3
Sistema de Steiner e Código de Golay

Considere o sistema de Steiner $S(5, 8, 24)$, chamaremos os seus blocos de **octads**. Assim, as octads são subconjuntos de 8 elementos de um conjunto Ω com 24 elementos tal que qualquer subconjunto com 5 elementos determina uma única octad. Donde, há $\frac{\binom{24}{5}}{\binom{8}{5}} = 759$ octads.

O sistema de Steiner $S(5, 8, 24)$ é um objeto muito especial. O seu grupo de simetrias é o grupo esporádico M_{24}. Neste capítulo falaremos de algumas propriedades do sistema de Steiner $S(5, 8, 24)$, do Código de Golay e como esses objetos se relacionam. E por fim, provaremos que o sistema de Steiner $S(5, 8, 24)$ é único a menos de isomorfismo.

Lema 3.0.1. *Seja $A \subseteq \Omega$ e denote por N_A o número de octads contendo A. Então,*

$$\begin{cases} N_A = \frac{\binom{24-k}{5-k}}{\binom{8-k}{5-k}}, & se \quad k < 5 \\ N_A = 0 \quad ou \quad 1, & se \quad k \geq 5 \end{cases}$$

Demonstração. Seja A um k-conjunto. Queremos determinar o número, N_A, de pares $(A, \mathcal{O})$ onde $\mathcal{O}$ é uma octad contendo A.

Se $k \geq 5$ como temos um sistema de Steiner $S(5, 8, 24)$, por definição, temos que $N_A = 1$.

Se $k < 5$, há $\binom{24-k}{5-k}$ maneiras de completar A a um 5-conjunto (que já sabemos que está contido em uma única octad). Mas observe que estaríamos completando o mesmo k-conjunto a um 5-conjunto dentro desta octad $\binom{8-k}{5-k}$ repetidas vezes. Donde $N_A = \frac{\binom{24-k}{5-k}}{\binom{8-k}{5-k}}$.

□

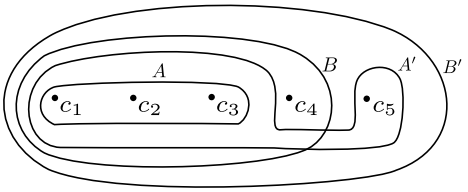
Observação 3.0.2. Observe que se $\mathcal{O} = \{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8\}$ é uma octad e A é um k-conjunto contido em $\mathcal{O}$ então, pelo lema anterior, o número de octads contendo A é 759, 253, 77, 21, 5, 1, 1, 1, 1 para $k = 0, ..., 8$, respectivamente.

Sejam $A \subseteq B \subseteq \Omega$. Chamaremos de $N_{B,A}$ o número de octads que intersectam B em A exatamente, isto é, o número de octads que obrigatoriamente contém os elementos de A e não contém os elementos de B\A.

PUC-Rio - Certificação Digital Nº 1012850/CA

Lema 3.0.3. *Considere $A \subseteq B \subseteq \Omega$ e x um ponto qualquer de $\Omega \backslash B$. Defina $B' := B \bigsqcup \{x\}$ e $A' := A \bigsqcup \{x\}$, então $N_{B,A} = N_{B',A} + N_{B,A'}$.*

Demonstração. Um desenho prova essa afirmação. Sem perda de generalidade,



$N_{B,A} = \#\{\mathcal{O} \mid c_1, c_2, c_3 \in \mathcal{O}, c_4 \notin \mathcal{O}\} = \#\{\mathcal{O} \mid c_1, c_2, c_3, c_5 \in \mathcal{O}, c_4 \notin \mathcal{O}\} + \#\{\mathcal{O} \mid c_1, c_2, c_3 \in \mathcal{O}, c_4, c_5 \notin \mathcal{O}\} = N_{B',A'} + N_{B',A}$. □

Lema 3.0.4. *Sejam $A \subseteq B \subseteq \Omega$. Então* $N_{B,A} = \sum_{A \subseteq S \subseteq B} (-1)^{|S \backslash A|} N_S$.

Demonstração. Como antes, $N_S = \#\{\mathcal{O} \mid S \subseteq \mathcal{O}\}$. Queremos provar que $N_{B,A} = \sum_{A \subseteq S \subseteq B} (-1)^{|S \backslash A|} N_S$, faremos a prova por indução em $|B - A|$ e usaremos o Príncipio da união e interseção.

