Universidad Nacional Autónoma
de México

Facultad de Ciencias

CONSTRUCCIÓN DE SISTEMAS TRIPLES DE STEINER NO CLÁSICOS

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

MATEMÁTICO

P R E S E N T A :

JUAN CARLOS GARCÍA ALTAMIRANO

DIRECTOR DE TESIS:

DR. OCTAVIO PÁEZ OSUNA

2013

Hoja de Datos del Jurado

1.Datos del alumno
García
Altamirano
Juan Carlos
55 19 39 00 30
Universidad Nacional Autónoma de México
Facultad de Ciencias
Matemáticas
303160175

2. Datos del tutor
Dr.
Octavio
Páez
Osuna

3. Datos del sinodal 1
Dra.
Eugenia
O'Reilly
Regueiro

4. Datos del sinodal 2
Dr.
Luis Bernardo
Morales
Mendoza

5. Datos del sinodal 3
Dr.
Carlos
Velarde
Velázquez

6. Datos del sinodal 4
Dr.
Rodolfo
San Agustín
Chi

7.Datos del trabajo escrito
Construcción de Sistemas Triples de Steiner no clásicos
75 p.
2013

Índice general

Introducción

Uno de los problemas más reconocidos en la teoría combinatoria es el **problema de las colegialas** propuesto en 1850 por Thomas Kirkman (1847); que dice más o menos así:

> "quince jovencitas de una escuela caminan en tres columnas durante siete días consecutivos: se requiere un arreglo diário de modo que no haya dos de ellas que caminen dos veces en la misma fila."

Las soluciones de este problema resultan ser casos particulares de los *Sistemas Triples de Steiner* con 15 puntos, dichos sistemas merecen el nombre a Jacob Steiner (1853).

Un Sistema Triple de Steiner es una estructura de incidencia con v puntos donde todos sus bloques son de tamaño 3 con la propiedad de que cada par de puntos está contenido en un único bloque. Si bien se conoce con exactitud en que situaciones se satisface la existencia de Sistemas Triples de Steiner; son pocos los casos en los que, con un determinado tamaño, se sabe cuantos sistemas hay no *isomorfos* y se construyen todos ellos. El objetivo principal de este trabajo es dar un ejemplo de como construir dos Sistemas Triples de Steiner no isomorfos, con $2^{n+1}-1$ y 3^n puntos, utilizando un singular método en el que se vislumbra una manera más general de construcción. Para ello nos apoyaremos de distintas teorías matemáticas: teoría de diseños, teoría de códigos y geometrías finitas, valiendonos de resultados de álgebra lineal y teoría combinatoria. Por supuesto, se dan todos los resultados necesarios para justificar nuestra construcción, incluso, en algunos casos se recurrió a introducir conceptos y resultados propios (muy sencillos) para que se viera de manera natural, tanto la construcción que haremos, como la relación que existe entre las antes mencionadas teorías matemáticas. Pero no sólo eso, sino que en cada tema de los respectivos capítulos, se exponen, de forma accesible, las definiciones y los resultados mas relevantes de modo que sea una introducción competente a dichos temas.

La tesis se divide en cinco capítulos; en el primer capítulo expondremos sobre los Sistemas de Steiner, viendo algunos resultados básicos de su estructura; aún más, nos enfocaremos en los Sistemas Triples de Steiner, ya que ellos serán parte central de la tesis, analizando y desarrollando sus principales propiedades. En el segundo capítulo; definiremos, a partir de axiomas, al plano Afín y al plano Proyectivo, y proporcionaremos las propiedades básicas dando así la motivación de conceptos más generales como son el Espacio Afín y el Espacio Proyectivo. De estos espacios, trabajando con campos finitos, veremos dos casos muy importantes que tienen como subestructuras a los Sistemas Triples de Steiner *clásicos*.

Para el tercer capítulo, además de los conceptos básicos de códigos lineales, daremos algunos resultados de códigos asociados a estructuras de incidencia, que serán de gran utilidad para concluir este trabajo. En el cuarto capítulo trabajaremos con la matriz de incidencia de un Sistema Triple de Steiner y se calculará el rango de dicha matriz sobre campos finitos, resultando así que los casos interesantes se dan cuando los campos tienen p elementos; con p igual a 2 y 3. Cabe mencionar que el resultado de este capítulo es de gran relevancia para generalizar nuestros resultados principales.

Y por último, en el quinto capítulo, nos ocuparemos de los códigos generados por las matrices de incidencia de los Sistemas Triples de Steiner clásicos, que a través de algunas modificaciones en su estructura se podrán obtener otros Sistemas Triples de Steiner no isomorfos a los primeros, siendo éste el resultado central de la tesis.

Capítulo 1

Sistemas de Steiner

Definición 1.0.1 *Una* ***estructura de incidencia*** S *es una pareja* $(\mathcal{P}, \mathcal{B})$ *donde* $\mathcal{P}$ *es un conjunto no vacío y* $\mathcal{B}$ *es una familia de subconjuntos de* $\mathcal{P}$ *no vacíos. A los elementos de* $\mathcal{P}$ *les llamamos* ***puntos*** *y a los elementos de* $\mathcal{B}$ *les llamamos* ***bloques****. En el caso de que* $\mathcal{P}$ *sea finito decimos que la estructura de incidencia es finita.*

Definición 1.0.2 *Dos estructuras de incidencia* S_1 *y* S_2 *son* ***isomorfas*** *si y sólo si existe una función biyectiva* ϕ *de los puntos de* S_1 *a los puntos de* S_2 *tal que; el conjunto de imágenes de los elementos de cada bloque en* S_1*, es un bloque en* S_2*, así como los elementos de cada bloque en* S_2*, son imágenes de los elementos de un bloque en* S_1*. En tal caso a* ϕ *le llamamos* ***isomorfismo*** *de* S_1 *a* S_2*. Si* $S_1 = S_2$ *entonces diremos que* ϕ *es un* ***automorfismo****.*

Definición 1.0.3 *Un* ***Sistema de Steiner*** $S(t, k, v)$*, es una estructura de incidencia finita* $(\mathcal{P}, \mathcal{B})$ *tal que: la cardinalidad de* $\mathcal{P}$ *es* v*, los subconjuntos de* $\mathcal{B}$ *tienen cardinalidad igual a* k *y tienen la propiedad de que cada subconjunto de* $\mathcal{P}$ *con tamaño* t *está contenido en un único bloque de* $\mathcal{B}$*.*

Dada dicha estructura diremos que los puntos de $\mathcal{P}$ y los bloques de $\mathcal{B}$ son elementos del $S(t, k, v)$.

