definição 87. *Uma função geradora para uma seqüência $(P_k(x))_k$ é definida como sendo a função $G(z)$, que possui $P_k(x)$ como coeficiente de z^k quando expressa em termos de potência de z, ou seja, $G(z) = \sum_{k=0}^{+\infty} P_k(x) z^k$.*

Considere a função denotada por $(1 + \gamma z)^{n-x}(1 - z)^x$. De (B.2) segue que

$$(1 + \gamma z)^{n-x}(1 - z)^x = \sum_{m=0}^{+\infty} \binom{n-x}{m} \gamma^m z^m \sum_{j=0}^{+\infty} \binom{x}{j} (-1)^j z^j.$$

Pela definição de produto de séries de potências formais,

$$\sum_{m=0}^{+\infty} \binom{n-x}{m} \gamma^m z^m \sum_{j=0}^{+\infty} \binom{x}{j} (-1)^j z^j = \sum_{k=0}^{+\infty} \sum_{j=0}^{k} (-1)^j \gamma^{k-j} \binom{x}{j} \binom{n-x}{k-j} z^k = \sum_{k=0}^{+\infty} P_k(x) z^k.$$

Portanto $(1 + \gamma z)^{n-x}(1 - z)^x$ é uma função geradora do polinômio de Krawtchowk.

Proposição 88. *Expressões alternativas para o polinômio de Krawtchouk:*

$$(i) \quad P_k(x) = \sum_{j=0}^{k} (-q)^j \gamma^{k-j} \binom{n-j}{k-j} \binom{x}{j}$$

$$(ii) \quad P_k(x) = \sum_{j=0}^{k} (-1)^j q^{k-j} \binom{n-k+j}{j} \binom{n-x}{k-j}$$

Demonstração. Como

$$(1+\gamma z)^{n-x}(1-z)^x = (1+\gamma z)^n \left(\frac{1-z}{1+\gamma z}\right)^x,$$

desenvolvendo o lado direito em séries de potências obtemos (i). Note que como $\gamma = q-1$, então

$$\begin{aligned}(1+\gamma z)^{n-x}(1-z)^x = \left(\frac{1+\gamma z}{1-z}\right)^{n-x}(1-z)^n &= \left(\frac{1+qz-z}{1-z}\right)^{n-x}(1-z)^n \\ &= \left(1+\frac{qz}{1-z}\right)^{n-x}(1-z)^n.\end{aligned}$$

Expandindo a última igualdade em séries de potência obtemos (ii). ■

Índice Remissivo

Referências Bibliográficas

[1] Alves, M. M. S., Paneck, L., e Firer, M. Error-block codes and poset metrics. *Advances in Mathematics of Communications 2*, 1 (2008), 95–111.

[2] Brualdi, R. A., Graves, J., e Lawrence, K. M. Codes with a poset metric. *Discrete Mathematics 147* (1995), 57–72.

[3] Felix, L. V., e Firer, M. Canonical-systematic form of hierarchical codes. Preprint, 2011.

[4] Feng, K., Xu, L., e Hickernell, F. J. Linear error-block codes. *Finite Fields and Their Applications 12* (2006), 638–652.

[5] Hamming, R. W. Error correcting and error correcting codes. *The Bell System Technical Journal 29*, 2 (1950), 147–160.

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

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

[8] Hyun, J. Y., e Kim, H. K. The poset structures admitting the extended binary Hamming code to be a perfect code. *Discrete Mathematics 288* (2004), 37–47.

[9] Jang, C., Kim, H. K., Oh, D. Y., e Rho, Y. The poset structures admitting the extended binary Golay code to be a perfect code. *Discrete Mathematics 308* (2008), 4057–4068.

[10] Kim, D. S., e Kim, D. C. Character sums and MacWilliams identities. *Discrete Mathematics 287* (2004), 155–160.

[11] Kim, D. S., e Lee, J. G. A MacWilliams-type identity for linear codes on weak order. *Discrete Mathematics 262* (2003), 181–194.

[12] Kim, H. K., e Oh, D. Y. A classification of posets admitting the MacWilliams identity. *IEEE Transactions on Information Theory 51*, 4 (Apr. 2005), 1424–1431.

[13] Lee, C. Y. Some properties of nonbinary error-correction codes. *IRE Transactions on Information Theory 4*, 2 (1958), 77–82.

[14] Lidl, R., e Niederreiter, H. *Finite Fields*, 2 ed. No. 20 in Encyclopedia of Mathematics and its Applications. Cambridge University Press, Cambridge, U.K., 1997.

[15] Ling, S., e Özbudak, F. Constructions and bounds on linear error-block codes. *Des. Codes Cryptogr. 45* (2007), 297–316.

[16] MacWilliams, F. J. *Combinatorial problems of elementary group theory*. PhD thesis, Department of Math., Harvard University, 1962.

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

[18] MacWilliams, F. J., e Sloane, N. J. *The Theory of Error-Correcting Codes*. North-Holland, Amsterdam, The Netherlands, 1977.

[19] Neggers, J., e Kim, H. S. *Basic Posets*. World Scientific, 1998.

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

[21] Panek, L., Firer, M., e Alves, M. M. S. Classification of Niederreiter-Rosenbloom-Tsfasman block codes. *IEEE Transactions on Information Theory 56*, 10 (2010), 5207–5216.

[22] Pinheiro, J. A., e Firer, M. Classification of poset-block spaces admitting MacWilliams-type identity. Preprint, 2011.

[23] Pinheiro, J. A., e Firer, M. MacWilliams-type identity in poset-block spaces. In *Proceedings Information Theory Workshop* (2011), pp. 490–494.

[24] Riordan, J. *Combinatorial Identities*. Wiley, New York, 1968.

[25] Shannon, C. E. A mathematical theory of communication. *Bell System Tech. 27* (1948), 379–423.

[26] Tietäväinen, A. On the nonexistence of perfect codes over finite fields. *SIAM J. Appl. Math. 24*, 1 (1973), 88–96.

[27] Ulrich, W. Non-binary error correction codes. *SIAM J. Appl. Math. 36*, 6 (1957), 1341–1388.

[28] van Lint, J. H. *Introdution to Coding Theory*, 3 rev. and exp. ed. Graduate Texts in Mathematics. Springer, the Netherlands, 1998.