

## 5

### Os grupos de Mathieu

#### 5.1

##### O Grupo $M_{24}$

##### 5.1.1

##### O $M_{24}$ , o Código de Golay e o $S(5, 8, 24)$

O maior grupo de Mathieu, o  $M_{24}$ , pode ser definido de diversas maneiras. A seguir, destaremos a relação do  $M_{24}$  com o Código de Golay e o sistema de Steiner  $S(5, 8, 24)$ .

##### 5.1.1.1

##### Grupo dos semi-automorfismos do hexacode

Como foi visto anteriormente, o hexacode  $\mathcal{H}_6$  é um subespaço vetorial 3 dimensional de  $\mathbb{F}_4^6$  gerado pelos vetores  $(w, \bar{w}, \bar{w}, w, \bar{w}, w)$ ,  $(\bar{w}, w, w, \bar{w}, \bar{w}, w)$  e  $(\bar{w}, w, \bar{w}, w, w, \bar{w})$ . Vimos também que uma forma de reconhecer se um vetor  $(a, b, c, d, e, f)$  está em  $\mathcal{H}_6$ , é verificar se existe uma função quadrática sobre  $\mathbb{F}_4$  satisfazendo  $\phi(0) = c$ ,  $\phi(1) = d$ ,  $\phi(w) = e$ ,  $\phi(\bar{w}) = f$ .

Seja  $G_A$  o grupo das matrizes  $M$  de permutação,  $M \in \mathbb{F}_4^{6 \times 6}$ , que preservam casais de um hexacodeword (ver 4.1.1). Dizemos que uma matriz  $M$  preserva casais de um hexacodeword quando para quaisquer  $x, y$  pertencentes a um casal do vetor temos que  $M.(x)$  e  $M.(y)$  também pertencem ao mesmo casal. Portanto como temos 3 casais sendo permutados e ainda pode haver uma troca dentro de cada casal segue que  $|G_A| = 3! \cdot 2^3 = 48$ . Porém, observe que nem todo elemento de  $G_A$  preserva o hexacode. Por exemplo, a matriz  $M$  de permutação em 5.1.1 preserva casais do hexacodeword mas não preserva o hexacode. De fato, a imagem do hexacodeword  $10\ 10\ w\bar{w}$  através de  $M$  é  $10\ 10\ \bar{w}w$  que não é um elemento do hexacode.

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} = (56) \quad (5.1.1)$$

Assim, podemos considerar  $G_B$  o subgrupo de  $G_A$  formado pelas matrizes de permutação que preservam o hexacode. Note que  $G_B \cong G_A$ , pois  $M \in G_A$  mas  $M \notin G_B$ . Pode-se checar que as três matrizes de permutação a seguir são elementos de  $G_B$  (lembre que  $w\bar{w} w\bar{w} w\bar{w} \in \mathcal{H}_6$ ):

$$(12)(34) = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$(13)(24) = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$(135)(246) = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

Assim, considere  $G_C$  subgrupo de  $G_B$  gerado por essas matrizes, isto é,  $G_C = \langle (12)(34), (13)(24), (135)(246) \rangle$ . Como  $S_4 \simeq \langle (12)(34), (13)(24), (135)(246) \rangle \cong S_4$ , temos que  $G_C$  tem 24 elementos. E portanto, temos:

$$G_C \leq G_B \cong G_A, \text{ com } |G_A| = 48 \text{ e } |G_C| = 24.$$

Donde  $G_C = G_B \cong S_4$ .

Desde que multiplicar por 1,  $w$  ou  $\bar{w}$  ainda preserva o hexacode podemos considerar  $G_S$  um grupo de simetrias do hexacode, gerado por multiplicações escalares e pelas permutações  $(12)(34)$ ,  $(13)(24)$ ,  $(135)(246)$ . Portanto,  $G_S \cong \mathbb{Z}/(3) \times S_4 = 3 \times S_4$ .

Denotaremos os grupos cíclicos  $\mathbb{Z}/(n)$  apenas por  $n$ .

O hexacode sobre a ação do grupo  $3 \times S_4$  está dividido em 5 órbitas. Listamos a seguir o tamanho e um representante de cada órbita:

Representante da órbita	Tamanho da órbita
$(0, 0, 0, 0, 0, 0)$	1
$(1, 1, 1, 1, 0, 0)$	9
$(w, \bar{w}, w, \bar{w}, w, \bar{w})$	12
$(1, 1, w, w, \bar{w}, \bar{w})$	6
$(0, 1, 0, 1, w, \bar{w})$	36

O grupo dos automorfismos do hexacode é definido como o conjunto das transformações lineares monomiais que preservam este código; denotaremos este grupo por  $G_{Aut}$ . A aplicação 5.1.2 é um exemplo de um elemento em  $G_{Aut}$ . Vamos mostrar que  $G_{Aut} = 3 \cdot A_6$ .

$$(x_1, x_2, x_3, x_4, x_5, x_6) \longmapsto (wx_1, \bar{w}x_2, x_3, x_6, x_4, x_5). \tag{5.1.2}$$

**Afirmção 5.1.1.** Substituir entradas não-nulas das matrizes monomiais pertencentes ao grupo de automorfismos do hexacode,  $G_{Aut}$ , define de maneira natural um homomorfismo  $\phi : G_{Aut} \longrightarrow S_6$ . Mais ainda, a imagem desta aplicação é  $A_6 < S_6$ .

*Demonstração.* Para obtermos  $A_6 \subseteq Im(\phi)$  basta tomarmos  $N \in G_{Aut}$  abaixo, (note que  $N$  é a matriz monomial que representa o automorfismo (5.1.2)):

$$N = \begin{pmatrix} w & 0 & 0 & 0 & 0 & 0 \\ 0 & \bar{w} & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \xrightarrow{\phi} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} = (456)$$

Verifica-se que as permutações  $(12)(34)$ ,  $(13)(24)$ ,  $(135)(246)$ ,  $(456)$  geram  $A_6$ . Logo,  $S_4 \subset A_6 \cong \langle (12)(34), (13)(24), (135)(246), (456) \rangle \subseteq Im(\phi)$ . Falta provarmos que  $Im(\phi) \subseteq A_6$ , isto é, se  $X \in G_{Aut}$  temos que  $\phi(X)$  é uma permutação par. Suponhamos, por absurdo, que  $Im(\phi) \neq A_6$ . Assim, teríamos:

$$A_6 \subsetneq Im(\phi) \subseteq S_6 \text{ e portanto } Im(\phi) = S_6.$$

Donde existiria, por exemplo, automorfismo de  $\mathcal{H}_6$  da forma:

$$A = \begin{pmatrix} + & 0 & 0 & 0 & 0 & 0 \\ 0 & + & 0 & 0 & 0 & 0 \\ 0 & 0 & + & 0 & 0 & 0 \\ 0 & 0 & 0 & + & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & + \\ 0 & 0 & 0 & 0 & + & 0 \end{pmatrix}, \text{ onde } + \in \{1, w, \bar{w}\}.$$

Olhando as imagens dos hexacodewords  $(1, 1, 1, 1, 0, 0)$  e  $(0, 0, 1, 1, 1, 1)$  através da matriz  $A$ , temos que:  $A.(1, 1, 1, 1, 0, 0) = (+, +, +, +, 0, 0) \in \mathcal{H}_6$ . Sem perda, podemos supor:  $A.(1, 1, 1, 1, 0, 0) = (1, 1, 1, 1, 0, 0)$  e

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

E assim,  $A.(0, 0, 1, 1, 1, 1) = (0, 0, 1, 1, +, +) \in \mathcal{H}_6$ . Donde teríamos:

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} = (5\ 6),$$

isto é, a permutação de coordenadas  $(5\ 6)$  seria uma automorfismo do hexacode. Mas de (5.1.1) já sabemos que  $A \notin G_{Aut}$ . Donde concluímos nossa afirmação.  $\square$

**Lema 5.1.2.** *O grupo de automorfismos do hexacode,  $G_{Aut}$ , é  $3 \cdot A_6$ .*

*Demonstração.* Pela afirmação anterior temos  $\phi : G_{Aut} \longrightarrow A_6$  homomorfismo de grupos sobrejetor. Tome  $M \in Ker(\phi)$ . Então:

$$M = \begin{pmatrix} + & 0 & 0 & 0 & 0 & 0 \\ 0 & + & 0 & 0 & 0 & 0 \\ 0 & 0 & + & 0 & 0 & 0 \\ 0 & 0 & 0 & + & 0 & 0 \\ 0 & 0 & 0 & 0 & + & 0 \\ 0 & 0 & 0 & 0 & 0 & + \end{pmatrix}, \text{ onde } + \in \{1, w, \bar{w}\}.$$

Considere os hexacodewords  $(1, 1, 1, 1, 0, 0)$  e  $(0, 0, 1, 1, 1, 1)$ . Portanto,  $M.(1, 1, 1, 1, 0, 0) = (x, x, x, x, 0, 0)$  e  $M.(0, 0, 1, 1, 1, 1) = (0, 0, y, y, y, y)$ .  
Donde

$$M = \begin{pmatrix} x & 0 & 0 & 0 & 0 & 0 \\ 0 & x & 0 & 0 & 0 & 0 \\ 0 & 0 & x=y & 0 & 0 & 0 \\ 0 & 0 & 0 & x=y & 0 & 0 \\ 0 & 0 & 0 & 0 & y & 0 \\ 0 & 0 & 0 & 0 & 0 & y \end{pmatrix} \implies M = x.Id, \text{ onde } x \in \mathbb{F}_4^*.$$

Portanto,  $Ker(\phi) \approx \mathbb{Z}/(3)$  e pelo Primeiro Teorema dos Isomorfismos, temos:  $G_{Aut}/Ker(\phi) \approx A_6$ . Donde,  $G_{Aut} = 3 \cdot A_6$ . □

Assim, vimos que nenhum automorfismo de  $\mathcal{H}_6$  induz permutações ímpares. No entanto, podemos estender o grupo  $3 \cdot A_6$  dos automorfismos do hexacode ao grupo  $3 \cdot S_6$  dos semi-automorfismos deste código pela adjunção do anti-automorfismo 5.1.3 abaixo.

$$(x_1, x_2, x_3, x_4, x_5, x_6) \longrightarrow (\overline{x_1}, \overline{x_2}, \overline{x_3}, \overline{x_4}, \overline{x_6}, \overline{x_5}). \tag{5.1.3}$$

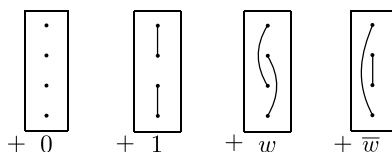
### 5.1.1.2

#### $3 \cdot S_6$ e o Código de Golay.

O maior **grupo de Mathieu**, o  $M_{24}$ , pode ser definido como o grupo de permutações de 24 pontos que preservam o Código de Golay. Equivalentemente,  $M_{24}$  é o grupo dos automorfismos do  $S(5, 8, 24)$ .

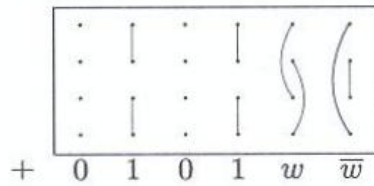
Vimos no capítulo 3 que é prático arrumar as 24 coordenadas de um vetor de  $\mathcal{C}_{24}$  no MOG. Nessa matriz os vetores de  $\mathcal{C}_{24}$  tem suas coordenadas indexadas pelos 24 pontos  $(i, x) \in X = \{1, \dots, 6\} \times \mathbb{F}_4$ . Veremos que a ação do hexacode e dos semi-automorfismos do hexacode em  $X$  definem de maneira natural elementos de  $M_{24}$ . Dessa maneira, teremos que  $2^6$  e  $3 \cdot S_6$  são subgrupos de  $M_{24}$ . Veremos que estes dois subgrupos geram um produto semi-direto  $2^6 : 3 \cdot S_6 < M_{24}$ .

Os elementos do hexacode (que como grupo aditivo é isomorfo a  $2^6$ ) agem sobre  $X$  por adição:  $(x_1, x_2, x_3, x_4, x_5, x_6)$  aplica  $(i, x)$  em  $(i, x + x_i)$ . Temos assim uma inclusão natural  $2^6 < M_{24}$ . Nas colunas do MOG isso funciona como na figura abaixo:



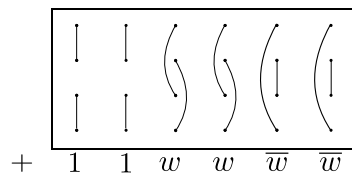
Vejamos alguns exemplos:

**Exemplo 25.** A ação do hexacodeword  $(0, 1, 0, 1, w, \bar{w})$  sobre os 24 pontos do MOG resulta no seguinte elemento de  $M_{24}$ :



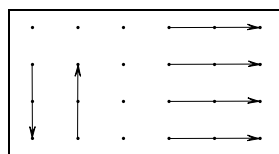
Dois pontos são ligados por uma aresta quando formam um ciclo de tamanho dois.