Además notamos que, para no tener sistemas triviales, debemos pedir que $t < k < v$.

Con $t = 2$ podemos entender la propiedad de la Definición 1.0.3 como que cada *par* de puntos está contenido en un único bloque de $\mathcal{B}$. En esta situación; si para cada $x \in \mathcal{P}$ denotamos por r_x a la cantidad de conjuntos en $\mathcal{B}$ que

contienen a x entonces r_x es independiente de la x, es decir, es el mismo valor r para cualquier x, aún más, sabemos cuanto vale explícitamente.

Proposición 1.0.1 *En un $S(2,k,v)$ cada punto está contenido en exactamente*

$$r = \frac{v-1}{k-1} \tag{1.1}$$

bloques.

Demostración. Sea $x \in S(2,k,v)$ y r_x la cantidad de bloques que contienen a x entonces cada uno de esos bloques contiene $k-1$ elementos distintos a x y como $t=2$, cualquier par de bloques sólo se intersectan en x, entonces estamos contando a todos los puntos de $S(2,k,v)$ excepto a x, es decir;

$$r_x(k-1) = v-1$$

$$\implies r_x = \frac{v-1}{k-1}$$

y por lo tanto no depende de la x,

$$\implies r = \frac{v-1}{k-1}.$$

□

Otro parámetro que se encuentra *implícito* es $b = |B|$, entonces notamos que los valores k, v, r, b están relacionados de manera intrínseca.

Definición 1.0.4 *Sea $S = (\mathcal{P}, \mathcal{B})$ una estructura de incidencia finita con $\mathcal{P} = \{p_1, p_2, ..., p_v\}$ y $\mathcal{B} = \{B_1, B_2, ..., B_b\}$. Entonces:*

a) para todo $A \subseteq \mathcal{P}$ definimos el ***vector de incidencia*** *de A como:*

$$\chi(A) := (\chi_A(p_1), \chi_A(p_2), ..., \chi_A(p_v)),$$

donde, $\chi_A(p_i) = 1$ si $p_i \in A$, y $\chi_A(p_i) = 0$ si $p_i \notin A$.

b) definimos una ***matriz de incidencia*** *$M_{b\times v}$ de S, como una matriz que tiene por renglones a los vectores de incidencia determinados por los bloques de S.*

Proposición 1.0.2 *En un $S(2,k,v)$*

$$bk = vr. \tag{1.2}$$

Demostración. Consideremos una matriz de incidencia $M_{b\times v}$ del $S(2,k,v)$. Entonces contamos a los $1's$ de dicha matriz de dos maneras distintas; si los contamos por renglones tenemos b renglones y cada renglón tiene k $1's$ ya que cada bloque tiene k puntos, y si los contamos por columnas, tenemos v columnas y cada columna tiene r $1's$ debido a que cada punto está contenido en r bloques, por lo tanto

$$bk = vr.$$

□

La matriz de incidencia que definimos anteriormente jugará un papel muy importante a lo largo del presente trabajo.

Además ya podemos contar el número de bloques en términos de los parámetros (t,k,v).

Corolario 1.0.1 *En un $S(2,k,v)$ la cantidad de bloques está dada por*

$$b = \frac{v(v-1)}{k(k-1)}. \tag{1.3}$$

Demostración. De la Proposición 1.0.1 tenemos que $r = \dfrac{v-1}{k-1}$, sustituimos en (1.2) y resulta

$$bk = v\Big(\frac{v-1}{k-1}\Big)$$
$$\Longrightarrow b = \frac{v(v-1)}{k(k-1)}.$$

□

Para ver un resultado importante, con respecto a estos parámetros, es necesario que recordemos un par de resultados de *Álgebra Lineal* [1].

Definición 1.0.5 *Sea A una matriz de $n\times m$ con entradas sobre un campo $\mathbb{F}$. Definimos la* ***transformación de multiplicación por la izquierda de*** *A, como el mapeo L_A, donde:*

$$\begin{aligned} L_A : \mathbb{F}^m &\longrightarrow \mathbb{F}^n \\ \bar{x} &\mapsto A\bar{x}^t. \end{aligned}$$

Definición 1.0.6 *Sea A una matriz de $n \times m$ con entradas sobre un campo $\mathbb{F}$. Definimos el* ***rango*** *de A, denotado $Rango(A)$, como el rango de la transformación lineal L_A.*

Lema 1.0.1 *Sea A una matriz de $n \times m$ y B una matriz tal que el producto AB está definido, entonces:*

(i) $Rango(A) \leq min\{n, m\}$

(ii) $Rango(AB) \leq Rango(A)$.