Se $A = B \rightarrow N_{B,A} = N_{A,A} = N_A = \sum_{A \subseteq S \subseteq B} (-1)^{|S \backslash A|} N_S$.

Se $B = A \sqcup \{x\} \rightarrow N_{B,A} = N_A - N_B = \sum_{A \subseteq S \subseteq B} (-1)^{|S \backslash A|} N_S$.

Se $B = A \sqcup \{x_1, x_2\} \rightarrow N_{B,A} = N_A - N_{A \sqcup \{x_1\}} - N_{A \sqcup \{x_2\}} + N_{A \sqcup \{x_1, x_2\}} = \sum_{A \subseteq S \subseteq B} (-1)^{|S \backslash A|} N_S$

Se $B = A \sqcup \{x_1, x_2, x_3\} \rightarrow N_{B,A} = N_A - N_{A \sqcup \{x_1\}} - N_{A \sqcup \{x_2\}} - N_{A \sqcup \{x_3\}} + N_{A \sqcup \{x_1, x_2\}} + N_{A \sqcup \{x_1, x_3\}} + N_{A \sqcup \{x_2, x_3\}} - N_{A \sqcup \{x_1, x_2, x_3\}} = \sum_{A \subseteq S \subseteq B} (-1)^{|S \backslash A|} N_S$ continuando o processo obtemos o resultado desejado. □

Teorema 3.0.5. *Sejam $\mathcal{O}$ uma octad, B um i-conjunto e A um j-conjunto com $A \subseteq B \subseteq \mathcal{O}$. Então $N_{B,A}$ é dado pela $(j+1)$-ésima entrada da $(i+1)$-ésima linha da tabela a seguir, chamada de triângulo das octads.*

												759												
										506				253										
								330				176				77								
						210				120				56				21						
					130			80				40				16				5				
				78			52			28				12				4				1		
			46			32			20			8				4			0			1		
		30			16			16			4			4			0			0			1	
	30			0			16			0			4			0			0			0		1

Figura 3.1: Triângulo das octads

PUC-Rio - Certificação Digital Nº 1012850/CA

Demonstração. Pela observação 1, temos que os valores de N_A, para $0 \leq j \leq 8$, são 759, 253, 77, 21, 5, 1, 1, 1, 1. Note que os valores de N_A ocupam o lado direito do triângulo das octads. Portanto, fixado um ponto em uma octad, o número de octads que não o contém é $759 - 253 = 506$; e assim por diante. Daí, e pelos lemas 3.0.3 e 3.0.4 completamos o triângulo das octads. □

Pela última linha do triângulo das octads podemos observar que 2 octads distintas podem apenas se intersectar em 0, 2 ou 4 pontos. Assim teremos subconjuntos de $P\Omega$ com 16, 12 ou 8 pontos, respectivamente.

Considere $\mathcal{G}$ o subespaço vetorial de $\mathbb{F}_2^{24}$ gerado pelas 759 octads do $S(5, 8, 24)$.

Lema 3.0.6. *O subespaço $\mathcal{G}$ de $P\Omega$ é totalmente singular e portanto tem dimensão no máximo 12.*

Demonstração. Sejam $\mathcal{O}_1$, $\mathcal{O}_2$ duas octads em $S(5, 8, 24)$. Pela última linha do triângulo das octads temos que $|\mathcal{O}_1 \cap \mathcal{O}_2| = 0, 2$ ou 4 pontos. Considere a forma bilinear

$$\begin{array}{rcl} B : \mathbb{F}_2^{24} & \longrightarrow & \mathbb{F}_2^{24} \\ (v_1, v_2) & \longmapsto & \langle v_1, v_2 \rangle \end{array}$$

Para todo v_1 e v_2 em $\mathcal{G}$, vetores associados a $\mathcal{O}_1$, $\mathcal{O}_2$ temos $B(v_1, v_2) = 0$. Donde $\mathcal{G}$ é totalmente singular e pela proposição 2.8.1 segue que $dim(\mathcal{G}) \leqslant \frac{24}{2} = 12$. □

Chamaremos de **dodecad** um 12-conjunto em $\mathcal{G}$ e de **antioctad** um 16-conjunto.