**Exemplo 26.** Analogamente a ação do hexacodeword  $(1, 1, w, w, \bar{w}, \bar{w})$  é



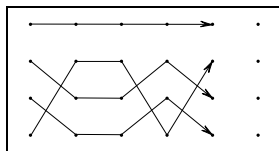
Temos também que automorfismos do hexacode definem permutações de  $X$  e automorfismos de  $\mathcal{C}_{24}$ . Assim,  $3 \cdot A_6 < M_{24}$ . Os elementos do grupo  $3 \cdot A_6$  agem em  $X$  aplicando  $(i, x)$  em  $(\pi(i), c_i x)$ , onde  $\pi \in A_6$  e  $c_i \in \mathbb{F}_4^*$ . Em outras palavras, um automorfismo  $\varphi$  do hexacode é tal que  $\varphi(xe_i) = c_i \cdot x \cdot e_{\pi(i)}$ . A seguir temos alguns exemplos de automorfismos  $\varphi$  do hexacode e sua ação no MOG:

**Exemplo 27.**  $\varphi : \mathcal{H}_6 \longrightarrow \mathcal{H}_6$   
 $(x_1, x_2, x_3, x_4, x_5, x_6) \longmapsto (wx_1, \bar{w}x_2, x_3, x_6, x_4, x_5)$

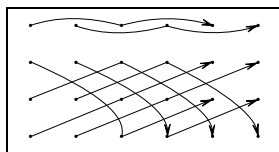


As setas ligando três pontos de  $X$  indicam um ciclo de tamanho três. Assim, neste exemplo, os pontos  $(4, 0), (5, 0)$  e  $(6, 0)$  formam um ciclo de tamanho 3 com  $(6, 0)$  sendo levado em  $(4, 0)$ . A seta indica a orientação do ciclo.

**Exemplo 28.**  $\varphi : \mathcal{H}_6 \longrightarrow \mathcal{H}_6$   
 $(x_1, x_2, x_3, x_4, x_5, x_6) \longmapsto (\bar{w}x_5, wx_1, x_2, \bar{w}x_3, wx_4, x_6)$



**Exemplo 29.**  $\varphi : \mathcal{H}_6 \longrightarrow \mathcal{H}_6$   
 $(x_1, x_2, x_3, x_4, x_5, x_6) \longmapsto (\overline{w}x_5, \overline{w}x_6, \overline{w}x_1, \overline{w}x_2, \overline{w}x_3, \overline{w}x_4)$

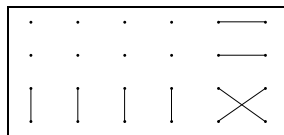


Similarmente, um anti-automorfismo do hexacode também define uma permutação de  $X$  e portanto um automorfismo de  $\mathcal{C}_{24}$ ; assim  $3 \cdot S_6 < M_{24}$ . Elementos de  $3 \cdot S_6$  agem em  $X$  aplicando  $(i, x)$  em  $(\pi(i), c_i \overline{x})$ , onde  $\pi \in S_6$  e  $c_i \in \mathbb{F}_4^*$ . Isto é, um anti-automorfismo  $\psi$  do hexacode é tal que  $\psi(xe_i) = c_i \cdot \overline{x} \cdot e_{\pi(i)}$ .

**Exemplo 30.** Considere a ação do anti-automorfismo 5.1.3 do hexacode no MOG:

$$\varphi : \mathcal{H}_6 \longrightarrow \mathcal{H}_6$$

$$(x_1, x_2, x_3, x_4, x_5, x_6) \longmapsto (\overline{x}_1, \overline{x}_2, \overline{x}_3, \overline{x}_4, \overline{x}_6, \overline{x}_5)$$



Portanto vimos que  $2^6$  e  $3 \cdot S_6$  são subgrupos de  $M_{24}$ . Agora veremos que estes dois subgrupos geram um produto semi-direto  $2^6 : 3 \cdot S_6$  que portanto também é subgrupo de  $M_{24}$ . Para isso, é suficiente provarmos que o hexacode é fechado por conjugação com respeito aos elementos de  $3 \cdot S_6$ . De fato, seja  $\psi : \mathbb{F}_4^6 \longrightarrow \mathbb{F}_4^6$  um semi-automorfismo do hexacode. Este, interpretado como permutação, nos dá um elemento  $\mu_\psi$  de  $M_{24}$ . Seja  $v$  um elemento do hexacode. A ação de  $v$  nos 24 pontos do MOG nos dá um elemento  $\mu_v \in M_{24}$ . Queremos mostrar que  $\mu_\psi \cdot \mu_v \cdot \mu_\psi^{-1} = \mu_{\psi(v)}$ . Mas isso realmente acontece, desde que:

$$(i, x) \xrightarrow{\mu_v} (i, x + iv_i) \xrightarrow{\mu_\psi} (\pi(i), c_i(x + v_i)),$$

$$(i, x) \xrightarrow{\mu_\psi} (\pi(i), c_i x) \xrightarrow{\mu_{\psi(v)}} (\pi(i), c_i x + c_i v_i).$$

**Conclusão:** Construimos um subgrupo  $2^6 : 3 \cdot S_6$  de  $M_{24}$ . Estas permutações de  $X$  respeitam a decomposição de  $X$  em 6 colunas. Assim,  $M_{24}$  age sobre o conjunto dos sextets e o subgrupo  $2^6 : 3 \cdot S_6$  estabiliza o sextet base. Veremos ainda que este subgrupo é maximal em  $M_{24}$ .

**5.1.1.3**

**$2^6 : 3 \cdot S_6$  é o estabilizador do sextet base.**

Vimos que o grupo  $2^6 : 3 \cdot S_6$  está contido no estabilizador do sextet base. Agora vamos provar que este subgrupo de  $M_{24}$  é o estabilizador do sextet base, isto é, nenhum subgrupo de  $M_{24}$  maior que  $2^6 : 3 \cdot S_6$  estabiliza esse sextet.

Para isso, defina  $G_1$  o subgrupo de  $M_{24}$  formado por permutações que respeitam o sextet base. A fim de facilitar a notação, chamaremos  $G_2 = 2^6 : 3 \cdot S_6 < G_1$ . Nosso objetivo é provar que  $G_1 = G_2$ .

**Proposição 5.1.3.** *As 759 octads do Código de Golay são divididas em 3 órbitas de comprimentos 384, 360 e 15, tanto por  $G_1$  quanto por  $G_2$ .*

*Demonstração.* Considere as 759 octads do Código de Golay. Abaixo temos um representante e a contagem dos elementos de cada órbita sobre a ação do grupo  $G_1$  ou  $G_2$ .

0	1	1	1	1	1
1					
1					
1					

Considere octads com distribuição coluna  $3^1 1^5$ .

Assim temos 6 possibilidades para a escolha da coluna que irá receber 3 pontos e  $2^6$  posições para as coordenadas diferentes em cada coluna. Logo temos  $6 \cdot (2^6) = 384$  elementos nesta órbita.

1	1	1	1
1	1	1	1

Considere octads com distribuição coluna  $2^4$ .

Note que os 8 hexacodewords que tem os 4 primeiros dígitos compostos apenas de zeros e uns preservam essa octad. Portanto temos  $8 = \frac{2^6}{2^3}$  possibilidades de hexacodewords, ainda podemos multiplicar por  $1, w$  e  $\bar{w}$  e  $15 = \binom{6}{2}$  pares de colunas vazias. Logo o número de octads nessa órbita é  $8 \cdot 3 \cdot 15 = 360$ .

1	1
1	1
1	1
1	1

Considere octads com distribuição coluna  $4^2$ .

Temos 6 colunas e queremos escolher duas para receber 4 pontos cada; logo



temos  $15 = \binom{6}{2}$  pares de colunas deste tipo. E portanto o número de elementos nesta órbita é 15.

Como  $384+360+15=759$ , concluímos nossa afirmação.  $\square$

Considere os seguintes homomorfismos  $\psi_1 : G_1 \rightarrow S_6$  e  $\psi_2 : G_2 \rightarrow S_6$ , definidos pela ação nas 6 colunas do MOG. É claro que  $\psi_2$  é sobrejetora e portanto  $\psi_1$  também o é. Chamemos de  $H_1$  e  $H_2$  os núcleos de  $\psi_1$  e  $\psi_2$ , respectivamente. Assim,  $H_1$  e  $H_2$  são formados por permutações que preservam o Código de Golay e cada coluna do sextet base. Pelo Primeiro Teorema dos Isomorfismos, temos  $G_1/H_1 \approx S_6$  e  $G_2/H_2 \approx S_6$ . Como,  $|G_2| = 2^6 \cdot 3 \cdot 6!$  e  $\frac{|G_2|}{|H_2|} = |S_6| = 6!$  segue que  $|H_2| = 2^6 \cdot 3$  e o índice de  $H_2$  em  $G_2$  é  $6!$ . Temos também que o índice do subgrupo  $H_1$  e  $G_1$  é  $6!$ .

Considere no conjunto das 759 octads do código de Golay a  $[G_1$  ou  $G_2]$ -órbita composta de 384 octads; cujo um representante é:

0	1	1	1	1	1
1					
1					
1					

Visto que  $H_2$  preserva o Código de Golay e cada coluna do sextet base, esta órbita sobre a ação deste grupo é dividida em 6 órbitas com 64 elementos cada. Abaixo listamos os 6 representantes para cada uma dessas órbitas:

0	1	1	1	1	1
1					
1					
1					

1	0	1	1	1	1
	1				
	1				
	1				

1	1	0	1	1	1
		1			
		1			
		1			

1	1	1	0	1	1
			1		
			1		
			1		

1	1	1	1	0	1
				1	
				1	
				1	

1	1	1	1	1	0
					1
					1
					1

E novamente  $H_1$  e  $H_2$  órbitas tem os mesmos elementos. Portanto  $H_1$  age transitivamente sobre o conjunto das 64 octads da forma:

0	1	1	1	1	1
1					
1					
1					

ou

3	1	1	1	1	1
---	---	---	---	---	---

(# de 1's por coluna)

Considere  $K_1 < H_1$  o estabilizador da octad

0	1	1	1	1	1
1					
1					
1					

. Mais

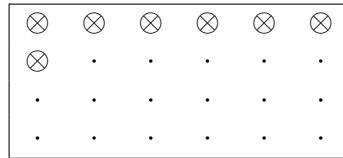
ainda,  $K_1$  consiste das permutações que respeitam Código de Golay, fixam cada coluna e cada elemento da primeira linha. Logo, os elementos de  $K_1$  são da forma abaixo, onde os parafusos  $\otimes$  indicam pontos obrigatoriamente fixos:

$\otimes$	$\otimes$	$\otimes$	$\otimes$	$\otimes$	$\otimes$
.	.	.	.	.	.
.	.	.	.	.	.
.	.	.	.	.	.

De maneira análoga, considere  $K_2 < H_2$  (e portanto  $K_2 < K_1$ ). Assim,  $K_2$  é gerado por

$\otimes$	$\otimes$	$\otimes$	$\otimes$	$\otimes$	$\otimes$
↓	↓	↓	↓	↓	↓
↓	↓	↓	↓	↓	↓

Donde  $K_2 \approx Z/(3)$  e  $id_{H_2}(K_2) = \frac{(2^6).3}{3} = 64$ . Chamemos de  $L_1$  o subgrupo de



$K_1$ , de índice 3, que além de fixar todos os elementos da primeira linha fixa também o elemento (1,1) do conjunto X. Assim,  $L_1$  fixa os seguintes elementos:

Analogamente, defina  $L_2$  subgrupo de  $K_2$  com a mesma propriedade.

**Afirmção 5.1.4.**  $L_1 = \{1\}$ .

(A prova dessa afirmação será feita a seguir).

Temos pela afirmação acima  $L_1 = \{1\}$ , e como  $L_2 < L_1$  segue que  $L_1 = \{1\}$  e  $id_{K_2}(L_2) = 3$ .

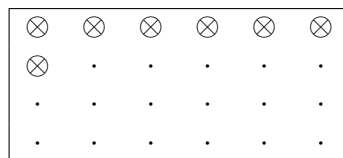
E portanto obtemos a seguinte cadeia de grupos:

$$\begin{array}{ccccccc} G_1 & \overset{6!}{>} & H_1 & \overset{2^6}{>} & K_1 & \overset{3}{>} & L_1 \\ \cup & & \cup & & \cup & & \cup \\ G_2 & \overset{6!}{>} & H_2 & \overset{2^6}{>} & K_2 & \overset{3}{>} & L_2 \end{array}$$

E de  $L_1 = L_2$ , resulta em  $H_1 = H_2$  e  $G_1 = G_2$ .

**Comentário 5.1.5.** Assim, desde que a afirmação 5.1.4 seja verdadeira teremos que o subgrupo  $2^6 : 3 \cdot S_6$  de  $M_{24}$  é o estabilizador do sextet base.

Vamos provar a afirmação 5.1.4, que nos dizia  $L_1 = \{1\}$ . Lembre que os seguintes pontos de X estavam fixos pela ação de  $L_1$ :



Lembre também que 5 pontos determinam uma única octad e que  $L_1$  fixa colunas. Vamos agora considerar o efeito de  $L_1$  sobre algumas octads a fim de obter o resultado desejado.

