Proceeding Series of the Brazilian Society of Applied and Computational Mathematics, Vol. 2, N. 1, 2014.
Trabalho apresentado no CMAC-Sul, Curitiba-PR, 2014.

Identidades de MacWilliams para códigos poset

Marcelo M. S. Alves, **Maycow G. Carneiro**,
UFPR - Programa de Pós Graduação em Matemática Aplicada
81531-980, Curitiba, PR
E-mail: mmunizbr@gmail.com, maycon.mgc@gmail.com,

Resumo: *Um dos resultados mais importantes na teoria de códigos são as identidades de MacWilliams, que relacionam a distribuição de pesos de um código com a de seu dual. Kim e Oh mostraram que quando estamos trabalhando com códigos lineares sobre conjuntos parcialmente ordenados (abrev. posets), tais identidades valem se e somente se o poset é hierárquico [6]. Choi et al. consideram distribuições de pesos de um código poset em que se leva em conta também uma relação de equivalência no conjunto $I(P)$ dos ideais de ordem do poset P, sendo que o polinômio enumerador clássico corresponde ao caso em que dois ideais são equivalentes se tem o mesmo número de elementos. Neste contexto derivam-se identidades semelhantes às de MacWilliams para posets não-hierárquicos, obtendo-se matrizes que relacionam as distribuições de peso do código com seu dual [2]. Neste trabalho mostramos que quando o poset é uma união disjunta de cadeias, tais matrizes são inteiramente determinadas a partir das entradas referentes a uma das cadeias do poset. Utilizamos os resultados obtidos para provar os resultados apresentados por Dougherty e Skriganov em [3] através da P-métrica obtida ao invés da ρ-métrica utilizada pelos autores. Finalmente, mostramos que todos os 3 casos de identidades generalizadas de MacWilliams apresentados em [2] correspondem a distribuições de pesos associadas a uma relação de equivalência dada pela ação de um grupo de automorfismos de P.*

Palavras-chave: *Código Lineares, Identidades de MacWilliams, Codigos Poset, Relações de equivalência de tipo MacWilliams*

Na teoria de Códigos Corretores de Erros, um dos resultados mais importantes são as identidades de MacWilliams, introduzidas por F.J. MacWilliams para espaços de Hamming, que relacionam o polinômio enumerador do código $\mathscr{C}$ com o de seu código dual $\mathscr{C}^{\perp}$.

Teorema 1 (Identidade de MacWilliams em espaços de Hamming). *Seja $\mathbb{F}_q^n$ um espaço de Hamming. Se $\mathscr{C}$ é um $[n,k,d_H]$ código linear sobre $\mathbb{F}_q$ então*

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

Neste trabalho, apresentaremos alguns conceitos e resultados obtidos em [3] e [2] e veremos que os resultados em [3] podem ser obtidos utilizando-se os métodos apresentados em [2] bem como alguns resultados interessantes que conseguimos.

Em 1997 Rosenbloom e Tsfasman [12] introduziram na teoria de códigos uma métrica ρ em $\mathrm{Mat}_{n,s}(\mathbb{F}_q)$. Estes códigos tem sido estudados tanto do ponto de vista de combinatória quanto de aplicações em teoria de informação [3, 7, 10, 11, 13].

Primeiramente, seja $n=1$ e $w=(\xi_1,\dots,\xi_s)\in \mathrm{Mat}_{n,s}(\mathbb{F}_q)$. Então colocamos $\rho(0)=0$ e $\rho(w)=\max\{i:\xi_i\neq 0\}$ para $w\neq 0$. Agora seja $\Omega=(w_1,\dots,w_n)^T\in \mathrm{Mat}_{n,s}(\mathbb{F}_q)$, $w_j\in \mathrm{Mat}_{1,s}(\mathbb{F}_q), 1\le j\le n$, colocamos $\rho(\Omega)=\sum_{j=1}^{n}\rho(w_j)$. Para um código linear $\mathscr{C}\subset \mathrm{Mat}_{n,s}(\mathbb{F}_q)$ dado, chamamos de espectro de ρ-peso do código $\mathscr{C}$ o conjunto de números inteiros $\omega_r(\mathscr{C})=|\{\Omega\in\mathscr{C}:\rho(\Omega)=r\}|, 0\le r\le ns$.