Lema 3.0.7. *Dodecads existem; desde que há pelo menos 2576 dodecads que podem ser escritas como soma de 2 octads que se intersectam em um 2-conjunto.*

Demonstração. Pelo triângulo das octads sabemos que $N_{8,2} = 16$, isto é, fixada uma octad e 2 pontos nela existem 16 outras octads que a intersectam neste 2-conjunto. Portanto dodecads existem desde que $\mathcal{D} = \mathcal{O} + \mathcal{O}'$ é uma, onde $\mathcal{O}$ e $\mathcal{O}'$ são octads que se intersectam em um 2-conjunto.

Denotemos por $\mathcal{A}$ o conjunto das dodecads que podem ser expressas como soma de 2 octads que se intersectam em um 2-conjunto e por $\mathcal{B}$ os pares ordenadas de octads que se intersectam em um 2-conjunto. Há uma bijeção natural,

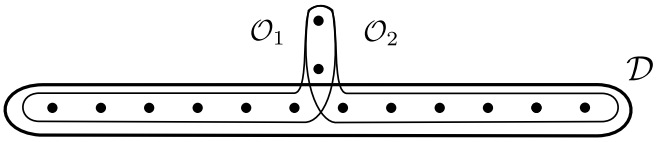
$$f : \mathcal{B} \to \mathcal{A}, (\mathcal{O}, \mathcal{O}') \mapsto \mathcal{O} + \mathcal{O}'.$$

PUC-Rio - Certificação Digital Nº 1012850/CA

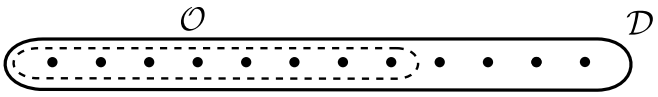
Fixe $\mathcal{O}$ uma octad. Defina $\mathcal{B}_{\mathcal{O}} = \{(\mathcal{O}_1, \mathcal{O}_2) \in \mathcal{B} \mid \mathcal{O}_1 = \mathcal{O}\}$. Então, $\mathcal{B}_{\mathcal{O}}$ tem $16.\binom{8}{2}$ elementos e portanto $\mathcal{B}$ tem $|S|.|\mathcal{B}_{\mathcal{O}}| = 759.\binom{8}{2}.16 = 340032$ elementos.

Agora tome $\mathcal{D} \in \mathcal{A}$ e considere o conjunto das expressões $\mathcal{O}_1 + \mathcal{O}_2 = \mathcal{D}$. Note que cada expressão determina um 6-conjunto em $\mathcal{D}$, $\mathcal{D} \cap \mathcal{O}_1$, que está contido em uma octad. Assim temos 2 possibilidades:

1) o 6-conjunto é completo a uma octad por um 2-conjunto que não pertence a docecad.



2) a octad que contém o 6-conjunto está inteiramente contida na dodecad. Seja n o número de octads contidas em $\mathcal{D}$ (no teorema 3.0.8 veremos que $n = 0$).



Na primeira situação há $\frac{\binom{12}{5}}{\binom{6}{5}}$ maneiras de determinar $\mathcal{O}_1$, e na segunda $n.\frac{\binom{8}{5}}{\binom{6}{5}}$. Donde,

$$|f^{-1}(\mathcal{D})| = \frac{\binom{12}{5} - n.\binom{8}{5}}{6} \leq 132.$$

Portanto,

$$|\mathcal{A}| = \frac{|\mathcal{B}|}{|f^{-1}(\mathcal{D})|} = \frac{340032}{132} \geq 2576.$$

□

Teorema 3.0.8. *O espaço vetorial $\mathcal{G}$ é 12 dimensional e tem a seguinte distribuição de peso:*

peso	*número de vetores*
0	*1*
8	*759*
12	*2576*
16	*759*
24	*1*

Mais ainda, se um vetor está em $\mathcal{G}$ então o seu complementar também está. Toda dodecad é a soma de 2 octads e nenhuma octad está contida em uma dodecad.