Pela definição de  $L_1$  e do  $S(5,8,24)$  temos que um elemento de  $L_1$  preserva, por exemplo, as octads abaixo:

$$\begin{array}{|c|c|c|c|} \hline 1 & 1 & 1 & 1 \\ \hline 1 & 1 & 1 & 1 \\ \hline \end{array} \quad \begin{array}{|c|c|c|c|} \hline 1 & 1 & & 1 & 1 \\ \hline 1 & 1 & & 1 & 1 \\ \hline \end{array} .$$

Donde todo elemento de  $L_1$  fixa todos os elementos da primeira e segunda

linha do MOG:

$$\begin{array}{|c|c|c|c|c|c|} \hline \otimes & \otimes & \otimes & \otimes & \otimes & \otimes \\ \hline \otimes & \otimes & \otimes & \otimes & \otimes & \otimes \\ \hline \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \hline \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \hline \end{array}$$

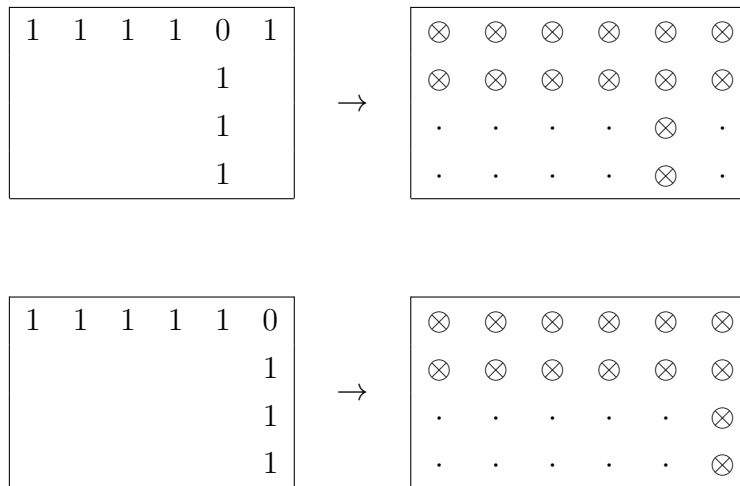
A partir daí e analisando o efeito de um elemento de  $L_1$  sobre as octads a seguir temos que  $L_1$  fixa os seguintes pontos:

$$\begin{array}{|c|c|c|c|c|c|} \hline 0 & 1 & 1 & 1 & 1 & 1 \\ \hline 1 & & & & & \\ \hline 1 & & & & & \\ \hline 1 & & & & & \\ \hline \end{array} \rightarrow \begin{array}{|c|c|c|c|c|c|} \hline \otimes & \otimes & \otimes & \otimes & \otimes & \otimes \\ \hline \otimes & \otimes & \otimes & \otimes & \otimes & \otimes \\ \hline \otimes & \cdot & \cdot & \cdot & \cdot & \cdot \\ \hline \otimes & \cdot & \cdot & \cdot & \cdot & \cdot \\ \hline \end{array}$$

$$\begin{array}{|c|c|c|c|c|c|} \hline 1 & 0 & 1 & 1 & 1 & 1 \\ \hline 1 & & & & & \\ \hline 1 & & & & & \\ \hline 1 & & & & & \\ \hline \end{array} \rightarrow \begin{array}{|c|c|c|c|c|c|} \hline \otimes & \otimes & \otimes & \otimes & \otimes & \otimes \\ \hline \otimes & \otimes & \otimes & \otimes & \otimes & \otimes \\ \hline \cdot & \otimes & \cdot & \cdot & \cdot & \cdot \\ \hline \cdot & \otimes & \cdot & \cdot & \cdot & \cdot \\ \hline \end{array}$$

$$\begin{array}{|c|c|c|c|c|c|} \hline 1 & 1 & 0 & 1 & 1 & 1 \\ \hline & 1 & & & & \\ \hline & 1 & & & & \\ \hline & 1 & & & & \\ \hline \end{array} \rightarrow \begin{array}{|c|c|c|c|c|c|} \hline \otimes & \otimes & \otimes & \otimes & \otimes & \otimes \\ \hline \otimes & \otimes & \otimes & \otimes & \otimes & \otimes \\ \hline \cdot & \cdot & \otimes & \cdot & \cdot & \cdot \\ \hline \cdot & \cdot & \otimes & \cdot & \cdot & \cdot \\ \hline \end{array}$$

$$\begin{array}{|c|c|c|c|c|c|} \hline 1 & 1 & 1 & 0 & 1 & 1 \\ \hline & & & 1 & & \\ \hline & & & 1 & & \\ \hline & & & 1 & & \\ \hline \end{array} \rightarrow \begin{array}{|c|c|c|c|c|c|} \hline \otimes & \otimes & \otimes & \otimes & \otimes & \otimes \\ \hline \otimes & \otimes & \otimes & \otimes & \otimes & \otimes \\ \hline \cdot & \cdot & \cdot & \otimes & \cdot & \cdot \\ \hline \cdot & \cdot & \cdot & \otimes & \cdot & \cdot \\ \hline \end{array}$$



Donde concluimos que todos os elementos são fixos pela ação de  $L_1$ . E portanto  $L_1 = \{1\}$ .

**Conclusão:** o subgrupo  $2^6 : 3 \cdot S_6$  de  $M_{24}$  é o estabilizador do sextet base.

#### 5.1.1.4

#### $M_{24}$ e seu subgrupo maximal $2^6 : 3 \cdot S_6$

Nesta seção encontraremos as órbitas dos sextets sobre a ação do  $2^6 : 3 \cdot S_6$  a fim de calcularmos a ordem de  $M_{24}$  e provarmos o fato deste grupo ser altamente transitivo em  $\Omega$ . Provaremos também que  $2^6 : 3 \cdot S_6$  é um subgrupo maximal de  $M_{24}$ .

**Afirmção 5.1.6.** Sabemos que existem 1771 sextets no Código de Golay. Sobre a ação do grupo  $2^6 : 3 \cdot S_6$  esses sextets são divididos em 4 órbitas. A primeira órbita, de tamanho 1, é o sextet base que consiste das seis colunas do MOG. A segunda órbita de tamanho 90, consiste dos sextets cuja cada tetrad (4-conjunto) que o compõe tem dois pontos em uma coluna e dois pontos na outra. A terceira órbita, de tamanho 240, consiste dos sextets que dois dos seus tetrads tem três pontos em uma coluna e um ponto em uma outra coluna. A quarta e última órbita, de tamanho 1440, consiste dos sextets que quatro dos seus tetrads tem dois pontos em uma coluna e os outros dois em outras duas colunas. Abaixo exibimos um representante para cada uma dessas órbitas:

1	2	3	4	5	6
1	2	3	4	5	6
1	2	3	4	5	6
1	2	3	4	5	6

1	1	3	3	5	5
1	1	3	3	5	5
2	2	4	4	6	6
2	2	4	4	6	6

1	2	3	3	3	3
2	1	4	4	4	4
2	1	5	5	5	5
2	1	6	6	6	6

1	1	1	2	5	6
1	2	2	2	4	3
3	5	6	4	3	6
4	6	5	3	5	4

onde os seis tetrads de cada sextet são rotulados de 1 a 6.

*Demonstração.* Inicialmente observe que qualquer tetrad com a distribuição coluna  $2^2, 3^1 1^1, 1^2 2^1$  realmente pertence a segunda, terceira, quarta órbita, respectivamente. Pois os elementos do grupo  $2^6 : 3 \cdot S_6$  nos permitem permutar as colunas, somar hexacodewords e multiplicar por  $1, w$  ou  $\bar{w}$ . Note que ao considerarmos tetrads com a distribuição coluna  $1^4$  eles podem pertencer a terceira ou quarta órbita.

Calcularemos explicitamente o comprimento das três órbitas não triviais dos 1771 sextets do Código de Golay sobre a ação do subgrupo  $2^6 : 3 \cdot S_6$  de  $M_{24}$ .

1	1	3	3	5	5
1	1	3	3	5	5
2	2	4	4	6	6
2	2	4	4	6	6

Considere um sextet na segunda órbita.

O número de 4-conjuntos com dois pontos em uma coluna e dois pontos em outra é  $\binom{6}{2} \cdot \binom{4}{2} \cdot \binom{4}{2} = 15 \cdot 6 \cdot 6$ . E como temos seis tetrads deste tipo nesta sextet e um tetrad determina um único sextet segue que, o número de sextets nesta órbita é:  $\frac{15 \cdot 6 \cdot 6}{6} = 90$ .

1	2	3	3	3	3
2	1	4	4	4	4
2	1	5	5	5	5
2	1	6	6	6	6

Considere um sextet na terceira órbita.

O número de 4-conjuntos com 3 pontos em uma coluna e 1 ponto em outra é  $\binom{6}{1} \cdot \binom{5}{1} \cdot \binom{4}{1} \cdot \binom{4}{3} = 6 \cdot 5 \cdot 4 \cdot 4$ . Desde que temos dois tetrads com essa distribuição coluna em cada sextet temos  $\frac{6 \cdot 5 \cdot 4 \cdot 4}{2} = 240$  elementos nesta órbita.

1	1	1	2	5	6
1	2	2	2	4	3
3	5	6	4	3	6
4	6	5	3	5	4

Considere um sextet na quarta órbita.

O número de 4-conjuntos com dois pontos em uma coluna e os outros dois em outras duas é:  $\binom{6}{1} \cdot \binom{5}{2} \cdot \binom{4}{2} \cdot \binom{4}{1} \cdot \binom{4}{1} = 6 \cdot \frac{5 \cdot 4}{2} \cdot \frac{4 \cdot 3}{2} \cdot 4 \cdot 4$ . Como temos quatro tetrads deste tipo neste sextet segue que temos  $\frac{6 \cdot \frac{5 \cdot 4}{2} \cdot \frac{4 \cdot 3}{2} \cdot 4 \cdot 4}{4} = 1440$ .

Como  $1+90+240+1440=1771$  temos que essas são todas as órbitas.  $\square$

**Teorema 5.1.7.** *O grupo  $M_{24}$  age transitivamente em sextets.*

*Demonstração.* Considere a permutação  $\alpha$  a seguir:

$$\alpha = \begin{array}{c} \begin{array}{|c|c|c|c|c|c|} \hline \cdot & \cdot & \cdot & \cdot & \diagup & \diagdown \\ \hline \cdot & \cdot & \cdot & \cdot & \diagdown & \diagup \\ \hline \hline & \hline & \hline & \hline & | & | \\ \hline \hline & \hline & \hline & \hline & | & | \\ \hline \end{array} \end{array} \tag{5.1.4}$$

Checando a ação de  $\alpha$  em uma base do Código de Golay temos que  $\alpha$  fixa este código; e portanto  $\alpha \in M_{24}$  (ver apêndice).

Mais ainda,  $\alpha$  torna as 4 órbitas dos sextets sobre a ação do  $2^6 : 3 \cdot S_6$  em uma única órbita sobre  $M_{24}$ . De fato, basta considerar a ação de  $\alpha$  nos sextets abaixo:

1	2	3	4	5	6
1	2	3	4	5	6
1	2	3	4	5	6
1	2	3	4	5	6

 $\xrightarrow{\alpha}$ 

1	2	3	4	6	5
1	2	3	4	6	5
2	1	4	3	5	6
2	1	4	3	5	6

3	1	1	3	5	5
4	2	2	4	6	5
4	2	2	4	5	6
3	1	1	3	6	6

 $\xrightarrow{\alpha}$ 

3	1	1	3	5	6
4	2	2	4	5	5
2	4	4	2	6	6
1	3	3	1	5	6

$$\begin{array}{|c|c|c|c|c|c|} \hline 2 & 3 & 1 & 3 & 3 & 3 \\ \hline 1 & 4 & 2 & 4 & 5 & 6 \\ \hline 1 & 6 & 2 & 6 & 4 & 5 \\ \hline 1 & 5 & 2 & 5 & 6 & 4 \\ \hline \end{array} \xrightarrow{\alpha} \begin{array}{|c|c|c|c|c|c|} \hline 2 & 3 & 1 & 3 & 6 & 5 \\ \hline 1 & 4 & 2 & 4 & 3 & 3 \\ \hline 6 & 1 & 6 & 2 & 6 & 4 \\ \hline 5 & 1 & 5 & 2 & 4 & 5 \\ \hline \end{array} .$$

Donde  $M_{24}$  age transitivamente em sextets.

□

Como sabemos que  $M_{24}$  é transitivo em sextets e o seu subgrupo  $2^6 : 3 \cdot S_6$  é o estabilizador do sextet base, segue que:

$$|M_{24}| = 1771 \cdot 2^6 \cdot 3 \cdot 6! = 244823040 = 2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23.$$

**Teorema 5.1.8.** *O subgrupo  $2^6 : 3 \cdot S_6$  é maximal em  $M_{24}$ .*

*Demonstração.* Suponha, por absurdo, que o subgrupo  $2^6 : 3 \cdot S_6$  não seja maximal em  $M_{24}$ . Assim existiria  $H$  subgrupo de  $M_{24}$ , com  $2^6 : 3 \cdot S_6 \subsetneq H < M_{24}$ . Considere o sextet base. Diremos que um sextet é atingido se existir uma permutação  $\pi$  em  $H$  tal que  $\pi(\text{sextet base}) = \text{sextet}$ . Como exemplo ilustrativo, consideremos o sextet abaixo, ele é dito atingido se existe  $\pi \in H$  tal que:

$$\begin{array}{|c|c|c|c|c|c|} \hline 1 & 2 & 3 & 4 & 5 & 6 \\ \hline 1 & 2 & 3 & 4 & 5 & 6 \\ \hline 1 & 2 & 3 & 4 & 5 & 6 \\ \hline 1 & 2 & 3 & 4 & 5 & 6 \\ \hline \end{array} \xrightarrow{\pi} \begin{array}{|c|c|c|c|c|c|} \hline 1 & 1 & 3 & 3 & 5 & 5 \\ \hline 1 & 1 & 3 & 3 & 5 & 5 \\ \hline 2 & 2 & 4 & 4 & 6 & 6 \\ \hline 2 & 2 & 4 & 4 & 6 & 6 \\ \hline \end{array}$$

Diremos que um sextet é totalmente atingido se para toda permutação em  $M_{24}$  com  $\pi(\text{sextet base}) = \text{sextet}$ , tem-se  $\pi \in H$ .