Assim como na teoria clássica, conseguimos definir o enumerador de ρ-peso de $\mathscr{C}$ por $W(\mathscr{C}|z) = \sum_{r=0}^{ns} \omega_r(\mathscr{C}) z^r = \sum_{\Omega\in\mathscr{C}} z^{\rho(\Omega)}$.

Introduza o seguinte produto interno em $\mathrm{Mat}_{n,s}(\mathbb{F}_q)$. Primeiramente, seja $n=1$ e $w_1 = (\xi'_1,\ldots,\xi'_s)$, $w_2 = (\xi''_1,\ldots,\xi''_s) \in \mathrm{Mat}_{1,s}(\mathbb{F}_q)$. Coloque $\langle w_1, w_2\rangle = \sum_{i=1}^{s} \xi'_i \xi''_{s+1-i}$. Agora seja $\Omega_i = (w_i^{(1)},\ldots,w_i^{(n)})^T \in \mathrm{Mat}_{n,s}(\mathbb{F}_q)$, $i=1,2$, $w_i^{(j)} \in \mathrm{Mat}_{1,s}(\mathbb{F}_q)$, $1\le j\le n$, coloque $\langle\Omega_1,\Omega_2\rangle = \sum_{j=1}^{n} \langle w_1^{(j)}, w_2^{(j)}\rangle$.

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

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

Para o caso $s=1$ e n arbitrário o ρ-peso satisfaz a identidade do Teorema 1. Por outro lado, para o caso $n=1$ e s arbitrário, em [3] foi dada a seguinte identidade:

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

Para o caso de n e s arbitrários, o seguinte contra-exemplo mostra que extensões diretas dos teoremas de tipo MacWilliams não existem para enumerador de ρ-peso.

Exemplo 1. Considere dois códigos lineares $\mathscr{C}_1$e$\mathscr{C}_2 \subset \mathrm{Mat}_{2,2}(\mathbb{F}_2)$

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

Assim $W(\mathscr{C}_1|z) = z^0 + z^2 = 1 + z^2 = W(\mathscr{C}_2|z)$.
Os códigos duais $\mathscr{C}_1^\perp$ e $\mathscr{C}_2^\perp \subset \mathrm{Mat}_{2,2}(\mathbb{F}_2)$ são:

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

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

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

Em [3] Dougherty e Skriganov, considerando órbitas de um grupo linear preservando o ρ-peso, mostram que o enumerador de peso associado a estas órbitas satisfaz os teoremas de tipo MacWilliams para códigos lineares mutuamente duais em $\mathrm{Mat}_{n,s}(\mathbb{F}_q)$ com respeito a ρ-métrica.

Para isso, sendo S_n o grupo simétrico de todas as permutações de linhas da matriz $\Omega \in \mathrm{Mat}_{n,s}(\mathbb{F}_q)$ e $S_n^{(R)} \subset S_n$ dado por $S_n^{(R)} = \{\sigma \in S_n : \sigma R = R\}$ o subgrupo de estabilização, tomando $Q_{n,s} \subset \mathbb{Z}^n$ como sendo o conjunto $Q_{n,s} = \{R = (r_1,...,r_n) : 0 \le r_j \le s, 1 \le j \le n\}$, para $R \in Q_{n,s}$ e uma permutação $\sigma \in S_n$, tomando o conjunto $Q_{n,s}/S_n = \{R = (r_1,\ldots,r_n) : 0 \le r_1 \le \cdots \le r_n \le s\}$ e considerando ainda esferas $S^{(n,s)}(r)$ em $\mathrm{Mat}_{n,s}(\mathbb{F}_q)$ com respeito a métrica ρ, e os conjuntos $F_R = \prod_{j=1}^{n} S^{(1,s)}(r_j)$, $R \in Q_{n,s}$, chamado fragmento e $\Phi_R = \bigcup_{\sigma\in S_n/S_n^{(R)}} F_{\sigma R}$, $R \in Q_{n,s}/S_n$, união disjunta de fragmentos.