Teorema 1.0.1 *En un $S(2, k, v)$, $v \leq b$.*

Demostración. Consideremos la matriz de incidencia $M_{b\times v}$ y su transpuesta $M^t_{v\times b}$ y obtengamos la matriz $M^t M_{v\times v}$ recordando que las entradas del producto se definen como:

$$a_{ij} = \sum_{k=1}^{b} n_{ik} m_{kj},$$

donde n_{ik} y m_{kj} son entradas de $M^t_{v\times b}$ y $M_{b\times v}$ respectivamente. En la entrada a_{ij}, lo que hacemos ,visto en la matriz de incidencia, es intersectar los $1's$ de la columna i de $M_{b\times v}$ con los de la coumna j de $M_{b\times v}$; entonces la entrada a_{ij} cuenta en cuantos bloques están contenidos los dos elementos i y j, por lo que a_{ij} es 1 si $i \neq j$, y a_{ij} es r si $i = j$. De manera que tenemos la siguiente situación:

$$M^t M_{v\times v} = \begin{pmatrix} r & 1 & \dots & 1 \\ 1 & r & \dots & 1 \\ \vdots & & \ddots & \vdots \\ 1 & 1 & \dots & r \end{pmatrix},$$

como $k < v \quad$ y $\quad r = \dfrac{v-1}{k-1}, \Longrightarrow r > 1$, entonces los v renglones de la matriz $M^t M_{v\times v}$ son linealmente independientes, $\Longrightarrow Rango(M^t M_{v\times v}) = v$, por el Lema 1.0.1,$\Longrightarrow Rango(M^t M_{v\times v}) \leq Rango(M_{b\times v})$, por lo tanto,
$v \leq Rango(M_{b\times v})$, y como $Rango(M_{b\times v}) \leq min\{b, v\}$, $\Longrightarrow v \leq b$.

□

En la Proposición 1.0.1 y en el Corolario 1.0.1 se encuentran condiciones necesarias para la existencia de un $S(2, k, v)$. En la siguiente sección profundizaremos un poco más en estos menesteres ya que nos interesa un caso en particular; $S(2, 3, v)$.

1.1. Sistemas Triples de Steiner

Definición 1.1.1 *Un **Sistema Triple de Steiner** $STS(v)$ es un Sistema de Steiner $S(2,3,v)$.*

Aquí nos podríamos preguntar que si una vez fijados los parámetros t y k, ¿siempre podemos construir un $STS(v)$ con cualquier valor de v?; veamos que no es así.

De los resultados anteriores tenemos que en un Sistema Triple de Steiner $STS(v)$:

1. $r = \dfrac{v-1}{2}$
2. $b = \dfrac{v(v-1)}{6}$.

Como ya notamos, estas igualdades son condiciones de existencia de un $STS(v)$; ya que r, que es la cantidad de bloques en los que está contenido cada punto, y b, el número de bloques del sistema, tienen que ser enteros.

Lema 1.1.1 *Si existe un $STS(v)$, entonces;*

$$v \equiv 1, 3 \ (mod\ 6).$$

Demostración. Que r sea entero, implica que 2 divide a $v-1$, entonces v es *impar*.

Y que b sea entero, nos dice que

$\dfrac{v(v-1)}{2 \cdot 3}$ es entero, entonces 3 divide a v ó 3 divide a $v-1$.

caso 1.
3 divide a v, como v es impar $\Longrightarrow v = 3(2n+1)$ p.a. $n \in \mathbb{N}$,
$\Longrightarrow v = 6n+3$ p.a. $n \in \mathbb{N}$,
$\Longrightarrow v \equiv 3 \pmod 6$.

caso 2.
3 divide a $v-1$, como $v-1$ es par $\Longrightarrow (v-1) = 3(2n)$ p.a. $n \in \mathbb{N}$,
$\Longrightarrow (v-1) = 6n$ p.a. $n \in \mathbb{N}$,
$\Longrightarrow v \equiv 1 \pmod 6$.

□

Ejemplos de $STS(v)$ cuando $v = 3, 7, 9$:

Ejemplo 1 $v = 3$, $\mathcal{P} = \mathcal{B} = \{0, 1, 2\}$.

Ejemplo 2 $v = 7$, $\mathcal{P} = \{1, 2, 3, 4, 5, 6, 7\}$,

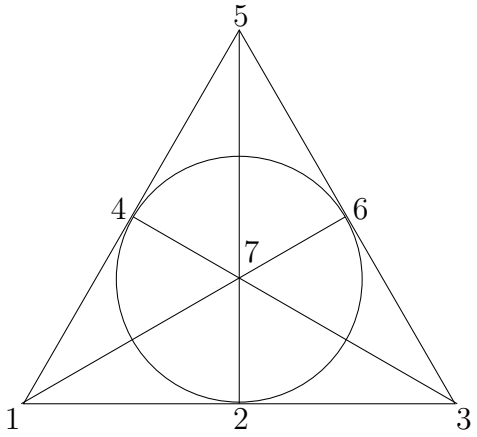


Figura 1.1: Sistema Triple de Steiner con 7 puntos.

$\mathcal{B} = \{\{1, 2, 3\}, \{1, 4, 5\}, \{1, 6, 7\}, \{2, 5, 7\}, \{3, 4, 7\}, \{3, 5, 6\}, \{2, 4, 6\}\}$.

Ejemplo 3 $v = 9$, $\mathcal{P} = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$,

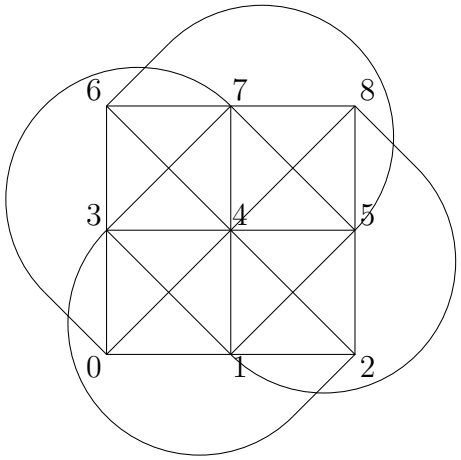


Figura 1.2: Sistema Triple de Steiner con 9 puntos.

$\mathcal{B} = \{\{0, 1, 2\}, \{0, 3, 6\}, \{0, 4, 8\}, \{0, 5, 7\}, \{1, 3, 8\}, \{1, 5, 6\}, \{1, 4, 7\},$
$\{2, 3, 7\}, \{2, 5, 8\}, \{2, 4, 6\}, \{3, 4, 5\}, \{6, 7, 8\}\}$.