**Afirmção.** Se um sextet é atingido então ele é totalmente atingido.

*Demonstração.* Suponha que exista um sextet atingido (que chamaremos de *sextet atingido*<sub>1</sub>). Assim, existe  $\pi_1 \in H$  tal que  $\pi_1(\text{sextet base}) = (\text{sextet atingido})_1$ . Considere  $\pi_2 \in M_{24}$  tal que  $\pi_2(\text{sextet base}) = (\text{sextet atingido})_1$ . Assim,  $\pi_2^{-1} \circ \pi_1$  preserva o sextet base. Donde temos  $\pi_2^{-1} \circ \pi_1 \in 2^6 : 3 \cdot S_6 < H$  e portanto  $\pi_2 \in H$ . □

**Afirmção.** Se um sextet é atingido então toda a sua classe é atingida.



*Demonstração.* Considere dois sextets na mesma classe (chamaremos estes de *sextet atingido*<sub>1</sub> e *sextet*). Como, por hipótese, um desses sextets é atingido existe  $\pi_1 \in H$  tal que  $\pi_1(\textit{sextet base}) = (\textit{sextet atingido}_1)$ . Como o *sextet atingido*<sub>1</sub> e o *sextet* pertencem a mesma classe, existe permutação  $\pi$  em  $2^6 : 3 \cdot S_6 < H$  tal que  $\pi(\textit{sextet atingido}_1) = (\textit{sextet})$ . Donde  $\pi \circ \pi_1 \in H$ , com  $\pi(\textit{sextet base}) = (\textit{sextet})$ , e portanto concluímos nossa afirmação.  $\square$

Sabemos que pela ação do  $2^6 : 3 \cdot S_6$  os 1771 sextets estão divididos em 4 órbitas de tamanho 1, 90, 240, 1771. Daí, e pela afirmação anterior temos as seguintes possibilidades para o índice de  $2^6 : 3 \cdot S_6$  em  $H$ :

$$1, 91, 241, 331, 1441, 1531, 1681, 1771.$$

Como o índice de  $2^6 : 3 \cdot S_6$  em  $M_{24}$  é 1771 temos que o índice de  $2^6 : 3 \cdot S_6$  em  $H$  divide 1771. Donde temos que o índice de  $2^6 : 3 \cdot S_6$  em  $H$  é 1 ou 1771. E portanto  $2^6 : 3 \cdot S_6$  é subgrupo maximal de  $M_{24}$ .  $\square$

**Lema 5.1.9.** *O subgrupo de  $M_{24}$  estabilizador pontual de uma tetrad é da forma  $2^4 : A_5$ .*

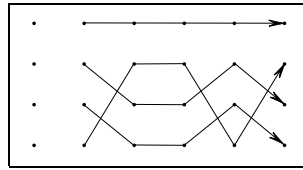
*Demonstração.* Tome 4 pontos em  $\Omega$ . Como 4 pontos determinam um único sextet e  $M_{24}$  é transitivo em sextets, sem perda, podemos considerar esses 4 pontos sendo a primeira coluna do MOG. Chamemos de  $G < M_{24}$  o estabilizador pontual dos 4 pontos a seguir:

⊗					
⊗					
⊗					
⊗					

Como  $G$  fixa a primeira coluna do MOG e esta é  $\mathbb{F}_4$ -linear temos que  $G < 2^6 : 3 \cdot A_6$ . A ação de  $G$  permuta as 5 colunas restantes, que formam um sistema de imprimitividade. Então, considere o homomorfismo  $\varphi : G \rightarrow S_5$ . O núcleo de  $\varphi$  é formado pelos elementos de  $G$  que fixam todas as colunas do MOG, donde inicialmente temos  $Ker(\varphi) \leq 2^6 : 3$ . Mais ainda, como a primeira coluna é fixada ponto-a-ponto temos  $Ker(\varphi) \leq 2^6$ . Logo o núcleo de  $\varphi$  é composto pelos hexacodewords cujo o primeiro dígito é zero. Conseqüentemente os elementos do núcleo de  $\varphi$  correspondem a somar hexacodewords com primeira coordenada igual a 0 e portanto  $Ker(\varphi) \cong 2^4$ . Como  $G < 2^6 : 3 \cdot A_6$  temos  $Im(\varphi) \leq A_5$ . Considerando o automorfismo do hexacode

$$(x_1, x_2, x_3, x_4, x_5, x_6) \mapsto (x_1, \bar{w}x_6, wx_2, x_3, \bar{w}x_4, wx_5)$$

cuja a ação nos 24 pontos do MOG é o elemento de  $G$  a seguir, temos que  $Im(\varphi) = A_5$



Segue do Primeiro Teorema dos Isomorfismos que  $G/2^4 \cong A_5$ . Logo  $|G| = 2^4 \cdot \frac{5!}{2}$ . Considere  $N < G$  formado pelos automorfismos do hexacode, isto é,  $N < 3 \cdot S_6$ . Como  $N$  fixa pontualmente a primeira coluna do MOG temos  $N < A_5$ . Certamente todas as permutações de  $A_5$  são realizadas nesse grupo. Logo  $N \cong A_5$ . Como  $A_5 \cap 2^4 = \{e\}$  temos que  $G = 2^4 : A_5$ .  $\square$

Note que  $2^4 : A_5$  age transitivamente sobre os 20 pontos restantes.

**Teorema 5.1.10.** *O grupo  $M_{24}$  é 5-transitivo nos 24 pontos de  $\Omega$ .*

*Demonstração.* Escolha dois conjuntos de 5 pontos distintos  $x_1, x_2, x_3, x_4, x_5$  e  $y_1, y_2, y_3, y_4, y_5$ . Como 4 pontos determinam um único sextet considere os 2 sextets contendo  $x_1, x_2, x_3, x_4$  e  $y_1, y_2, y_3, y_4$ . Como  $M_{24}$  é transitivo em sextets podemos supor que ambos os sextets foram levados no sextet base. Daí, e como o grupo estabilizador de um sextet é transitivo nos seis tetrads temos que existe elemento nesse grupo que leva o tetrad composto por  $x_1, x_2, x_3, x_4$  no tetrad composto por  $y_1, y_2, y_3, y_4$ . Mais ainda, fixando esse tetrad temos que todas as permutações de  $S_4$  são realizadas nos pontos desse tetrad. Portanto, podemos considerar que  $x_i$  foi levado em  $y_i$  para todo  $1 \leq i \leq 4$ . E finalmente como o grupo estabilizador de um tetrad é o  $2^4 : A_5$  o qual é transitivo nos 20 pontos restantes, temos que  $x_5$  é levado em  $y_5$ . Donde  $M_{24}$  é 5-transitivo.  $\square$

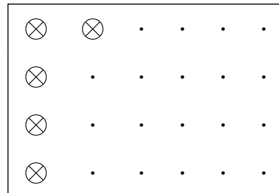
**5.1.1.5**  
**O estabilizador de uma octad**

**Teorema 5.1.11.** *O grupo  $M_{24}$  age transitivamente em octads.*

*Demonstração.* Sejam duas octads  $\mathcal{O}_1$  e  $\mathcal{O}_2$ . Queremos provar que existe permutação  $\pi$  em  $M_{24}$  tal que  $\pi(\mathcal{O}_1) = \mathcal{O}_2$ . Para isso, tome quaisquer dois conjuntos de 5 pontos  $\{x_1, x_2, x_3, x_4, x_5\}$  e  $\{y_1, y_2, y_3, y_4, y_5\}$  contidos em  $\mathcal{O}_1$  e  $\mathcal{O}_2$ , respectivamente. Como  $M_{24}$  é 5-transitivo, segue que existe permutação  $\pi$  em  $M_{24}$  com  $\pi(\{x_1, x_2, x_3, x_4, x_5\}) = \{y_1, y_2, y_3, y_4, y_5\}$ . Daí e como, por definição,  $M_{24}$  preserva o sistema de Steiner  $S(5, 8, 24)$  temos que  $\pi(\mathcal{O}_1) = \mathcal{O}_2$ .  $\square$

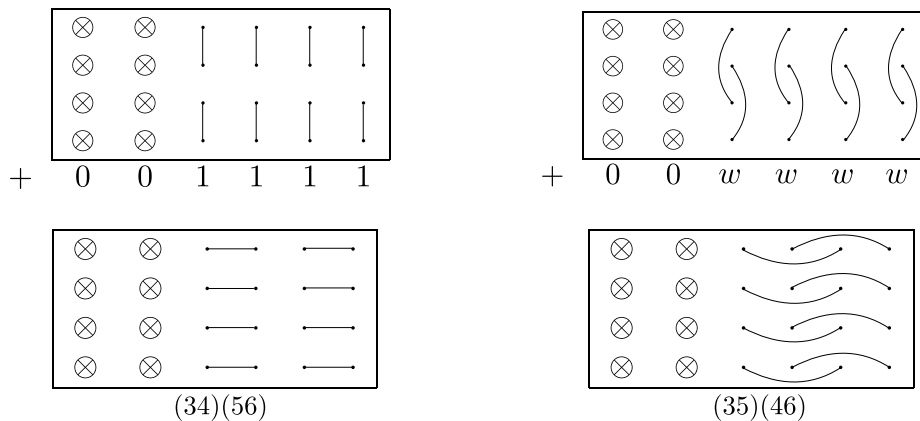
**Lema 5.1.12.** *O subgrupo de  $M_{24}$  estabilizador pontual de 5 pontos de  $\Omega$  é  $2^2 : A_4 = 2^4 : 3$ .*

*Demonstração.* Como  $M_{24}$  é 5-transitivo,  $N$  independe da escolha dos 5 pontos de  $\Omega$ . Sem perda, considere  $N$  o subgrupo de  $M_{24}$  estabilizador dos 5 pontos a seguir:



Como os elementos de  $N$  fixam os 4 primeiros pontos segue  $N \leq 2^4 : A_5$ . Além disso como  $2^4 : A_5$  age transitivamente nos 20 pontos, o índice de  $N$  é 20. Automorfismos de  $\mathcal{H}_6$  realizam todas as permutações pares das 4 colunas restantes. Soma de um hexacodeword com as 2 primeiras coordenadas iguais a 0 definem um subgrupo normal isomorfo a  $2^2$ . Assim  $2^2 : A_4 \leq N$ , como os índices são iguais temos a igualdade.

Sabemos que  $A_4 = 2^2 : 3$  donde  $N = 2^2 : (2^2 : 3)$ . Na verdade  $N$  admite um subgrupo normal isomorfo a  $2^4$  gerado pelos elementos abaixo:



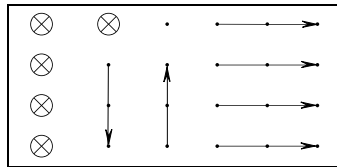
O estabilizador de um ponto que não está na segunda coluna define um subgrupo de  $N$  isomorfo a 3. Para o primeiro ponto da terceira coluna temos o automorfismo do hexacode

$$(x_1, x_2, x_3, x_4, x_5, x_6) \mapsto (x_1, wx_2, \bar{w}x_3, x_6, x_4, x_5)$$

que corresponde ao seguinte elemento de  $N$ :

Assim,  $N = 2^4 : 3$ . □

**Comentário 5.1.13.** Note que podemos calcular a ordem de  $M_{24}$  de outra maneira. Como já sabemos que  $M_{24}$  é 5-transitivo em  $\Omega$  e o estabilizador de



uma pentad (5-conjunto) é  $2^4 : 3$ , temos que o índice de  $2^4 : 3$  em  $M_{24}$  é  $24.23.22.21.20$ . Donde a ordem de  $M_{24}$  é

$$|M_{24}| = 24.23.22.21.20.16.3 = 244823040.$$

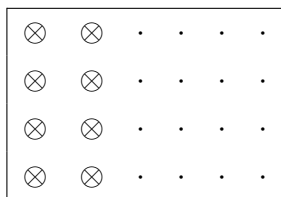
**Lema 5.1.14.** *O subgrupo de  $M_{24}$  estabilizador pontual de uma octad é o  $2^4$ .*

*Demonstração.* Chamemos de  $G < M_{24}$  o estabilizador pontual de uma octad. Como  $M_{24}$  age transitivamente em octads podemos supor que estamos falando da octad base. Assim  $G$  fixa os 5 primeiros pontos e portanto  $G \leq 2^4 : 3$ . Em  $2^4 : 3$ , o sexto ponto pode ser levado no sexto, sétimo ou oitavo ponto (e estas três possibilidades de fato ocorrem). Além disso, se o sexto ponto ficar fixo o sétimo e o oitavo também ficam. Assim, o índice de  $G$  em  $2^4 : 3$  é 3. O grupo  $G$  é isomorfo a  $2^4$ , gerado pelos 4 elementos de ordem 2 mostrados na demonstração do lema anterior.  $\square$

**Teorema 5.1.15.** *O subgrupo de  $M_{24}$  estabilizador de uma octad é o  $2^4 : A_8$ .*

*Demonstração.* Seja  $G < M_{24}$  o estabilizador da octad  $\{1, 2, 3, 4, 5, 6, 7, 8\}$ . Podemos assumir essa octad composta pelas primeiras duas colunas do MOG, isto é, a octad base. Assim,  $\pi \in G$  se e só se,  $\pi(\{1, 2, 3, 4, 5, 6, 7, 8\}) = \{1, 2, 3, 4, 5, 6, 7, 8\}$ . Como  $M_{24}$  é transitivo em octads temos  $|G| = \frac{|M_{24}|}{759} = 322560$ .