Para um código linear $\mathscr{C} \subset \mathrm{Mat}_{n,s}(\mathbb{F}_q)$, são chamados T e H-espectro do código $\mathscr{C}$ respectivamente, os seguinte conjuntos

$$t_R(\mathscr{C}) = |\{\mathscr{C} \cap F_R\}|, R \in Q_{n,s} \quad \text{e} \quad h_R(\mathscr{C}) = |\{\mathscr{C} \cap \Phi_R\}| = \sum_{\sigma\in S_n} t_{\sigma R}(\mathscr{C}), R \in Q_{n,s}/S_n.$$

Define-se então o T-enumerador por $T(\mathscr{C}|Z_1,\dots,Z_n) = \sum_{R\in Q_{n,s}} t_R(\mathscr{C}) \prod_{j=1}^{n} z_{r_j}^{(j)}$, onde $Z_j = (z_0^{(j)},\dots,z_s^{(j)})^T \in \mathbb{C}^{s+1}$, $1\le j\le n$ e o H-enumerador por $H(\mathscr{C}|Z) = \sum_{R\in Q_{n,s}/S_n} h_R(\mathscr{C}) \prod_{j=1}^{n} z_{r_j}$, onde $Z=(z_0,\dots,z_s)^T \in \mathbb{C}^{s+1}$ e se introduz então uma transformação linear $\Theta_s : \mathbb{C}^{s+1} \to \mathbb{C}^{s+1}$ colocando $Z^{'} = \Theta_s Z$, onde as entradas da matriz $\Theta_s = [\theta_{lk}], 0\le l,k\le s$ são dadas por

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

obtendo assim resultados em identidades de tipo MacWilliams para o T- e H-enumeradores, os quais são enunciados a seguir.

Teorema 2. *O T-enumerador dos códigos lineares mutuamente duais $\mathscr{C}$ e $\mathscr{C}^\perp \subset Mat_{n,s}(\mathbb{F}_q)$ são relacionados por*

$$T(\mathscr{C}^\perp|Z_1,\dots,Z_n) = \frac{1}{|\mathscr{C}|} T(\mathscr{C}|\Theta_s Z_1,\dots,\Theta_s Z_n).$$

Teorema 3. *O H-enumerador dos códigos lineares mutuamente duais $\mathscr{C}$ e $\mathscr{C}^\perp \subset Mat_{n,s}(\mathbb{F}_q)$ são relacionados por*

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

Utilizam-se no trabalho entre outras coisas, transformadas de Fourier para provar os teoremas e explicar como as entradas da matriz Θ_s são obtidas.

Porém, se considerarmos conjuntos parcialmente ordenados (abrev. posets), notamos que a ρ-métrica pode ser vista como uma métrica poset sobre união disjunta de cadeias de mesma cardinalidade.

Seja P um poset em $[n]$ com relação de ordem $\preceq$. Um ideal em P é um subconjunto I de P tal que se $x\in I$ e $y\in P$ satisfaz $y\preceq x$ então $y\in I$. Se X é um subconjunto de P, o ideal gerado por X, denotado por $\langle X\rangle_P$, é o menor ideal de P contendo X. Verifica-se que $\langle X\rangle_P = \{y\in P; \exists x\in X \text{ com } y\preceq x\}$.

O espaço vetorial $\mathbb{F}_q^n$ possui uma métrica naturalmente induzida por P. Para um vetor $x\in\mathbb{F}_q^n$, definimos o suporte de x como sendo $\mathrm{supp}(x) = \{i : x_i \ne 0\}$, o P-peso de x, $\omega_P(x)$, como $\omega_P(x) = |\langle \mathrm{supp}(x)\rangle_P|$, e definimos ainda a P-distância entre $x,y\in\mathbb{F}_q^n$ como $d_P(x,y) = \omega_P(x-y)$. Temos que d_P define uma métrica em $\mathbb{F}_q^n$, assim, se $\mathbb{F}_q^n$ está munida dessa métrica, então um código de $\mathbb{F}_q^n$ é chamado P-código. Estes códigos foram introduzidos em [1] e possíveis extensões das identidades de MacWilliams para estes códigos foram estudadas em [4, 5, 6].