Entonces las preguntas inmediatas que nos surgen son: ¿existirá un $STS(v)$ con $v = 13, 15, 19, ...?$, y en caso de existir ¿podríamos tener más de un Sistema Triple de Steiner con el mismo parámetro v y que no sean isomorfos?, ya que hasta ahora nos hemos limitado a estudiar los parámetros que forman un Sistema de Steiner, pero debemos notar que algo igual de importante, es la *estructura* de dicho sistema.

Definición 1.1.2 *Un* ***subsistema*** *de un Sistema Triple de Steiner $STS(v)$, es un conjunto S' de puntos del $STS(v)$ tal que; cada bloque del $STS(v)$ que tenga dos puntos de S', está totalmente contenido en S'. Si $S' \neq S$, decimos que S' es un subsistema propio.*

Lema 1.1.2 *Si S' es un subsistema del $STS(v)$, entonces S' también es un Sistema Triple de Steiner.*

Demostración. Sean x y y puntos en S' como $S' \subseteq STS(v)$; x y y están contenidos en el $STS(v)$, entonces existe un único bloque en el $STS(v)$ que contiene a x y y, dado que S' es subsistema de $STS(v)$ implica que ese bloque está enteramente contenido en S'. Por lo tanto existe un único bloque en S' que contiene a x y y.

□

Teorema 1.1.1 *Si existen un $STS(v_1)$ y un $STS(v_2)$, entonces también existe el $STS(v_1v_2)$ conteniendo subsistemas isomorfos al $STS(v_1)$ y al $STS(v_2)$.*

Demostración. Denotemos los puntos del $STS(v_1)$ como $x_1, x_2, ..., x_{v_1}$ y los del $STS(v_2)$ como $y_1, y_2, ..., y_{v_2}$. Los puntos del $STS(v_1v_2)$ serán los elementos $z_{ij} := (x_i, y_j)$, con $1 \leq i \leq v_1$, $1 \leq j \leq v_2$, del producto cartesiano $\{x_1, ..., x_{v_1}\} \times \{y_1, ..., y_{v_2}\}$.

Vamos a construir los bloques del $STS(v_1v_2)$. El conjunto $\{z_{lf}, z_{mg}, z_{nh}\}$ es un bloque del $STS(v_1v_2)$ si y sólo si cumple con alguna de las siguientes condiciones:

(*i*) $f = g = h$ y $\{x_l, x_m, x_n\}$ es un bloque del $STS(v_1)$.

(*ii*) $l = m = n$ y $\{y_f, y_g, y_h\}$ es un bloque del $STS(v_2)$.

(*iii*) l, m y n son diferentes dos a dos y $\{x_l, x_m, x_n\}$ es un bloque en el $STS(v_1)$, y f, g y h son diferentes dos a dos y $\{y_f, y_g, y_h\}$ es un bloque del $STS(v_2)$.

Nos falta probar que estos puntos y bloques en verdad cumplen las condiciones de el sistema deseado, para ello debemos probar que para cualquier par de elementos que tomemos del producto cartesiano exista un único bloque qu los contenga a ambos.

Sean z_{lf} y z_{mg} dos puntos diferentes del producto cartesiano, consideremos tres casos:

caso 1.

$f = g$ y así $l \neq m$, entonces existe un único bloque en el $STS(v_1)$ que contiene a x_l y x_m, sea $\{x_l, x_m, x_n\}$ tal bloque, por lo tanto el único bloque que tiene a z_{lf} y z_{mg} es $\{z_{lf}, z_{mf}, z_{nf}\}$.

caso 2.

$l = m$ y así $f \neq g$, entonces existe un único bloque en el $STS(v_2)$ que contiene a y_f y y_g, sea $\{y_f, y_g, y_h\}$ tal bloque, por lo tanto el único bloque que tiene a z_{lf} y z_{mg} es $\{z_{lf}, z_{lg}, z_{lh}\}$.

caso 3.

$l \neq m$ y $f \neq g$ entonces los bloques que tienen a x_l y a x_m en el $STS(v_1)$, y a y_f y y_g en el $STS(v_2)$, son únicos, sean $\{x_l, x_m, x_n\}$ y $\{y_f, y_g, y_h\}$ dichos bloques, entonces el único bloque al que le corresponden z_{lf} y z_{mg} es $\{z_{lf}, z_{mg}, z_{nh}\}$.

Por otro lado, si nos fijamos sólo en los elementos de los bloques $\{z_{lf}, z_{mg}, z_{nh}\}$ con $l = n = m = 1$, tenemos un subsistema isomorfo al $STS(v_1)$, así como los elementos de los bloques con $f = g = h = 1$ son un subsistema isomorfo al $STS(v_2)$.

□

Teorema 1.1.2 *Si existen el $STS(v_1)$, el $STS(v_2)$ y $S \subset STS(v_2)$ tal que, $|S| = v_3$ y S es un subsistema del $STS(v_2)$ o S es un punto ($v_3 = 1$), entonces también existe el $STS(v_3 + v_1(v_2 - v_3))$ conteniendo subsistemas isomorfos al $STS(v_1)$, al $STS(v_2)$ y a S.*

Demostración. Empezamos numerando los puntos del $STS(v_1)$, luego numeramos los puntos de $STS(v_2) \setminus S$ continuando esta numeración en S.Para esta construcción consideremos los siguientes $v_1 + 1$ conjuntos:

$$\begin{array}{lccccc} S_0: & a_{s+1} & a_{s+2} & \cdots & a_{v_2} & \\ S_1: & b_{11} & b_{12} & \cdots & b_{1s} & \\ S_2: & b_{21} & b_{22} & \cdots & b_{2s} & , \text{ donde } s = v_2 - v_3. \\ \vdots & \vdots & \vdots & \vdots & \vdots & \\ S_{v_1}: & b_{v_1 1} & b_{v_1 2} & \cdots & b_{v_1 s} & \end{array}$$

Los puntos de $STS(v_3 + v_1(v_2 - v_3))$, a construir, son los puntos de $\bigcup_{\lambda=0}^{v_1} S_\lambda$.

Es claro que $\left| \bigcup_{\lambda=0}^{v_1} S_\lambda \right| = v_3 + v_1(v_2 - v_3)$.