Seja  $H < G$  o estabilizador pontual da octad  $\{1, 2, 3, 4, 5, 6, 7, 8\}$ , isto é,  $\pi \in H$  se e só se  $\pi(i) = i$  para todo  $1 \leq i \leq 8$ . Assim,  $H$  fixa a octad base:

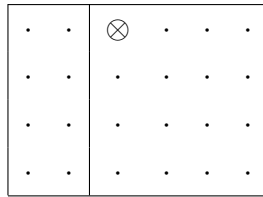


, onde  $\otimes$  são os pontos fixos pela ação do grupo.

Pelo resultado anterior  $H \cong 2^4 = (\mathbb{Z}/(2))^4$ . Portanto o índice de  $H$  em  $G$  é,  $id_G H = \frac{|G|}{|H|} = \frac{322560}{2^4} = 20160 = \frac{8!}{2}$ .

Defina o homomorfismo  $\phi : G \rightarrow S_8$  pela ação de  $G$  sobre o conjunto  $\{1, 2, 3, 4, 5, 6, 7, 8\}$ . Assim,  $Ker(\phi) = H$  e  $Im(\phi) < S_8$  com  $|Im(\phi)| = \frac{|G|}{|H|} = \frac{8!}{2}$ . Donde  $\frac{|S_8|}{|Im(\phi)|} = 2$  e portanto  $Im(\phi) \triangleleft S_8$ . Logo,  $Im(\phi) = A_8$ .

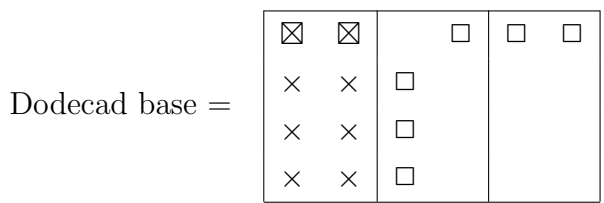
Considere  $K < G$  o estabilizador pontual de um dos 16 pontos fora da octad base, logo  $id_G K = 16$ . Digamos que  $K$  fixa o ponto 9, a saber:



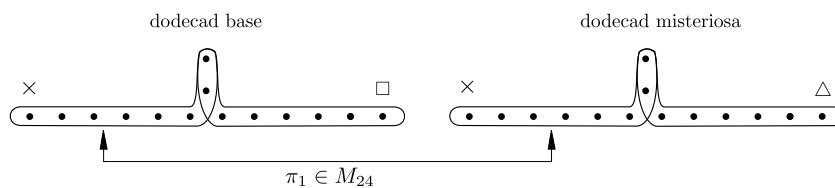
E analogamente, defina  $\varphi : K \rightarrow A_8$  pela ação de  $K$  sobre o conjunto  $\{1, 2, 3, 4, 5, 6, 7, 8\}$ . Vamos provar que  $\varphi$  é isomorfismo. Primeiramente,  $\varphi$  é sobrejetora. De fato, dada uma permutação  $\pi_1 \in A_8$ , como  $\phi|_{A_8}$  é sobrejetora, existe  $\pi \in G$  tal que  $\pi|_{\{1, \dots, 8\}} = \pi_1$ . Tome  $\sigma \in H$  com  $\sigma(9) = \pi(9)$ . Como  $(\sigma^{-1} \cdot \pi)|_{\{1, \dots, 8\}}$  e  $(\sigma^{-1} \cdot \pi)(9) = 9$  segue que  $(\sigma^{-1} \cdot \pi) \in K$ . Como  $id_{A_8} G = \frac{|G|}{|A_8|} = \frac{16 \cdot \frac{8!}{2}}{\frac{8!}{2}} = 16$  e  $id_G K = 16$  segue que  $|K| = |A_8|$ . Daí e como  $\varphi$  é sobrejetora temos  $\varphi$  injetora, logo  $K \approx A_8$ . E desde que  $H \approx 2^4 \triangleleft G$  e  $K \approx A_8 < G$  temos  $G = 2^4 : A_8$ .  $\square$

**Teorema 5.1.16.** *O grupo  $M_{24}$  age transitivamente no conjunto de pares de octads  $(\mathcal{O}_1, \mathcal{O}_2)$  com  $|\mathcal{O}_1 \cap \mathcal{O}_2| = 2$ . Em particular,  $M_{24}$  age transitivamente em dodecads.*

*Demonstração.* Tome duas dodecads no Código de Golay. Sem perda, considere uma dodecad sendo a dodecad base abaixo, onde  $\square$  e  $\times$  indicam os elementos das octads que compõem esta dodecad e  $\boxtimes$  indica os dois pontos de interseção dessas octads. A dodecad desconhecida, chamaremos de dodecad misteriosa.



Queremos provar que  $M_{24}$  é transitivo em dodecads, isto é, que existe permutação  $\pi$  em  $M_{24}$  tal que  $\pi(\text{dodecad base}) = \text{dodecad misteriosa}$ . Mais ainda, isso ocorre respeitando a decomposição dessas dodecads como soma de duas octads que se intersectam em um 2-conjunto. Como  $M_{24}$  age transitivamente em octads podemos supor que a primeira octad da dodecad misteriosa é a octad base, isto é,



Sabemos que existe permutação  $\pi_2 \in 2^4 : A_8$  que aplica os dois pontos de interseção das duas octads uns nos outros. Sem perda,

$\triangle$	$\triangle$		$\square$		$\square$	$\square$
$\times$	$\times$	$\square$				
$\times$	$\times$	$\square$				
$\times$	$\times$	$\square$				

Agora devemos completar a octad composta por  $\triangle$ . Note que o hexacodeword determinado pela octad formada por  $\triangle$  tem a forma  $00\ xx\ xx$ , tal que  $x \in \mathbb{F}_4$ . Observe também que como as primeiras duas colunas do MOG tem pontuação ímpar todas as colunas e a primeira linha do MOG deverão ter um número ímpar de  $\triangle$ . Assim, como nos restam 4 colunas e 6 pontos devemos escolher uma coluna para receber três  $\triangle$  e três colunas para receber um único  $\triangle$ . Assim, temos  $16 = 4 \cdot 4$  possibilidades para completar esta octad. Por exemplo, fazendo  $x = w$  e escolhendo a quarta coluna para receber três  $\triangle$  temos a seguinte octad:

$\triangle$	$\triangle$		$\triangle$			
			$\triangle$			
		$\triangle$		$\triangle$	$\triangle$	$x$
			$\triangle$			
0	0	$x$	$x$	$x$	$x$	

Finalmente como existe  $\rho \in 2^4 < M_{24}$  tal que  $\rho(\text{octad}_\square) = \text{octad}_\triangle$  segue que  $M_{24}$  age transitivamente no conjunto de pares de octads que se intersectam em um 2-conjunto. Particularmente temos que  $M_{24}$  é transitivo em dodecads.  $\square$

**Observação 5.1.17.** Aqui podemos observar facilmente que o número de dodecads  $D_{i,j}$  fornecido pelo triângulo das dodecads no teorema 3.0.9 independe dos  $i$  e  $j$  pontos escolhidos nos conjuntos  $A$  e  $B$ , respectivamente. Depende apenas da cardinalidade desses conjuntos. Isso deve-se ao fato de  $M_{24}$  agir transitivamente em dodecads, ser 5-transitivo nos 24 pontos de  $\Omega$ , e ser o estabilizador do  $S(5, 8, 24)$ .

**Comentário 5.1.18.** O grupo  $M_{24}$  tem vários subgrupos maximais além do  $2^6 : 3 \cdot S_6$ . Veremos a seguir alguns outros exemplos, inclusive  $M_{23}$ . O menor subgrupo maximal de  $M_{24}$  é isomorfo a  $PSL_2(7)$ , o grupo dos automorfismos do sistema de Steiner  $S(2, 3, 7)$ .

A seguir, iremos provar que o grupo  $M_{24}$  é simples. Para isso, usaremos o lema de Iwasawa (veja Lema 2.3.2), com  $H = 2^6 : 3 \cdot S_6$ ,  $\Omega_H$  o conjunto das 1771 sextets e  $A = 2^6 < H$  e usaremos também os lemas ( 5.1.19, 5.1.20 e 5.1.21).

**Lema 5.1.19.** *O grupo  $M_{24}$  age fielmente nos 1771 sextets.*

*Demonstração.* Para provarmos que  $M_{24}$  age fielmente nos 1771 sextets, devemos mostrar que se  $\pi \in M_{24}$  fixa todo sextet  $\sigma$  (isto é,  $\pi(\sigma) = \sigma$ ), então  $\pi = Id$ .

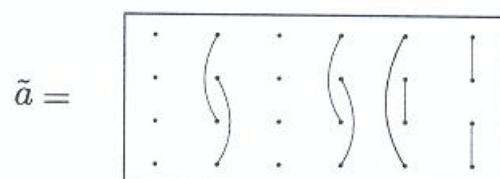
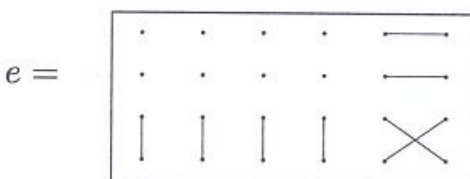
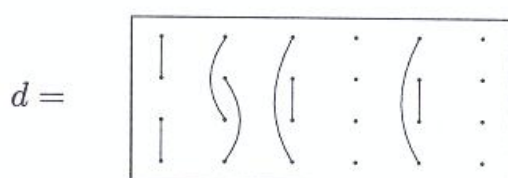
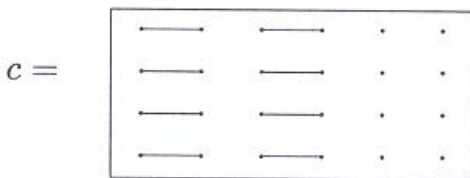
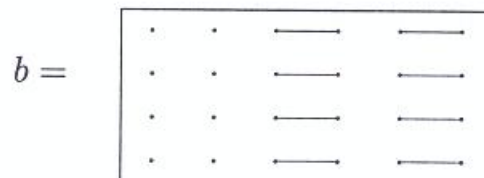
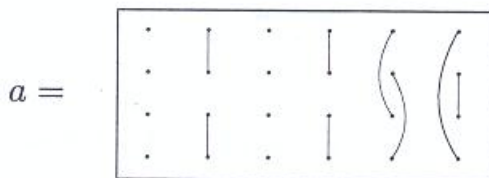
Seja  $\pi \in M_{24}$  satisfazendo a condição acima. Considerando a ação de  $\pi$  nos sextets abaixo é suficiente para concluirmos que  $\pi$  é a identidade.

1 2 3 4 5 6	1 1 1 2 5 6
1 2 3 4 5 6	1 2 2 2 4 3
1 2 3 4 5 6	3 5 6 4 3 6
1 2 3 4 5 6	4 6 5 3 5 4
1 1 1 1 3 2	1 3 4 2 1 1
4 4 4 4 2 3	1 3 4 2 3 3
5 5 5 5 2 3	6 5 5 5 4 2
6 6 6 6 2 3	5 6 6 6 2 4

□

**Lema 5.1.20.** *Elementos comutadores de  $H$  geram  $A$ .*

*Demonstração.* Para isso considere os elementos,  $a, b, c, d, e, \tilde{a}, \tilde{e}, \hat{e}$  de  $H$  abaixo.



$$\tilde{e} = \begin{array}{|c|c|c|c|c|} \hline \text{---} & \cdot & \cdot & \cdot & \cdot \\ \hline \text{---} & \cdot & \cdot & \cdot & \cdot \\ \hline \diagdown & | & | & | & | \\ \hline \end{array} \quad \hat{e} = \begin{array}{|c|c|c|c|c|} \hline \cdot & \cdot & \text{---} & \cdot & \cdot \\ \hline \cdot & \cdot & \text{---} & \cdot & \cdot \\ \hline | & | & \diagdown & | & | \\ \hline \end{array}$$

Assim temos que os comutadores  $abab$ ,  $acac$ ,  $eded$ ,  $\tilde{a}\tilde{b}\tilde{a}\tilde{b}$ ,  $\tilde{a}\tilde{c}\tilde{a}\tilde{c}$ ,  $\hat{e}\hat{d}\hat{e}\hat{d}$  geram  $A$ .