PUC-Rio - Certificação Digital Nº 1012850/CA

Demonstração. Seja $d = dim\mathcal{G}$. Pelo triângulo das octads sabemos que duas octads só podem se intersectar em 0, 2 ou 4 pontos. Donde temos 759 vetores de peso 16, pelo menos 2576 vetores de peso 12 e 759 vetores de peso 8. Temos também um vetor de peso 24 que surge da soma de todas as 759 octads e certamente temos o vetor nulo (de peso 0). Portanto já temos $759 + 2576 + 759 + 1 + 1 = 2^{12}$ vetores em $\mathcal{G}$. Daí, e como pelo lema 3.0.6 a dimensão de $\mathcal{G}$ é no máximo 12, concluímos que $d = 12$ e esses são todos os vetores de $\mathcal{G}$. Portanto nenhuma octad está contida em uma dodecad, pois do contrário $\mathcal{G}$ teria vetores de peso 4 e isso não ocorre, e toda dodecad surge da soma de 2 octads que se intersectam em um 2-conjunto (logo provamos que $n = 0$ no lema 3.0.7).

□

Motivação: Pelo teorema 3.0.8 provamos que existem exatamente 2576 dodecads que surgem da interseção de 2 octads em um 2-conjunto. Agora, fixe uma octad. Podemos nos perguntar quantas dodecads

contém obrigatoriamente alguns dos pontos dessa octad, não contém alguns outros e outros a dodecad pode ou não conter (esses pontos serão chamados de livres). Podemos também estar interessados em saber quantas dodecads existem contendo um subconjunto desta octad. No próximo teorema provaremos o triângulo das dodecads, que nos fornece a resposta a essas perguntas.

A fim de ilustrar, tome a octad $\{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8\}$. Sejam $B = \{a_2, a_3, a_4, a_5, a_7\}$ e $A = \{a_2, a_4, a_5\}$. Estamos interessados em saber o número de dodecads, $\mathcal{D}_{B,A}$, que encontram B em A exatamente, isto é, quantas são as dodecadas que obrigatoriamente contém os pontos de A e não contém os pontos de B \ A. Assim, queremos descobrir o número de dodecads que obrigatoriamente contém a_2, a_4 e a_5, não contém a_3, a_7 e os pontos a_1, a_6 e a_8 são livres. Veremos, pelo triângulo das dodecads, que temos 88 ($= \mathcal{D}_{5,3}$) tais dodecads. Observe também que quando temos A = B estamos interessados em quantas são as dodecads que obrigatoriamente contém A. Assim, no nosso exemplo, se $A = B = \{a_2, a_3, a_4, a_5, a_7\}$ veremos, pelo triângulo das dodecads, que existem 48 ($= \mathcal{D}_{5,5}$) dodecads contendo A. É fundamental notar que o número de dodecads contendo um i-conjunto contido em uma octad independe dos i pontos escolhidos, depende apenas da cardinalidade do conjunto.(veja mais detalhes em 5.1.17).

Teorema 3.0.9. *Sejam $\{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8\}$ uma octad, B um i-conjunto e A um j-conjunto, com $A \subseteq B \subseteq \mathcal{O}$. Então o número de dodecads*

PUC-Rio - Certificação Digital Nº 1012850/CA

$\mathcal{D}_{i,j}$ que encontram B em A exatamente é dado pela (j+1)-ésima entrada da $(i+1)$-ésima linha do triângulo das dodecads abaixo.

										2576														
								1288				1288												
						616				672				616										
				280				336				336				280								
			120			160				176				160				120						
		48			72			88				88			72				48					
	16			32			40			48			40			32				16				
0			16			16			24			24			16			16			0			
0		0			16			0			24			0			16			0			0	

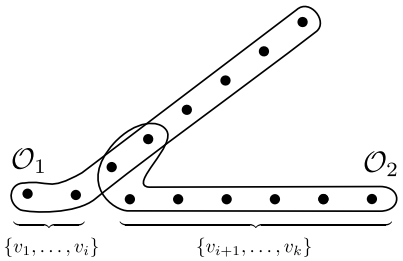
Figura 3.2: Triângulo das dodecads

Demonstração. Seja $k = 0, ..., 8$. Suponha que exista uma octad $\widetilde{\mathcal{O}}$ tal que $\{v_1, ..., v_k\} \subseteq \widetilde{\mathcal{O}}$. Queremos determinar D_k o número de dodecads $\mathcal{D}$ com $\{v_1, ..., v_k\} \subseteq \mathcal{D}$, para $k = 0, ..., 8$.