Para construir los bloques seguimos estas reglas:

(i) $\{a_l, a_m, a_n\}$ es un bloque si $\{l, m, n\}$ es un bloque de S.

(ii) $\{a_f, b_{lg}, b_{lh}\}$ o $\{b_{lf}, b_{lg}, b_{lh}\}$ son bloques si $\{f, g, h\}$ es un bloque del $STS(v_2)$.

(iii) $\{b_{lf}, b_{mg}, b_{nh}\}$ es un bloque si $\{l, m, n\}$ es un bloque del $STS(v_1)$ y f, g, h son tales que $f + g + h \equiv 0 \ (mod\ s)$.

Lo que necesitamos para asegurar que estas reglas definen un Sistema Triple de Steiner es; que para cualquier par de puntos que tomemos, exista un único bloque al que los contenga a ambos.

caso 1.

Si ambos elementos son $a's$, entonces por (i) existe un único bloque al que le atañen.

caso 2.

Si un elemento es a_f y el otro es b_{lg}, por (ii) hay un único bloque que los contiene.

caso 3.

Los dos puntos son $b's$ y pertenecen al mismo renglón, entonces la regla (ii) cubre este caso.

caso 4.

Los puntos son $b's$ y no son parte del mismo renglón, es decir, son b_{lf} y b_{mg}, y como en el $STS(v_1)$, sólo el bloque $\{l, m, n\}$ es el que tiene l

y m, y aunado a ello hay un único entero h entre 1 y s tal que $f + g + h \equiv 0 \ (mod\ s)$, por (iii) queda claro la existencia y unicidad del bloque en cuestión.

En cuanto a los subsistemas; los bloques descritos; en (i) son isomorfos a S, en (ii) para una "i" fija son isomorfos al $STS(v_2)$, y los de (iii) con $f = g = h = s$ son isomorfos al $STS(v_1)$.

□

Con estos dos últimos Teoremas y con los ejemplos 1,2 y 3, ya podemos construir una cantidad infinita de Sistemas Triples de Steiner; en particular las familias que a continuación se muestran.

Corolario 1.1.1 *Para toda $n \in \mathbb{N}$, existe un $STS(2^{n+1} - 1)$.*

Demostración. Por inducción; del Ejemplo 1 sabemos que existe un Sistema Triple de Steiner con 3 puntos, pero $3 = 2^{1+1} - 1$. Ahora, si suponemos que existe un $STS(2^n - 1)$, por el Teorema 1.1.2 con $v_1 = 2^n - 1$, $v_2 = 3$ y $v_3 = 1$, resulta que existe un

$$STS(1 + (2^n - 1)(3 - 1)) = STS(1 + 2^{n+1} - 2) = STS(2^{n+1} - 1).$$

□

Corolario 1.1.2 *Para toda $n \in \mathbb{N}$, existe un $STS(3^n)$.*

Demostración. También por inducción; por el Ejemplo 1 existe un Sistema Triple de Steiner con 3 puntos. Si suponemos que existe un $STS(3^{n-1})$ entonces por el Teorema 1.1.1 con $v_1 = 3$ y $v_2 = 3^{n-1}$, existe un $STS(3^n)$.

□

Aprovecharemos la oportunidad para mencionar otro tipo de Sistemas de Steiner.

1.2. Sistemas Cuádruples de Steiner

Definición 1.2.1 *Un **Sistema Cuádruple de Steiner** $SQS(v)$ es un Sistema de Steiner $S(3, 4, v)$.*

La demostración de siguiente Teorema puede ser consultada en [2], nosotros la omitimos dado que es muy larga y el resultado, a pesar de ser muy fuerte, no es indispensable para el desrrollo de nuestro trabajo.

Teorema 1.2.1 *Un $SQS(v)$ existe $\Leftrightarrow v \equiv 2, 4$ (mod 6).*

Definición 1.2.2 *Sea $S(t, k, v)$ un Sistema de Steiner con $\mathcal{P}$ puntos y $\mathcal{B}$ bloques, $I \subseteq \mathcal{P}$ con $|I| \leq t$, entonces a la **subestructura** S_I formada por los puntos $\mathcal{P}' = \mathcal{P} \backslash I$ y los bloques $\mathcal{B}' = \{B \backslash I : I \subseteq B \in \mathcal{B}\}$, le llamamos **sistema derivado** del $S(t, k, v)$. Y si $I = \{p\}$, esto es, I es solamente un punto; a S_p le llamaremos **contracción** de $S(t, k, v)$ en el punto p.*

Proposición 1.2.1 *Sea $S(t, k, v)$ un Sistema de Steiner; si S_I es un sistema derivado de $S(t, k, v)$ con $|I| = i$, entonces S_I es un $S(t - i, k - i, v - i)$.*

Demostración. Es obvio que $|\mathcal{P}'| = v - i$. Veamos ahora que la cardinalidad de todos los bloques de S_I es $k - i$ Sea B' un bloque de S_I entonces existe un bloque B en $\mathcal{B}$ tal que $B' = B \backslash I$. Pero

$$k = |B| = |B \backslash I \cup I| = |B \backslash I| + |I|,$$

por lo tanto $|B'| = k - i$. Por útimo escojamos un conjunto $T \subset \mathcal{P}'$ con $|T| = t - i$, entonces $T \cup I$ es un conjunto tal que $T \cup I \subset \mathcal{P}$ y $|T \cup I| = t$ entonces existe un único bloque $B \in \mathcal{B}$ con $T \cup I \subset B$, entonces $B \backslash I$ es el único bloque en $\mathcal{B}'$ tal que $T \subset B \backslash I$.