Em [2], Choi et al. definem relações de equivalências no conjunto de ideais ordenados do poset P, denotado por $I(P)$ e resultados sobre equivalências de tipo MacWilliams, as quais podem ser utilizadas para se provar os resultados obtidos em [3] , além de obtermos alguns resultados interessantes, como veremos.

Primeiramente, seja P um poset em $[n]$ com relação de ordem $\preceq$ e P^* o poset dual, ou seja, com as relações de ordem invertidas, isto é, $x \preceq_{P^*} y$ se e somente se $y\preceq_P x$. Denotemos por $\mathcal{I}(P)$ ao conjunto de ideais de ordem de P e seja E uma relação de equivalência em $\mathcal{I}(P)$. Se I é um ideal de ordem em $\mathcal{I}(P)$, então claramente o complemento I^c de I é um ideal de ordem de P^*.

Se P é um poset em $[n]$ e E é uma relação de equivalência em $\mathcal{I}(P)$, dizemos que E^* é a relação dual em $\mathcal{I}(P^*)$ de E se satisfaz a seguinte propriedade: $(I,J)\in E$ é definido pela propriedade (A) em $\mathcal{I}(P)$, então $(I^c,J^c)\in E^*$ é também definida pela propriedade (A) em $\mathcal{I}(P^*)$

Definimos ainda algumas relações de equivalência que serão utilizadas, para isso, seja P um poset em $[n]$ e $I,J\in\mathcal{I}(P)$.

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

DOI: 10.5540/03.2014.002.01.0049

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

A relação E_S em $I(P)$ é definida pela regra $(I,J) \in E_S \Leftrightarrow I \simeq J$ como um poset. Então E_S é uma relação de equivalência em $I(P)$.

Afim de conseguirmos a relação dual de E_S precisamos definir um poset complemento de isomorfismo. Um poset P é um poset complemento de isomorfismo se satisfaz a seguinte condição: para qualquer I e J em $I(P)$ temos que $I \simeq J \Leftrightarrow I^c \simeq J^c$.

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

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

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

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

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

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

$$A_{\overline{I},E}(\mathscr{C}) := |S_{\overline{I},E} \cap \mathscr{C}| \quad \text{ e } \quad W(\mathscr{C},P,E) := \left[A_{\overline{I},E}(\mathscr{C})\right]_{\overline{I} \in I(P)/E}.$$

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

Temos então dois teoremas que são dados em [2]

Teorema 4. *Seja P um poset em $[n]$, E uma relação de equivalência em $I(P)$ e E^* a relação dual em $I(P^*)$. São equivalentes:*

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

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

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

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

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

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

Definimos as matrizes Q_{E^*} e P_E como: $P_E = [p_{\overline{J^c},\overline{I}}]$ e $Q_{E^*} = [q_{\overline{I},\overline{J^c}}]$, onde $p_{\overline{J^c},\overline{I}} = \displaystyle\sum_{v \in S_{\overline{J^c},E^*}} \chi(u \cdot v)$ para $u \in S_{\overline{I},E}$ e $q_{\overline{I},\overline{J^c}} = \displaystyle\sum_{u \in S_{\overline{I},E}} \chi(u \cdot v)$ para $v \in S_{\overline{J^c},E^*}$. Aqui χ é um caracter aditivo não trivial.