$$abab = \begin{array}{|c|c|c|c|c|} \hline \cdot & \cdot & | & | & | & | \\ \hline \cdot & \cdot & | & | & | & | \\ \hline \cdot & \cdot & | & | & | & | \\ \hline \cdot & \cdot & | & | & | & | \\ \hline \end{array} + \begin{array}{cccccc} 0 & 0 & 1 & 1 & 1 & 1 \end{array}$$

$$acac = \begin{array}{|c|c|c|c|c|c|} \hline | & | & | & | & \cdot & \cdot \\ \hline | & | & | & | & \cdot & \cdot \\ \hline | & | & | & | & \cdot & \cdot \\ \hline | & | & | & | & \cdot & \cdot \\ \hline \end{array} + \begin{array}{cccccc} 1 & 1 & 1 & 1 & 0 & 0 \end{array}$$

$$eded = \begin{array}{|c|c|c|c|c|c|} \hline \cdot & | & | & \cdot & \left( \begin{array}{c} | \\ \cdot \end{array} \right) & \left( \begin{array}{c} | \\ \cdot \end{array} \right) \\ \hline \cdot & | & | & \cdot & \left( \begin{array}{c} | \\ \cdot \end{array} \right) & \left( \begin{array}{c} | \\ \cdot \end{array} \right) \\ \hline \cdot & | & | & \cdot & \left( \begin{array}{c} | \\ \cdot \end{array} \right) & \left( \begin{array}{c} | \\ \cdot \end{array} \right) \\ \hline \cdot & | & | & \cdot & \left( \begin{array}{c} | \\ \cdot \end{array} \right) & \left( \begin{array}{c} | \\ \cdot \end{array} \right) \\ \hline \end{array} + \begin{array}{cccccc} 0 & 1 & 1 & 0 & \bar{w} & w \end{array}$$

$$\tilde{a}\tilde{b}\tilde{a}\tilde{b} = \begin{array}{|c|c|c|c|c|c|} \hline \cdot & \cdot & \left( \begin{array}{c} | \\ \cdot \end{array} \right) & \left( \begin{array}{c} | \\ \cdot \end{array} \right) & \left( \begin{array}{c} | \\ \cdot \end{array} \right) & \left( \begin{array}{c} | \\ \cdot \end{array} \right) \\ \hline \cdot & \cdot & \left( \begin{array}{c} | \\ \cdot \end{array} \right) & \left( \begin{array}{c} | \\ \cdot \end{array} \right) & \left( \begin{array}{c} | \\ \cdot \end{array} \right) & \left( \begin{array}{c} | \\ \cdot \end{array} \right) \\ \hline \cdot & \cdot & \left( \begin{array}{c} | \\ \cdot \end{array} \right) & \left( \begin{array}{c} | \\ \cdot \end{array} \right) & \left( \begin{array}{c} | \\ \cdot \end{array} \right) & \left( \begin{array}{c} | \\ \cdot \end{array} \right) \\ \hline \cdot & \cdot & \left( \begin{array}{c} | \\ \cdot \end{array} \right) & \left( \begin{array}{c} | \\ \cdot \end{array} \right) & \left( \begin{array}{c} | \\ \cdot \end{array} \right) & \left( \begin{array}{c} | \\ \cdot \end{array} \right) \\ \hline \end{array} + \begin{array}{cccccc} 0 & 0 & w & w & w & w \end{array}$$

$$\tilde{a}\tilde{c}\tilde{a}\tilde{c} = \begin{array}{|c|c|c|c|c|c|} \hline \left( \begin{array}{c} | \\ \cdot \end{array} \right) & \left( \begin{array}{c} | \\ \cdot \end{array} \right) & \left( \begin{array}{c} | \\ \cdot \end{array} \right) & \left( \begin{array}{c} | \\ \cdot \end{array} \right) & \cdot & \cdot \\ \hline \left( \begin{array}{c} | \\ \cdot \end{array} \right) & \left( \begin{array}{c} | \\ \cdot \end{array} \right) & \left( \begin{array}{c} | \\ \cdot \end{array} \right) & \left( \begin{array}{c} | \\ \cdot \end{array} \right) & \cdot & \cdot \\ \hline \left( \begin{array}{c} | \\ \cdot \end{array} \right) & \left( \begin{array}{c} | \\ \cdot \end{array} \right) & \left( \begin{array}{c} | \\ \cdot \end{array} \right) & \left( \begin{array}{c} | \\ \cdot \end{array} \right) & \cdot & \cdot \\ \hline \left( \begin{array}{c} | \\ \cdot \end{array} \right) & \left( \begin{array}{c} | \\ \cdot \end{array} \right) & \left( \begin{array}{c} | \\ \cdot \end{array} \right) & \left( \begin{array}{c} | \\ \cdot \end{array} \right) & \cdot & \cdot \\ \hline \end{array} + \begin{array}{cccccc} w & w & w & w & 0 & 0 \end{array}$$

$$\hat{e}\hat{d}\hat{e}\hat{d} = \begin{array}{|c|c|c|c|c|c|} \hline \cdot & | & \left( \begin{array}{c} | \\ \cdot \end{array} \right) & \left( \begin{array}{c} | \\ \cdot \end{array} \right) & | & \cdot \\ \hline \cdot & | & \left( \begin{array}{c} | \\ \cdot \end{array} \right) & \left( \begin{array}{c} | \\ \cdot \end{array} \right) & | & \cdot \\ \hline \cdot & | & \left( \begin{array}{c} | \\ \cdot \end{array} \right) & \left( \begin{array}{c} | \\ \cdot \end{array} \right) & | & \cdot \\ \hline \cdot & | & \left( \begin{array}{c} | \\ \cdot \end{array} \right) & \left( \begin{array}{c} | \\ \cdot \end{array} \right) & | & \cdot \\ \hline \end{array} + \begin{array}{cccccc} 0 & 1 & \bar{w} & w & 1 & 0 \end{array}$$

□

**Lema 5.1.21.** *O grupo  $H$  é gerado por conjugados de  $A$ .*

*Demonstração.* Isto segue do fato de que conjugados do elemento (5.1.5), o qual é conjugado de  $A$ , geram  $H$ .

$$\begin{array}{|c|c|c|c|c|} \hline \cdot & \cdot & \cdot & \cdot & \text{---} \\ \hline \cdot & \cdot & \cdot & \cdot & \text{---} \\ \hline | & | & | & | & \diagdown \\ \hline \end{array} \tag{5.1.5}$$

□

**Teorema 5.1.22.** *O grupo  $M_{24}$  é simples.*



*Demonstração.* Sabemos que  $M_{24}$  age transitivamente sobre os 1771 sextets e o estabilizador de um ponto de  $\Omega_H$ , por exemplo, do sextet base, é  $H = 2^6 : 3 \cdot S_6$ , subgrupo maximal de  $M_{24}$ . Daí, e pela proposição (2.3.1), segue que  $M_{24}$  age primitivamente em  $\Omega_H$ . Pelo Lema 5.1.19, temos que  $M_{24}$  age fielmente em  $\Omega_H$ . No Lema 5.1.20 vimos que elementos comutadores de  $H$  geram  $A$ . O grupo  $H$  é gerado pelos conjugados de  $A$  via  $M_{24}$  (Lema 5.1.21). Conjugados de  $A$  geram também a permutação  $\alpha$  definida em 5.1.4. Daí, e como conjugados de comutadores são ainda comutadores geramos  $M_{24}$ , donde  $M_{24}$  é perfeito. Assim, verificamos todas as hipóteses do Lema de Iwasawa donde  $M_{24}$  é simples.  $\square$

### 5.1.2

#### $M_{24}$ a partir de $PSL_2(23)$

Rotule os pontos do MOG com os pontos da linha projetiva  $\Omega = PL(23)$  como segue (veja Atlas (3)):

0	$\infty$	1	11	2	22
19	3	20	4	10	18
15	6	14	16	17	8
5	9	21	13	7	12

Com essa rotulagem do MOG e como  $PSL_2(23)$  é gerado por

$$\alpha : x \longrightarrow x + 1, \quad \beta : x \longrightarrow 2x, \quad \gamma : x \longrightarrow -x^{-1},$$

temos  $PSL_2(23)$  subgrupo de  $M_{24}$ . O grupo  $PSL_2(23)$  agindo em  $PL(23)$  pode ser estendido a  $M_{24}$  pela adjunção da aplicação  $\delta : x \longrightarrow x^3/9$  ( $x \in Q$ ) ou  $x \longrightarrow 9x^3$  ( $x \in N$ ), onde  $Q = \{0, 1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}$  e  $N = \{\infty, 5, 7, 10, 11, 14, 15, 17, 19, 20, 21, 22\}$ .

A lista dos geradores de  $M_{24}$  é:

$$\alpha = (\infty)(0 \ 1 \ 2 \ 3 \ 4 \ 5 \ 6 \ 7 \ 8 \ 9 \ 10 \ 11 \ 12 \ 13 \ 14 \ 15 \ 16 \ 17 \ 18 \ 19 \ 20 \ 21 \ 22),$$

$$\beta = (\infty)(15 \ 7 \ 14 \ 5 \ 10 \ 20 \ 17 \ 11 \ 22 \ 21 \ 19)(0)(3 \ 6 \ 12 \ 1 \ 2 \ 4 \ 8 \ 16 \ 9 \ 18 \ 13),$$

$$\gamma = (\infty \ 0)(15 \ 3)(7 \ 13)(14 \ 18)(5 \ 9)(10 \ 16)(20 \ 8)(17 \ 4)(11 \ 2)(22 \ 1)(21 \ 12)(19 \ 6),$$

$$\delta = (\infty)(14 \ 17 \ 11 \ 19 \ 22)(15)(20 \ 10 \ 7 \ 5 \ 21)(0)(18 \ 4 \ 2 \ 6 \ 1)(3)(8 \ 16 \ 13 \ 9 \ 12).$$

## 5.2

### O grupo $M_{23}$

Os Grupos de Mathieu  $M_{23}$  e  $M_{22}$  são melhores entendidos como subgrupos de  $M_{24}$ . Aqui falaremos brevemente desses grupos.

Definimos o **Grupo de Mathieu**  $M_{23}$  como o estabilizador de um ponto em  $M_{24}$ ; e este é um subgrupo maximal de  $M_{24}$ . Portanto  $M_{23}$  tem ordem

$$\frac{|M_{24}|}{24} = \frac{2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23}{2^3 \cdot 3} = 2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 23 = 10200960.$$

Como  $M_{24}$  é 5-transitivo temos que  $M_{23}$  é 4-transitivo. O grupo  $M_{23}$  pode também ser definido como o estabilizador do sistema de Steiner  $S(4, 7, 23)$  obtido através do sistema Steiner  $S(5, 8, 24)$ , deletando um dado ponto de todas as octads de  $S(5, 8, 24)$  que o contém. O número de heptads resultantes no sistema de Steiner  $S(4, 7, 23)$  é  $253 = \frac{\binom{23}{4}}{\binom{7}{4}}$ .

Similarmente, removendo uma coordenada fixada de todos os  $2^{12}$  vetores do Código de Golay obtemos o Código binário de Golay não estendido  $\mathcal{C}_{23}$  que tem a seguinte distribuição de peso

$$0^1 \ 7^{253} \ 8^{506} \ 11^{1288} \ 12^{1288} \ 15^{506} \ 16^{253} \ 23^1.$$

**Comentário 5.2.1.** Os pesos do Código de Golay não estendido podem ser facilmente entendidos em conexão com o triângulo das octads, que nos diz que dado um ponto em  $\Omega$  existem 253 octads que o contém e 506 que não o contém. Assim como existem 759 vetores de peso 8 (octads) no código de Golay, removendo uma coordenada desses vetores teremos 253 vetores de peso 7 caso o ponto removido pertença a octad e 506 vetores de peso 8 caso contrário. Pelo mesmo raciocínio e desde que um vetor de peso 16 (anti-octad) no Código de Golay é sempre o complementar de uma octad teremos em  $\mathcal{C}_{23}$  253 vetores de peso 16 caso o ponto removido não pertença a anti-octad e 506 vetores de peso 15 caso contrário (isto é, o ponto removido não pertença a octad). Como temos 2576 dodecads no Código de Golay teremos 1288 vetores de peso 11 e 1288 vetores de peso 12 caso o ponto removido esteja ou não na dodecad, respectivamente.

### 5.3

#### O grupo $M_{22}$

Definimos o **Grupo de Mathieu**  $M_{22}$  como o estabilizador de dois pontos em  $M_{24}$ . Então  $M_{22}$  tem ordem

$$\frac{|M_{23}|}{23} = \frac{2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 23}{23} = 2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 = 443520.$$

Como  $M_{23}$  é 4-transitivo segue que  $M_{22}$  é 3-transitivo. O grupo  $M_{22}$  pode ser definido como o estabilizador do sistema de Steiner  $S(3, 6, 22)$  obtido deletando dois pontos de todas as octads de  $S(5, 8, 24)$  que contém ambos os pontos. O número de hexads do sistema de Steiner  $S(3, 6, 22)$  é  $\frac{\binom{22}{3}}{\binom{6}{3}} = 77$ .

**Comentário 5.3.1.** Similarmente, o subgrupo de  $M_{24}$  estabilizador de 3 pontos tem ordem

$$\frac{|M_{22}|}{22} = \frac{2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11}{22} = 2^6 \cdot 3^2 \cdot 5 \cdot 7 = 20160,$$

e muitas vezes é chamado de  $M_{21}$ . Porém este grupo não é um grupo esporádico, pois é isomorfo a  $PSL_3(4)$ .