Denotemos por $o(k)$ o número de octads $\mathcal{O}$ com $\{v_1, ..., v_k\} \subseteq \mathcal{O}$, para $k = 0, 1, ..., 8$. Assim, pelo triângulo das octads, sabemos que $o(k)$ assume os valores $759, 253, 77, 21, 5, 1, 1, 1, 1$ para $k = 0, 1, 2, 3, 4, 5, 6, 7, 8$, respectivamente.

Denotemos por $\overline{o}(k)$ o número de antioctads (complementar de uma octad) $\hat{\mathcal{O}}$ com $\{v_1, ..., v_k\} \cap \hat{\mathcal{O}} = \emptyset$. Temos, pelo triângulo das octads, que $\overline{o}(k)$ vale $759, 506, 330, 210, 130, 78, 46, 30, 30$ para $k = 0, 1, 2, 3, 4, 5, 6, 7, 8$, respectivamente.

Chamemos de $Z(k)$ o número de pares de octads $\mathcal{O}_1, \mathcal{O}_2$ com $\{v_1, ..., v_k\} \subseteq \mathcal{O}_1 + \mathcal{O}_2$. Note que nenhum v_i, $0 \leq i \leq k$, pode pertencer a $\mathcal{O}_1 \cap \mathcal{O}_2$ pois do contrário não pertenceria a $\mathcal{O}_1 + \mathcal{O}_2$



Assim,

$$Z(k) = \sum_{i=0}^{k} \binom{k}{i} N_{k,i} N_{k,k-i} = 30.\overline{o}(k) + 280.o(k) + 132.\mathcal{D}_k + [k = 0].759.$$

Daí, e pelo triângulo das octads somos capazes de determinar todo o lado direito do triângulo das dodecads, isto é, temos 2576, 1288, 616, 280, 120, 48, 16, 0, 0 dodecads contendo 0, 1, 2, 3, 4, 5, 6, 7 ou 8 pontos de uma octad fixa.

Desde que existem 2576 dodecads e fixado um ponto em uma octad existem 1288 dodecads que o contém temos que existem $2576 - 1288 = 1288$

PUC-Rio - Certificação Digital Nº 1012850/CA

dodecads que não o contém. Fixado 2 pontos em uma octad existem 616 dodecads que o contém, 1288 dodecads que contém apenas um deles e portanto $1288 - 616 = 672$ dodecads que dos 2 pontos contém obrigatoriamente 1 deles e não contém o outro. Procedendo dessa maneira, completamos o triângulo das dodecads.

□

Comentário 3.0.10. Pela última linha do triângulo das dodecads, podemos observar que uma dodecad pode intersectar uma octad em 2, 4 ou 6 pontos. Mais ainda, existem 16, 24, 16 dodecads intersectando uma octad em 2, 4 ou 6 pontos, respectivamente.

Lema 3.0.11. *Considere F um corpo finito com f elementos. Sejam V um F-espaço vetorial de dimensão n e S um subespaço de dimensão d. Então, há exatamente f^{n-d} subespaços transladados de S.*

Demonstração. Fixe $v_0 \neq 0$. O subespaço transladado de S por v_0 é $S + v_0 := \{v \in V; \exists s \in S; v = s+v_0\}$. Como V é grupo (abeliano) aditivo, todo subespaço S é subgrupo normal. Donde $|\{S + v_0; v_0 \in V\}| = |(V/S)| = |V|/|S| = \frac{f^n}{f^d} = f^{n-d}$. □

Para um código $\mathcal{C} \leq F^n$ um **cocódigo** é $F^n/\mathcal{C}$. Agora estudaremos um pouco da estrutura do **cocódigo de Golay** $\mathbb{F}_2^{24}/\mathcal{C}_{24}$.

Teorema 3.0.12. *Seja G um [24, 12, 8] código binário. Então todo subespaço transladado de G em $\mathbb{Z}_2^{24}$ tem um peso n unicamente definido de 0 a 4, de acordo se ele contém um vetor de peso n. Um subespaço transladado de peso n contém exatamente um vetor de peso n se $n = 0, 1, 2$ ou 3 e 6 de peso 4 se $n = 4$. Nós temos $\binom{24}{0} + \binom{24}{1} + \binom{24}{2} + \binom{24}{3} + \frac{1}{6}\binom{24}{4} = 4096$ subespaços transladados.*