□

Corolario 1.2.1 *Si $v \equiv 1, 3$ $(mod\ 6) \Longrightarrow$ existe un $STS(v)$.*

Demostración. Sea $w = v + 1$ entonces $w \equiv 2, 4$ $(mod\ 6)$, por el Teorema 1.2.1 sabemos que existe un $SQS(w)$ entonces escojamos un punto p de los w puntos y consideremos S_p, por la Proposición 1.2.1;

$$S_p = S(3 - 1, 4 - 1, w - 1) = STS(v).$$

□

Con esto hemos respondido una de nuestras interrogantes, pero surgen otras: si $v \equiv 1, 3$ $(mod\ 6)$ el $STS(v)$ que existe; ¿será único salvo isomorfismos?, en caso de que no, ¿cuántos hay no-isomorfos a él?, ¿cómo encontrar todos los no-isomorfos?. Estas preguntas aún no han sido respondidas excepto en algunos casos.

Capítulo 2

Geometría Afín y Geometría Proyectiva

Definición 2.0.3 *Un **espacio** S es una estructura de incidencia (P_S, L_S), donde los elementos p de P_S se llaman **puntos** de S y los elementos l de L_S se llaman **líneas** de S. Decimos que " p está en l" o " l pasa por p" cuando el punto p es elemento de la línea l. Dos líneas, l_1 y l_2, son **paralelas** si $l_1 = l_2$ o $l_1 \cap l_2 = \emptyset$, lo denotamos como $l \parallel m$. Los puntos $p_1, p_2, ..., p_n$, son **colineales** si existe una línea l que los contiene. Las líneas $l_1, l_2, ..., l_m$, **concurren** en un punto p si $p \in l_i$ para toda $i = 1, ..., m$. Un **haz de líneas** es el conjunto L_p de todas las líneas que contienen a un punto p en particular, o el conjunto $[l]$ de todas las líneas paralelas a una línea l, en este caso llamamos a $[l]$ **punto al infinito** en la dirección de l.*

2.1. Plano Afín

Definición 2.1.1 *Un **plano Afín** $\mathcal{A}$ es un espacio que cumple con los siguientes axiomas:*

A_1 *Dados dos puntos distintos p y q, existe una y sólo una línea que los contiene.*

A_2 *Dados una línea l y un punto p que no pertenece a l, existe una y sólo una línea m, paralela a l, que pasa por p.*

A_3 *Existen tres puntos no-colineales.*

Proposición 2.1.1 *En un plano Afín, dos líneas distintas tienen a lo más un punto en común.*

Demostración. Si l y m, pasan por dos puntos distintos p y q, por el axioma A_1; $l = m$.

□

Proposición 2.1.2 *En un plano Afín, el paralelismo es una relación de equivalencia.*

Demostración. Debemos probar que:

1. Una línea es paralela a si misma,
2. Si $l \parallel m$, entonces $m \parallel l$.
3. Si $l \parallel m$, y $m \parallel n$, entonces $l \parallel n$.

De la definición de paralelismo, son obvios 1 y 2, y si en 3, $l = n$, no hay nada que demostrar. Para demostrar 3, sean l, m y n líneas tal que $l \parallel m$, y $m \parallel n$ y $l \neq n$. Supongamos que $p = l \cap n$. Entonces tenemos que por el punto p pasan dos líneas distintas, paralelas a m, contradiciendo A_2. Por lo tanto $l \cap n = \emptyset$, entonces $l \parallel n$.

□

Proposición 2.1.3 *En un plano Afín cada línea tiene al menos dos puntos.*

Demostración. Sea l una línea de un plano Afín, por A_3 existen tres puntos p, q y r no-colineales, entonces las líneas l_{pq}, l_{qr} y l_{rp} que pasan por ellos no son paralelas dos a dos, por lo que l no es paralela a al menos dos de éllas; sin pérdida de generalidad sean l_{pq} y l_{qr} líneas que no son paralelas a l, entonces existen $x = l \cap l_{pq}$ y $y = l \cap l_{qr}$;

si $x = y$ implica que $x = y = q$ y como $q \notin l_{rp}$ entonces l no es paralela a l_{rp}, y así existe $z = l \cap l_{rp}$, por esta razón l contiene al menos a los dos puntos q y z,

si $x \neq y$ entonces ya tenemos al menos dos puntos en l.

□

Proposición 2.1.4 *Un plano Afín tiene al menos cuatro puntos.*

Demostración. Por A_3 sabemos que existen tres puntos no-colineales, sean p, q y r. Por A_1 existe una línea l_{pq} que pasa por p y q, y una línea m_{qr} que pasa por q y r. De A_2 tenemos que existe, una línea l paralela a l_{pq} que pasa por r, y una línea m paralela a m_{qr} que pasa por p. Si l y m fueran paralelas, tendríamos que $l_{pq} \parallel l \parallel m \parallel m_{qr}$, pero $l_{pq} \cap m_{qr} = q$, entonces $l_{pq} = m_{qr}$, por lo que p, q y r serían colineales. Entonces sea $t = l \cap m$, el punto t no pertenece a la línea l_{pq} ya que t está en l que es distinta a l_{pq}, t tampoco esta en m_{qr} porque m es distinta a m_{qr}, entonces $t \neq p, q, r$. Por lo tanto t es el cuarto punto.

□

Proposición 2.1.5 *Existe un plano Afín con cuatro puntos.*

Demostración. Consideremos los puntos y las líneas de la demostración anterior. Unamos la líneas $l_1 = \{p, r\}$ y $l_2 = \{q, t\}$. Entonces el plano Afín consiste de los cuatro puntos $\{p, q, r, t\}$ y las seis líneas $\{p, q\}, \{q, r\}, \{r, t\}, \{t, q\}$, $\{p, r\}$ y $\{q, t\}$.

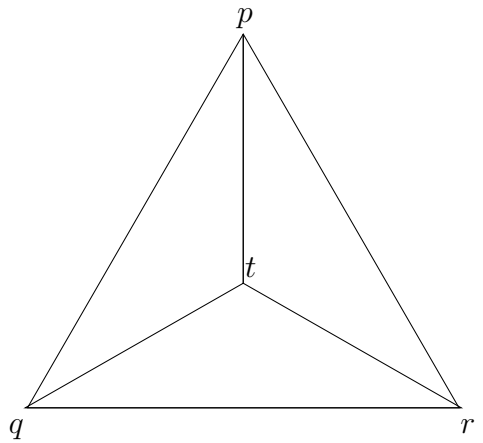


Figura 2.1: Plano Afín con 4 puntos.