Teorema 5. *Seja P um poset em $[n]$ e H um subgrupo de $Aut(P)$.*

DOI: 10.5540/03.2014.002.01.0049

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

(ii) *São equivalentes:*

- **(a)** *P é um poset hierárquico.*
- **(b)** *E_C é uma relação de equivalência de tipo MacWilliams em $I(P)$.*
- **(c)** *As duas relações de equivalência E_C e $E_{Aut(P)}$ são as mesmas.*

(iii) *São equivalentes:*

- **(i)** *P é um poset complemento de isomorfismo.*
- **(ii)** *E_S é uma relação de equivalência de tipo MacWilliams em $I(P)$.*

Agora estamos em posição de apresentar alguns resultados que obtemos analisando os conceitos e resultados obtidos em [2] e a relação com os resultados de [3] .

Primeiramente, vemos que a relação de equivalência E_S possui uma relação dual E_S^* se o poset P for um complemento de isomorfismo e pelo Teorema 5 vemos que neste caso a relação é de tipo MacWilliams. Porém, conseguimos mostrar que neste caso, as relações E_S e E_H são as mesmas, ou seja, todo isomorfismo entre ideais pode ser estendido a um automorfismo do poset.

Teorema 6. *Seja P um poset complemento de isomorfismo, sejam I, J ideais de P e seja $f : I \to J$ um isomorfismo. Então existe um automorfismo $\tilde{f}$ de P tal que $\tilde{f}|_I = f$.*

Demonstração: De fato, seja $f : I \to J$ um isomorfismo, então temos um isomorfismo $g : I^c \to J^c$. Seja x um elemento de I^c tal que $x \not\succ y$, para qualquer $y \in I$. Afirmamos que o elemento $y = g(x)$ em J^c é tal que $y \not\succ z$ para qualquer $z \in M(J)$, onde $M(J)$ denota o conjunto dos elementos maximais em J.

Suponha que existe um elemento $f(a) \in M(J)$ tal que $y \succ f(a)$, como $g : I^c - \{x\} \to J^c - \{g(x)\}$ é um isomorfismo e P é um complemento de isomorfismo então $\varphi : I \cup \{x\} \to J \cup \{g(x)\}$ é um isomorfismo, então teríamos $|M(I \cup \{x\})| = |M(I)| + 1 = |M(J)| + 1 > |M(J \cup \{g(x)\})|$ o que é uma contradição. Logo, o elento $y = g(x) \in J^c$ é tal que $y \not\succ z$ para qualquer $z \in J$, e $\tilde{f} : I \cup \{x\} \to J \cup \{g(x)\}$ definida por $\tilde{f}(x) = g(x)$ e $\tilde{f}(w \neq x) = f(w)$ é um isomorfismo. Portanto podemos estender f para todos os elementos de I^c dessa forma.

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

Como τ é um isomorfismo, $|M(L \cup \{h(x)\})| = 1$, mas temos que $h(x) \in M(L \cup \{h(x)\})$, pois caso contrário existiria um elemento $z \in L$ tal que $z \succ h(x)$ e teríamos que $h(x) \in L$ o que é uma contradição. Logo temos que $|M(\langle h(x) \rangle_M)| = k$. Portanto podemos estender f a todos os elementos dessa forma em I^c.

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

Além desse resultado, tomando P como um poset união de n cadeias disjuntas de comprimento s, conseguimos mostrar que há uma isometria entre $\mathrm{Mat}_{n,s}(\mathbb{F}_q)$ e $\mathbb{F}_q^{ns}$ e uma relação biunívoca entre os conjuntos $I(P)$ e $Q_{n,s}$, bem como $I(P^*)$ e $Q_{n,s}$. Com isso conseguimos relacionar os conjuntos F_R e S_I e tomando $H = S_n$ temos também uma relação biúnivoca entre $I(P)/E_H$ e $Q_{n,s}/S_n$, bem como $I(P^*)/E_H^*$ e $Q_{n,s}/S_n$ e entre Φ_R e $S_{\overline{I},E_H}$ bem como Φ_R e $S_{\overline{J^c},E_H^*}$.