### 5.4

#### O grupo $M_{12}$

O **grupo de Mathieu**  $M_{12}$  é definido como o estabilizador de uma dodecad no código binário de Golay estendido, desde que  $M_{24}$  age transitivamente nas 2576 dodecads deste código (ver 5.1.16). Assim, a ordem de  $M_{12}$  é

$$\frac{|M_{24}|}{2576} = \frac{2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23}{2^4 \cdot 7 \cdot 23} = 2^6 \cdot 3^3 \cdot 5 \cdot 11 = 95040.$$

Esta definição de  $M_{12}$  não é a mesma dada originalmente por Mathieu, que construía esse grupo de maneira independente de  $M_{24}$ . O fato de  $M_{12}$  ser um subgrupo de  $M_{24}$  foi primeiro descoberto por Frobenius. Note que o subgrupo  $M_{12}$  não é maximal em  $M_{24}$ . De fato, como o complemento de uma dodecad é também uma dodecad e  $M_{24}$  age transitivamente em dodecads, temos um subgrupo  $M_{12} : 2$  que fixa pares de dodecads complementares. O subgrupo  $M_{12} : 2$  é maximal em  $M_{24}$ , porém não é simples.

Vimos pela última linha do triângulo das dodecads que em  $\mathcal{C}_{24}$  uma octad pode intersectar uma dodecad em 2, 4 ou 6 de seus pontos. Fixada uma dodecad há  $132 = \frac{\binom{12}{5}}{6}$  octads a intersectando em 6 pontos, por completamento, há 132 intersectando em 2 pontos e desde que um tetrad determina um único sextet temos  $495 = \binom{12}{4}$  intersectando em 4 pontos (ver figuras 5.1 e 5.2). As interseções de tamanho 6 formam um conjunto com 132 blocos chamados **hexads**. Como cada hexad está contida em uma única octad esse conjunto tem

a propriedade (herdada de  $S(5, 8, 24)$ ) que qualquer 5-conjunto determina um único bloco. Assim,  $M_{12}$  pode ser definido como o estabilizador do  $S(5, 6, 12)$  sistema de Steiner.

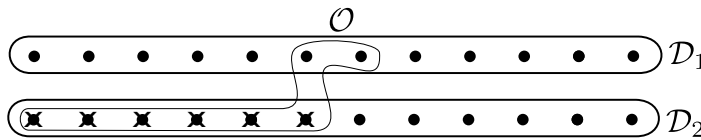


Figura 5.1: Dodecad intersectando uma octad em 2 ou 6 pontos.

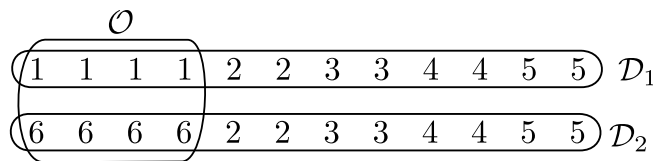


Figura 5.2: Dodecad intersectando uma octad em 4 pontos.

Considere  $h = \{h_1, h_2, h_3, h_4, h_5, h_6\}$  uma hexad e  $A$  um  $k$ -conjunto contido em  $h$ . Pela definição do  $S(5, 6, 12)$  sistema de Steiner temos que o número de hexads contendo  $A$  é dado por  $\frac{\binom{12-k}{5-k}}{\binom{6-k}{5-k}}$ , se  $k \in \{1, \dots, 4\}$  e é 1 se  $k \in \{5, 6\}$ . Portanto o número de hexads contendo um  $k$ -conjunto é 132, 66, 30, 12, 4, 1, 1 para  $k = 0, \dots, 6$ , respectivamente. Consequentemente, o número de hexads que não contém um ponto é  $132 - 66 = 66$ , e assim por diante. Assim, de maneira análoga à construção do triângulo das octads construímos o triângulo das hexads. Considere  $h$  uma hexad tal que  $B$  é um  $i$ -conjunto e  $A$  um  $j$ -conjunto com  $A \subseteq B \subseteq h$ . Então, o número de hexads que contém os elementos de  $A$  e não contém os elementos de  $B \setminus A$  é dado pela  $(j + 1)$ -ésima entrada da  $(i + 1)$ -ésima linha da tabela abaixo:

				132					
				66		66			
			30		36		30		
		12		18		18		12	
		4	8		10		8		4
	1	3		5		5		3	1
1	0	3		2		3		0	1

Figura 5.3: Triângulo das hexads.

Pela última linha do triângulo das hexads vemos que existem 1, 3, 2, e 3 hexads intersectando uma hexad dada em 0, 2, 3 ou 4 pontos, respectivamente. Em particular, o complemento de uma hexad é sempre uma outra hexad.

**Lema 5.4.1.** *O estabilizador pontual de um hexad em  $M_{12}$  é o grupo trivial.*

*Demonstração.* Tome uma hexad contida em uma dodecad. Certamente essa hexad está contida em uma octad e a soma (diferença simétrica) desses não está contida na dodecad. O estabilizador pontual da hexad fixa toda a octad que contém essa hexad. De fato, inicialmente os dois pontos da octad que não pertencem a hexad poderiam ser permutados. Mas isso não ocorre, desde que o grupo estabilizador de uma octad é  $2^4 : A_8$ , isto é, só permutações pares são realizadas dentro da octad fixada.

Daí, e como o estabilizador pontual da octad é o  $2^4$  e  $M_{12}$ , por definição, fixa a dodecad segue que o grupo estabilizador da hexad é o trivial.  $\square$

**Teorema 5.4.2.**  $|M_{12}| = 132|S_6|$ ,  $M_{12}$  é transitivo em hexads e o estabilizador como conjunto de um hexad é  $S_6$  agindo naturalmente nos 6 pontos do hexad. Portanto,  $M_{12}$  é 5-transitivo em 12 pontos.

*Demonstração.* Já sabemos que  $|M_{12}| = 95040$  e que, por definição, as 132 hexads do sistema de Steiner  $S(5, 6, 12)$  são preservadas por  $M_{12}$ .

Fixe uma hexad, chamaremos esta de hexad base. Considere a órbita da hexad base, e denotemos esta por  $G_{hexad\ base} = \{\pi(hexad\ base); \pi \in M_{12}\}$ . Assim,  $|G_{hexad\ base}| = n \leq 132 = 2^3 \cdot 3 \cdot 11$ .

Chamemos de  $G$  o estabilizador como conjunto da hexad base. Em outras palavras,  $G < M_{12}$  tal que  $\pi \in G$  se e só se  $\pi(hexad\ base) = hexad\ base$ . Portanto,  $|G| = \frac{|M_{12}|}{n} \geq \frac{2^6 \cdot 3 \cdot 5 \cdot 11}{2^2 \cdot 3 \cdot 11} = 2^4 \cdot 3^2 \cdot 5 = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 = 6!$ .  $G$  age sobre os 6 pontos da hexad base logo  $G$  realiza  $m \leq 6!$  permutações. Chamemos de  $H$  o estabilizador pontual da hexad base, isto é,  $H \leq G$  tal que  $\pi \in H$  se e só se  $\pi|_{hexad\ base} = Id$ . Donde  $|H| = \frac{|G|}{m} \geq \frac{6!}{6!} = 1$ . Mas pelo lema anterior o estabilizador pontual de um hexad em  $M_{12}$  é o grupo trivial. Donde  $|H| = 1$  e todas as desigualdades acima são igualdades. Portanto,  $m = 6!, n = 132$ ,  $G = S_6$  e  $|M_{12}| = 132|S_6|$ . E desde que um 5-conjunto determina uma única hexad e  $|M_{12}|$  é transitivo em hexads segue  $M_{12}$  é 5-transitivo em um 12-conjunto.  $\square$

### 5.4.1

#### O $M_{12}$ , o MINIMOG e o $S(5, 6, 12)$

O grupo de Mathieu  $M_{12}$  é ao mesmo tempo um subgrupo de  $M_{24}$  e um análogo dele. Aqui veremos algumas dessas semelhanças.

Os blocos do  $S(5, 6, 12)$  sistema de Steiner não geram um código binário no mesmo caminho dos blocos de  $S(5, 8, 24)$ , pois duas hexads podem se intersectar em 0, 2, 3 ou 4 pontos. Mas colocando sinais nos pontos das hexads conseguimos um código ternário, o  $C_{12}[12, 6, 6]$  (ver seção 2.9). O  $S(5, 6, 12)$

sistema de Steiner também é único a menos de isomorfismo. O grupo  $M_{12}$ , que pode ser definido como o estabilizador do  $S(5, 6, 12)$  sistema de Steiner, é melhor entendido em conexão com o código ternário de Golay. Nos iremos aqui definir o  $C_{12}$  em termos do tetracode e do MINIMOG.

O Tetracode,  $\mathcal{C}_4[4, 2, 3]$ , é um subespaço vetorial de  $\mathbb{F}_3^4$  de dimensão 2 e consiste das seguintes palavras, que chamaremos de **tetracodewords**:

$$\begin{array}{lll} 0\ 000 & 0\ +\ +\ + & 0\ -\ -\ - \\ +\ 0\ +\ - & +\ +\ -\ 0 & -\ -\ +\ 0 \\ -\ 0\ -\ + & -\ +\ 0\ - & -\ -\ +\ 0. \end{array}$$

Para cada função  $\phi(x) = ax + b$  sobre  $\mathbb{F}_3$  definimos uma palavra  $a\ bcd$  em  $\mathcal{C}_4$ , onde  $(a, b)$  especificam a função  $\phi$  e  $(b, c, d)$  são obtidos avaliando a função  $\phi$  respectivamente em  $0, +, -$ :

$$a, b = \phi(0), c = \phi(+), d = \phi(-).$$

Isto torna fácil resolver dois tipos de problemas:

1. **O 2-problema:** completar um tetracodeword a partir de 2 de seus pontos.
2. **O 4-problema:** corrigir um tetracodeword dados todos os seus 4 pontos (algum dígito pode estar errado).

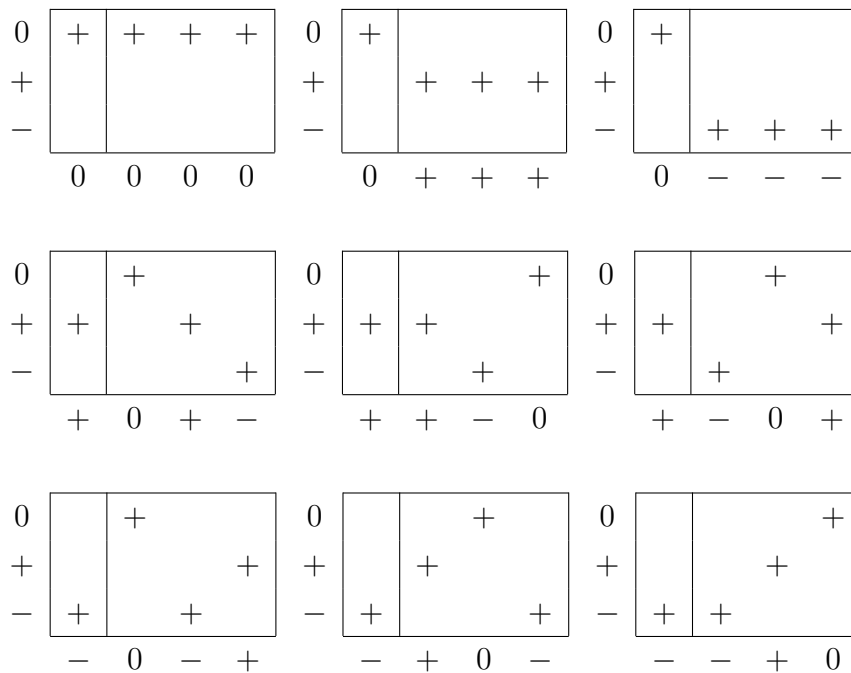
O **MINIMOG** é uma matriz  $3 \times 4$  cujas linhas são rotuladas pelos elementos  $0, +, -$  de  $\mathbb{F}_3$  e cujas colunas correspondem aos 4 dígitos do tetracodeword. Muitas vezes, em cima de cada coluna colocamos sua pontuação, isto é, o seu número de dígitos não nulos. Nós usaremos a palavra *coluna*, abreviadamente 'col', para as palavras de comprimento 12 com dígitos  $+$  em todas as entradas de uma coluna e dígitos  $0$  nos outros lugares. E usaremos a palavra *tetrad*, abreviadamente 'tet', para as palavras de comprimento 4 com dígitos  $+$  nas entradas correspondentes ao tetracodeword e dígitos  $0$  nos outros lugares.

Vamos listar todos os cols e todos os tets:

cols:

$$\begin{array}{cccc} 0 & \begin{array}{|c|c|} \hline + & \\ \hline + & \\ \hline - & + \\ \hline \end{array} & 0 & \begin{array}{|c|c|} \hline & + \\ \hline + & + \\ \hline - & + \\ \hline \end{array} & 0 & \begin{array}{|c|c|} \hline & + \\ \hline + & + \\ \hline - & + \\ \hline \end{array} & 0 & \begin{array}{|c|c|} \hline & + \\ \hline + & + \\ \hline - & + \\ \hline \end{array} \end{array}$$

tets:



O código  $\mathcal{C}_{12}[12, 6, 6]$  é um subespaço vetorial de  $\mathbb{F}_3^{12}$  de dimensão 6. Em termos de cols e tets  $\mathcal{C}_{12}$  é gerado por:

$$\text{col-col, tet-tet, col+tet.}$$

Em particular, isso nos diz que a combinações

$$\text{col-col, tet-tet, col+tet, col+col-tet}$$

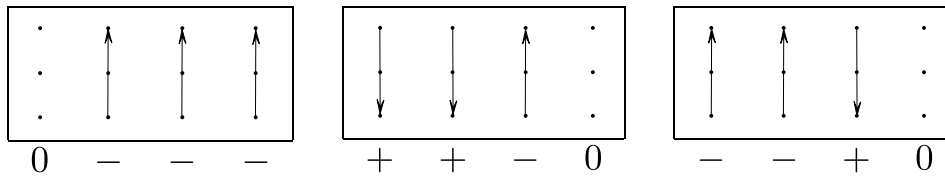
funcionam como palavras em  $\mathcal{C}_{12}$  de peso 6 denominadas **hexads com sinal**.