□

2.2. Plano Proyectivo

Definición 2.2.1 *Un **plano Proyectivo** $\mathcal{P}$ es un espacio que cumple los siguientes axiomas:*

P_1 *Dados dos puntos distintos p y q, existe una y sólo una línea que los contiene.*

P_2 *Cualesquiera dos líneas se intersectan en al menos un punto.*

P_3 *Existen tres puntos no-colineales.*

P_4 *Toda línea contiene al menos tres puntos.*

Proposición 2.2.1 *En un plano Proyectivo, dos líneas distintas se intersectan en un solo punto.*

Demostración. Sean l y m líneas distintas, por P_2 se intersectan. Supongamos que se intersectan en dos puntos distintos; por P_1 tenemos que $l = m$; contradicción. Por lo tanto l y m sólo se intersectan en un punto.

□

Lema 2.2.1 *En un plano Proyectivo $\mathcal{P}$, dado un punto existe al menos una línea que no pasa por él.*

Demostración. Sea x un punto. Por P_3, tenemos tres puntos no-colineales. Si consideramos las líneas que pasan por estos tres puntos, obtenemos tres líneas no-concurrentes; x pasa en a lo más dos de ellas, por lo que existe al menos una línea que no pasa por x.

□

Lema 2.2.2 *En un plano Proyectivo $\mathcal{P}$, dadas dos líneas distintas, existe al menos dos puntos que no pertenecen a ninguna de ellas.*

Demostración. Sean l y m dos líneas distintas. Por la Proposición 2.2.1 se intersectan en un solo punto p, por P_4 cada línea tiene al menos tres puntos sean q y r puntos en l y m respectivamente, distntos a p, entonces por P_1 existe una única línea l_{qr} que contiene a q y r. Nuevamente, por P_4, l_{qr} tiene otro punto s distinto a q y r. Entonces s no pertenece a l ni a m ya que $l \neq l_{qr} \neq m$, además la línea l_{ps} tienen otro punto t que tampoco pertenece a l y m ya que $t \neq p = l \cap m$.

□

Corolario 2.2.1 *Existen cuatro puntos tales que no existe una línea que contenga a almenos tres de ellos.*

Demostración. Por el axioma P_3 existen tres puntos p, q y r no-colineales, consideramos las líneas $l = l_{pq}$ y $m = l_{pr}$, de la demostración del Lema anterior existen s y t tales que no pertenecen a l ni a m, y $s \in l_{qr}$ pero $t \notin l_{qr}$. Por lo tanto, los puntos buscados son $\{p, q, r, t\}$.

□

Proposición 2.2.2 *En un plano Proyectivo $\mathcal{P}$, todo par de línaes tiene la misma cantidad de puntos.*

Demostración. Sean l y m dos líneas distintas que se intersectan en p, y sea o un punto fuera de ellas. Por cada punto $x \in l$, con $x \neq p$, consideremos la línea l_{ox}, que es la única que pasa por o y x. Como o se encuentra fuera de m, l_{ox} intersecta a m en un solo punto y_x. Entonces la siguiente función está bien definida:

$$\begin{aligned} f : \ l \ &\longrightarrow m \\ p \ &\mapsto \ p \\ x \neq p &\mapsto \ y_x. \end{aligned}$$

Supongamos que $f(x_1)=f(x_2)$, esto es, $y_{x_1} = y_{x_2}$, quiere decir que $l_{ox_1} \cap m = l_{ox_2} \cap m$, por lo que $x_1 = x_2$, entonces f es inyectiva. Para ver que f es suprayectiva tomemos $y \in m$ y consideremos la única línea m_{oy} que pasa por o y y, como $o \notin l$ entonces $m_{oy} \cap l \neq \emptyset$. Sea $x = m_{oy} \cap l$, como m_{oy} es única $f(x) = y$. Entonces f es una biyección de los puntos de l a los puntos de m. Por lo tanto $|l| = |m|$.

□

Proposición 2.2.3 *En un plano Proyectivo $\mathcal{P}$; por cualquier punto pasa la misma cantidad de líneas. Más aún, la cantidad de líneas por un punto es igual a la cantidad de puntos en una línea.*

Demostración. Sea x un punto y l una línea que no pasa por x. Para cada $y \in l$ generamos la línea l_{xy} que pasa por x y y. Sea $\mathcal{L} = \{l_{xy} : y \in l\}$ es claro que $|\mathcal{L}| = |l|$. Ahora, sea m una línea que pasa por x, entonces $m \neq l$, por lo que existe $y \in m$ tal que $y = m \cap l$. Por lo tanto $m \in \mathcal{L}$. Entonces la cantidad de líneas que pasa por un punto es $|l|$.

□

A partir de este momento sólo nos ocuparemos de los planos Proyectivos *finitos*, es decir, con una cantidad finita de puntos. Es evidente que ésto implica que cada línea tiene un número finito de puntos y que hay un número finito de líneas. Hecha esta explicación y con las proposiciones anteriores obtenemos resultados interesantes.

Teorema 2.2.1 *Sea $\mathcal{P}$ un plano Proyectivo con P como su conjunto de puntos y L su conjunto de líneas. Entonces existe un número natural $n \geq 2$ tal que:*

i) $|L_p| = |l| = n + 1$, $\forall l \in L$ *y* $\forall p \in P$,

ii) $|P| = |L| = n^2 + n + 1$.