Conseguimos mostrar então que, tomando $H = Id \in \mathrm{Aut}(P)$, temos $F_R \simeq S_{I,E} = S_{\overline{I},E}$ e $F_R \simeq S_{\overline{J^c},E^*}$ e além disso $t_R(\mathscr{C}) \simeq A_{\overline{I},E}(\mathscr{C})$ e $t_R(\mathscr{C}^\perp) \simeq A_{\overline{J^c},E^*}(\mathscr{C}^\perp)$, donde conseguimos a identidade de

DOI: 10.5540/03.2014.002.01.0049

MacWilliams para o T enumerador dado em ... utilizando identidade dada no item (ii) do Teorema 4. O mesmo pode ser feito para o H enumerador visto que $H(\mathscr{C}|Z) = T(\mathscr{C}|Z, Z, \ldots, Z)$.

Outro resultado encontrado foi uma relação entre a matriz Θ_s e a matriz $Q^T_{E^*_H}$.

Teorema 7. *Seja P um poset união de n cadeias disjuntas de comprimento s.*

(i) *Se $n = 1$, então a matriz $Q^T_{E^*_H}$ obtida é a matriz Θ_s.*

(ii) *Se $n > 1$, a matriz $Q_{E^*_H}$ referente ao conjunto $I(P^*)$ de todos os ideais no poset, é totalmente determinada pelas entradas obtidas no item (i).*

Concluímos então que no caso em que as relações de equivalência são de tipo MacWilliams, podemos analisar apenas as relações E_H e E_C, e que sob a luz dos resultados obtidos em [2] podemos conseguir os resultados em [3] .

Referências

[1] R. A. Brualdi, J. S. Graves, e K. M. Lawrence, Codes with a poset metric. *Discrete Math. 147*, 1-3(Dec. 1995), 57-72.

[2] S. Choi, J. Y. Hyun, D. Y. Oh, H. K. Kim, MacWilliams-type equivalence relations *ArXiv e-prints* (May 2012).

[3] S. T. Dougherty, M. M. Skriganov, MacWilliams duality and the Rosenbloom-Tsfasman metric, *Moscow Mathematical Journal 2*, 1 (2002) 81-97.

[4] Y. Jang, J. Park, On a MacWilliams type identity and a perfectness for a binary linear $(n, n-1, j)$-poset code, Discrete Mathematics, Volume 265, Issues 1-3, (April 2003), 85-104.

[5] D. S. Kim, J. G. Lee, A MacWilliams-type identity for linear codes on weak order, *Discrete Mathematics*, Volume 262, Issues 1-3, (2003), 181-194.

[6] H. K. Kim, e D. Y. Oh, A classification of posets admitting the MacWilliams identity. *IEEE Trans. Inf. Theor. 51*, 4 (Apr. 2005), 1424-1431.

[7] K. Lee, Automorphism group of the Rosenbloom-Tsfasman space, *Eur. J. Combin.*, 24 (2003), pp. 607-612

[8] R. Lidl, e H. Niederreiter, Finite Fields. *No. v.20,pt. 1 in Encyclopedia of Mathematics and its Applications.* Cambridge University Press, 1997.

[9] F. MacWilliams, e N. Sloane, The Theory of Error-Correcting Codes, 2nd ed. North-holland Publishing Company, 1978.

[10] M. Ozen and I. Siap, On the estructure and decoding of linear codes with respect to Rosenbloom-Tsfasman metric, *Selçuk Journal of Applied Mathematics* 5 (2) (2004) 25-31.

[11] L. Panek, M. Firer, M.M.S. Alves, Classification of Niederreiter-Rosenbloom-Tsfasman Block Codes, *IEEE Transactions on Information Theory*, v. 56, (2010) 5207-5216.

[12] M.Yu. Rosenbloom, M.A. Tsfasman, Codes for the m-metric, *Probl. Inf. Transm.* 33 (1) (1997) 45-52.

[13] M.M. Skriganov, On linear codes with large weights simultaneously for the Rosenbloom-Tsfasman and Hamming metrics, *Journal of Complexity*, Vol. 23, Issues 4-6, (2007), 926-936.

DOI: 10.5540/03.2014.002.01.0049