Demonstração. Seja $v_0 \in \mathbb{Z}_2^{24}$. Considere o subespaço transladado $G+v_0$. Sejam x e $y \in v_0 + G$ com pesos $m, n \leq 4$. Então se x tem peso $m < 4$, y deverá ter peso $n \geq 8 - m$; visto que $x + y \in G$ e G tem peso mínimo 8. Portanto os vetores de peso 0, 1, 2 ou 3 são únicos nos subespaços transladados com este peso. Mas se x e $y \in v_0 + G$, $x \neq y$, com pesos $m, n = 4$ então x e y devem ser disjuntos e $|\{w \in G + v_0; |w| = 4\}| \leq 6$. Como a dimensão de G é 12, pelo lema anterior, G tem exatamente 2^{12} subespaços transladados. O limite inferior para o número de subespaços transladados com distância mínima ≤ 4 é: $\binom{24}{0} + \binom{24}{1} + \binom{24}{2} + \binom{24}{3} + \frac{1}{6}\binom{24}{4} = 4096$, e portanto esses são todos os subespaços transladados. □

O cocódigo de Golay tem a seguinte distribuição de peso

PUC-Rio - Certificação Digital Nº 1012850/CA

$$0^1\ 1^{24}\ 2^{276}\ 3^{2024}\ 4^{1771}.$$

Um **sextet** é uma coleção de seis 4-conjuntos tais que a união de quaisquer 2 é uma octad. Qualquer **tetrad** (4-conjunto) determina um único sextet. O número de sextets é $\frac{1}{6}\binom{24}{4} = \frac{10626}{6} = 1771 = 7.11.23$. Chamaremos de **sextet base** aquele cujos seis tetrads são as colunas da matriz MOG, conforme mostra a figura 3.3.

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

Figura 3.3: Sextet base

Proposição 3.0.13. *Existe bijeção entre um representante da classe dos sistema de Steiner $S(5, 8, 24)$ em Ω e o $\mathcal{C}_{24}$ código binário de Golay, obtida da seguinte maneira: o gerador linear de um sistema de Steiner é um código de Golay e o conjunto de vetores de peso 8 no código de Golay é um sistema de Steiner.*

Demonstração. Pelo teorema 3.0.8 temos que o sistema de Steiner $S(5, 8, 24)$ determina um código binário de Golay. Falta provarmos que código binário de Golay determina um sistema de Steiner. Para isso, considere S o conjunto de vetores de peso 8 em $\mathcal{C}_{24}$. Vamos mostrar que S é um sistema de Steiner. Tome F um 5-conjunto em $\mathbb{Z}_2^{24}$. Considere o subespaço transladado $F + \mathcal{C}_{24}$. Pelo teorema 3.0.12, $F + \mathcal{C}_{24}$ tem peso mínimo ≤ 4. Digamos que isso ocorra em $T \in \mathcal{C}_{24}$. Suponhamos, $n = 4$. Denote por $\mathcal{A}$ o conjunto dos 4-conjuntos em $F + \mathcal{C}_{24}$. Seja $U \in \mathcal{A}$ um 4-conjunto que contém $k, 1 \leq k \leq 4$, pontos em F. Então $F + U \in \mathcal{C}_{24}$ e tem peso $7, 5, 3$ ou 1 de acordo se $k = 1, 2, 3$ ou 4, respectivamente. Mas isso não é possível, pois $\mathcal{C}_{24}$ contém apenas vetores de peso $0, 8, 12, 16$ e 24. Portanto, $n \leq 3$. Veremos que $n = 3$. Mas antes, façamos o mesmo para $n = 2$. Assim, sejam $\mathcal{A}$ o conjunto dos 2-conjuntos em $F + \mathcal{C}_{24}$ e $U \in \mathcal{A}$ um 2-conjunto que contém 1 ou 2 pontos em F. Portanto, $F + U$ terá peso 6 caso tenha um ponto em comum com F e peso 3 caso esteja contido em F, mas ambos os pesos não ocorrem em $\mathcal{C}_{24}$. Analogamente temos que n não pode ser 1 e portanto $n = 3$. E F está contido no 8-conjunto $F + T = F \sqcup T \in \mathcal{C}_{24}$. Pelo teorema 2 sabemos que este subespaço transladado tem um único vetor de peso 3. Donde o 8-conjunto $F + T$ é único. □

Donde concluimos que o sistema de Steiner $S(5, 8, 24)$ é único a menos de isomorfismo.

PUC-Rio - Certificação Digital Nº 1012850/CA