**Exemplo 31.** Abaixo temos um exemplo de hexad com sinal em  $\mathcal{C}_{12}$  obtido a partir de col+col-tet:

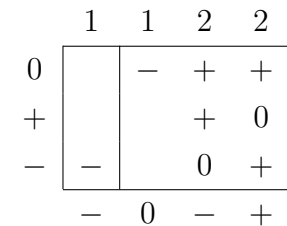
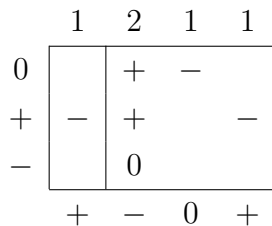
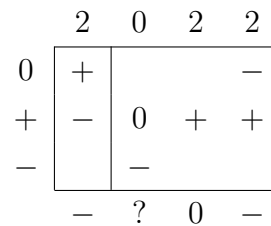
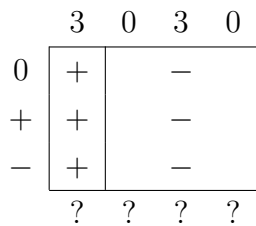
$$\begin{array}{|c|c|c|c|} \hline & + & & \\ \hline & + & & \\ \hline & + & & \\ \hline \end{array} + \begin{array}{|c|c|c|c|} \hline & + & & \\ \hline & + & & \\ \hline & + & & \\ \hline \end{array} - \begin{array}{|c|c|c|c|} \hline & & & + \\ \hline + & + & & \\ \hline & & + & \\ \hline \end{array}$$

$$= \begin{array}{|c|c|c|c|} \hline & + & + & - \\ \hline - & 0 & + & \\ \hline & + & 0 & \\ \hline \end{array} = (0, -, 0, +, 0, +, +, +, 0, -, 0, 0) \in \mathcal{C}_{12}.$$

**Comentário 5.4.3.** O tetracode age nos 12 pontos do MINIMOG por adição, donde temos uma inclusão natural  $\mathcal{C}_4 = 3^2 \subset M_{12}$ . Abaixo temos a ação das palavras 0 ---, + + -0 e - - +0 no MINIMOG:



Para cada codeword em  $\mathcal{C}_{12}$  de peso 6 podemos definir, para cada coluna da matriz MINIMOG, o seu **odd-men-out**. Para cada coluna o odd-men-out será a linha correspondente ao único dígito não nulo ou ao único dígito nulo naquela coluna. Caso para alguma coluna o odd-men-out não exista, escrevemos ? abaixo dela.



Se nós ignorarmos os sinais dos 264 hexads com sinal existentes em  $\mathcal{C}_{12}$  obtemos os 132 hexads de  $S(5,6,12)$ . Assim os hexads de  $S(5,6,12)$  podem ser descritos como:

1. O conjunto de seis pontos cuja distribuição coluna não é 3 210, e
2. o odd-men-out faz parte de um tetracodeword.

Dessa maneira, o problema de completar um hexad conhecendo 5 de seus pontos pode ser resolvido a partir do 2-problema ou 4-problema desde que um tetracodeword é sempre determinado por quaisquer duas de suas coordenadas e o odd-men-out sempre determina um único tetracodeword e então colocando os sinais usando expressões em termos de colunas e tetrads obtemos o hexad com sinal desejado.

Nos próximos exemplos veremos como determinar hexads em  $S(5,6,12)$  a partir de 5 de seus pontos, prosseguiremos usando expressões de cols e tets a fim de determinarmos hexads com sinal em  $\mathcal{C}_{12}[12,6,6]$ .



**Exemplo 32.**

0		*	*	*
+			*	
-		*		
	?	+	-	0

Acima temos um conjunto de 5 pontos (pentad) de  $S(5, 6, 12)$  e os odd-men-out. Logo,  $\phi(x) = ax+1$  e portanto  $\phi(+)=a+1=-1 \Rightarrow a=1$  e  $\phi(x)=x+1$ ,  $\phi(-1)=0$ .

Donde determinamos o tetracodeword e todos os odd-men-out, obtendo assim uma hexad do  $S(5, 6, 12)$  :

0		*	*	*
+	*		*	
-		*		
	+	+	-	0

$\in S(5, 6, 12)$

Agora usando as expressões de cols e tets podemos terminar os sinais. Como o hexad tem a distribuição coluna  $(2^2 1^2)$  isso nos diz que ele foi obtido a partir de col+col-tet e conseqüentemente obtemos o hexad com sinal de  $\mathcal{C}_{12}$  :

<table border="1" style="border-collapse: collapse;"> <tr><td></td><td>+</td></tr> <tr><td></td><td>+</td></tr> <tr><td></td><td>+</td></tr> </table>		+		+		+	+	<table border="1" style="border-collapse: collapse;"> <tr><td></td><td>+</td></tr> <tr><td></td><td>+</td></tr> <tr><td></td><td>+</td></tr> </table>		+		+		+	-	<table border="1" style="border-collapse: collapse;"> <tr><td>+</td><td></td><td></td><td>+</td></tr> <tr><td></td><td>+</td><td></td><td></td></tr> <tr><td></td><td></td><td>+</td><td></td></tr> </table>	+			+		+					+	
	+																											
	+																											
	+																											
	+																											
	+																											
	+																											
+			+																									
	+																											
		+																										
$= \begin{matrix} & & 1 & 2 & 2 & 1 \\ 0 & & & + & + & - \\ + & - & & 0 & + & \\ - & & & + & 0 & \end{matrix} \in \mathcal{C}_{12}$																												
$\begin{matrix} & & + & + & - \\ & & + & + & 0 \\ & & + & 0 & \end{matrix}$																												
$\begin{matrix} & & + & + & - \\ & & + & + & 0 \\ & & + & 0 & \end{matrix}$																												

**Exemplo 33.**

0	*	*		
+	*			
-	*	*		
	?	?	?	?

Como a distribuição 3 210 é proibida devemos completar o hexad colocando a \* que falta na segunda coluna:

$$\begin{array}{c}
 0 \\
 + \\
 - \\
 ? \quad ? \quad ? \quad ?
 \end{array}
 \begin{array}{|c|c|}
 \hline
 * & * \\
 \hline
 * & * \\
 \hline
 * & * \\
 \hline
 \end{array}
 \in S(5, 6, 12)$$

Obtendo assim a distribuição  $3^2 0^2$ , o que nos diz que o hexad foi obtido a partir de col-col. Donde,

$$\begin{array}{|c|c|}
 \hline
 + \\
 \hline
 + \\
 \hline
 + \\
 \hline
 \end{array}
 -
 \begin{array}{|c|c|}
 \hline
 + \\
 \hline
 + \\
 \hline
 + \\
 \hline
 \end{array}
 =
 \begin{array}{c}
 3 \quad 3 \quad 0 \quad 0 \\
 0 \\
 + \\
 - \\
 ? \quad ? \quad ? \quad ?
 \end{array}
 \begin{array}{|c|c|}
 \hline
 + & - \\
 \hline
 + & - \\
 \hline
 + & - \\
 \hline
 \end{array}
 \in \mathcal{C}_{12}$$

**Exemplo 34.**

$$\begin{array}{c}
 0 \\
 + \\
 - \\
 0 \quad ? \quad ? \quad 0
 \end{array}
 \begin{array}{|c|c|}
 \hline
 * & * \\
 \hline
 * & * \\
 \hline
 \end{array}$$

Novamente, como a distribuição  $3 \ 2 \ 1 \ 0$  é proibida podemos alterar apenas a segunda e a terceira coluna. Como  $a = 0$  e  $d = 0$  o tetracodeword é  $0 \ 000$ , logo:

$$\begin{array}{c}
 0 \\
 + \\
 - \\
 0 \quad 0 \quad 0 \quad 0
 \end{array}
 \begin{array}{|c|c|c|c|}
 \hline
 * & * & * \\
 \hline
 * & * & * \\
 \hline
 \end{array}
 \in S(5, 6, 12)$$

Como a distribuição é  $2^3 0^1$ , temos que o hexad foi obtido a partir de tet-tet. E portanto completamos o seguinte hexad com sinal:

$$\begin{array}{|c|c|c|}
 \hline
 + \\
 \hline
 + \\
 \hline
 \end{array}
 -
 \begin{array}{|c|c|c|}
 \hline
 + \\
 \hline
 + \\
 \hline
 + \\
 \hline
 \end{array}
 =
 \begin{array}{c}
 2 \quad 0 \quad 2 \quad 2 \\
 0 \\
 - \\
 + \\
 0 \quad 0 \quad 0 \quad 0
 \end{array}
 \begin{array}{|c|c|c|}
 \hline
 0 \\
 \hline
 - & - & + \\
 \hline
 + & + & - \\
 \hline
 \end{array}
 \in \mathcal{C}_{12}$$

**Exemplo 35.**

$$\begin{array}{c}
 0 \\
 + \\
 - \\
 - \quad ? \quad ? \quad +
 \end{array}
 \begin{array}{|c|c|c|}
 \hline
 * & * \\
 \hline
 * & * \\
 \hline
 * & * \\
 \hline
 \end{array}$$

Analogamente ao exemplo anterior, podemos alterar apenas a segunda e a terceira coluna. Como  $\phi(x) = -x + b$  e  $\phi(-) = 1 + b = 1$ , temos  $b = 0$ . Donde  $\phi(x) = -x$ ,  $\phi(0) = 0$ ,  $\phi(+)$  e  $\phi(-)$  são  $-1$  e  $0$ . Logo completamos o hexad de  $S(5, 6, 12)$  abaixo:

$$\begin{array}{c} 0 \\ + \\ - \end{array} \begin{array}{|c|c|c|} \hline * & & * \\ \hline * & * & \\ \hline * & * & * \\ \hline \end{array} \in S(5, 6, 12)$$

- 0 - 0

Colocando os sinais, obtemos o hexad com sinal de  $\mathcal{C}_{12}$ :

$$\begin{array}{|c|c|c|} \hline & & + \\ \hline + & + & \\ \hline & & + \\ \hline \end{array} - \begin{array}{|c|c|c|} \hline + & & \\ \hline & + & + \\ \hline & + & + \\ \hline \end{array} = \begin{array}{c} 2 \quad 2 \quad 0 \quad 2 \\ \begin{array}{|c|c|c|} \hline - & & + \\ \hline + & + & \\ \hline & - & 0 \\ \hline - & 0 & - \\ \hline \end{array} \in \mathcal{C}_{12}$$

**Exemplo 36.**

$$\begin{array}{c} 0 \\ + \\ - \end{array} \begin{array}{|c|c|c|} \hline & & * \\ \hline & * & * \\ \hline & * & * \\ \hline \end{array}$$

? 0 - ?

Temos 2 dígitos corretos do tetracodeword, logo:  $\phi(x) = ax + 0$  e  $\phi(+)$  e  $\phi(-)$  são  $a$  e  $-1$   $\Rightarrow \phi(x) = -x$ ,  $\phi(-) = -$ . Donde completamos o tetracodeword e descobrimos o odd-men-out:

$$\begin{array}{c} 0 \\ + \\ - \end{array} \begin{array}{|c|c|c|} \hline & & * \\ \hline & * & * \\ \hline * & * & \\ \hline \end{array} \in S(5, 6, 12)$$

- 0 - +

Como a distribuição coluna é  $2^2 1^2$  devemos ter col+col-tet. Colocando os sinais, temos:

$$\begin{array}{|c|c|} \hline + \\ \hline + \\ \hline + \\ \hline \end{array} + \begin{array}{|c|c|} \hline + \\ \hline + \\ \hline + \\ \hline \end{array} - \begin{array}{|c|c|} \hline + & \\ \hline & + \\ \hline + & + \\ \hline \end{array}$$



## 5.5

### O Grupo $M_{11}$

Definimos o **grupo de Mathieu**  $M_{11}$  como o estabilizador de um ponto em  $M_{12}$ . Donde temos

$$\frac{|M_{12}|}{12} = \frac{2^6 \cdot 3^3 \cdot 5 \cdot 11}{12} = 2^4 \cdot 3^2 \cdot 5 \cdot 11 = 7920.$$

Como  $M_{12}$  é 5-transitivo temos que  $M_{11}$  é 4-transitivo em um conjunto de 11 pontos. O grupo  $M_{11}$  pode ser definido como o estabilizador do sistema de Steiner  $S(4, 5, 11)$ . O número de pentads do sistema de Steiner  $S(4, 5, 11)$  é  $\frac{\binom{11}{4}}{\binom{5}{4}} = 66$ . O grupo  $M_{11}$  é o menor grupo de Mathieu.