Al número n le llamamos ***orden*** *de $\mathcal{P}$.*

Demostración.

i) Sea l una línea y p un punto, por la Proposición 2.2.3 tenemos que $|L_p| = |l|$ y de P_4 sabemos que $|l| \geq 3$, entonces existe $n \geq 2$ tal que $|l| = n + 1$.

ii) Sea p un punto fijo. Por un lado tenemos que cada punto q en $P \setminus p$ está contenido en una única línea de L_p y cada línea en L_p tiene n puntos distintos de p, entonces $|P \setminus p| = |L_p|n = (n + 1)n = n^2 + n$, dado que $|P \setminus p| = |P| - 1$, implica que $|P| = n^2 + n + 1$. Por otro lado, cuando contamos a los puntos y las líneas que pasan por ellos $|P||L_p|$, estamos contando $|l|$ veces a cada línea, entonces;

$$|L| = \frac{|P||L_p|}{|l|} = |P|.$$

□

Corolario 2.2.2 *Un plano Proyectivo tiene al menos siete puntos.*

Demostración. Sea P el conjunto de puntos de un plano Proyectivo, por el Teorema anterior sabemos que $|P| = n^2 + n + 1$ para alguna $n \geq 2$, por lo que;

$$|P| \geq 2^2 + 2 + 1 = 7.$$

□

Proposición 2.2.4 *Existe un plano Proyectivo con siete puntos.*

Demostración. Basta con mostrarlo.
$P = \{1, 2, 3, 4, 5, 6, 7\}$,
$L = \{\{1, 2, 3\}, \{1, 4, 5\}, \{1, 6, 7\}, \{2, 5, 7\}, \{3, 4, 7\}, \{3, 5, 6\}, \{2, 4, 6\}\}$.

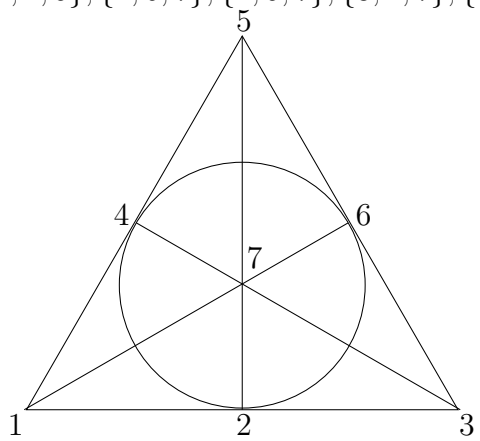


Figura 2.2: Plano Proyrectivo con 7 puntos.

□

Notamos que hay una estrecha relación entre planos Afínes y planos Proyectivos para asimilarlo de mejor manera veamos como podemos generar uno a partir del otro.

Definición 2.2.2 *Sea $\mathcal{A}$ un plano Afín y l_∞ la línea que consiste de todos los puntos al infinito. Definimos la* ***proyectivización*** *de $\mathcal{A}$ como el espacio $\mathcal{P}_\mathcal{A}$ formado de la siguiente manera:*
$P_\mathcal{A} = \{\textit{puntos de } \mathcal{A}\} \cup \{\textit{puntos al infinito de } \mathcal{A}\}$,
$L_\mathcal{A} = \{l \cup [l] : l \in \mathcal{A}\} \cup l_\infty$.

Teorema 2.2.2 *Sea $\mathcal{A}$ un plano Afín, entonces $\mathcal{P}_\mathcal{A}$ es un plano Proyectivo.*

Demostración. Veamos que efectivamente $\mathcal{P}_\mathcal{A}$ cumple los axiomas de un plano Proyectivo:

P_1 sean p y q puntos distintos en $\mathcal{P}_\mathcal{A}$: Si p y q están en $\mathcal{A}$, por A_1 existe una y sólo una línea que los contiene. Si $p \in \mathcal{A}$ y $q = [l]$, por A_2 existe una y sólo una línea m paralela a l que pasa por p. Entonces $m \cup [l]$ es la única línea que contiene a p y q. Si son puntos al infinito, la única línea que los contiene es la línea al infinito.

P_2 Si l y m pertenecen a $\mathcal{A}$ y no son paralelas; se intersectan. Si l y m pertenecen a $\mathcal{A}$ y son paralelas, entonces $[l] = [m]$ por lo que también se intersectan en este caso. Si $l \in \mathcal{A}$ y m es la línea al infinito, entonces l y m se intersectan en $[l]$.

P_3 Por A_3 existen tres puntos no-colineales en $\mathcal{A}$ y ninguno de ellos pertenece a l_∞, por lo que siguen siendo no-colineales en $\mathcal{P}_\mathcal{A}$.

P_4 En $\mathcal{A}$; por la Proposición 2.1.3 toda línea contiene al menos dos puntos, entonces en $\mathcal{P}_\mathcal{A}$; toda línea contiene al menos tres puntos ya que a cada una de ellas le agregamos su punto al infinito correspodiente.

□

Ejemplo 4 *Proyectivizando el plano Afín con cuatro puntos obtenenos el plano Proyectivo con siete puntos.*

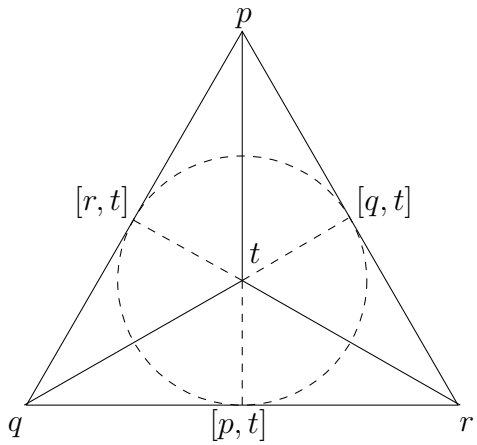


Figura 2.3: Proyectivización del Plano Afín con 4 puntos.

Definición 2.2.3 *Sea $\mathcal{P}$ un plano Proyectivo con P como su conjunto de puntos, L como su conjunto de líneas y l una de sus líneas. Definimos la* ***afinización*** *de $\mathcal{P}$ con respecto a l como el espacio $\mathcal{A}_{\mathcal{P}_l} = (L_l, P_l)$, donde;*

$P_l = P \setminus l$

$L_l = \{m_l = m \setminus (m \cap l) : m \in L \setminus l\}$.

Teorema 2.2.3 *Sea $\mathcal{P}$ un plano Proyectivo y l una de sus líneas, entonces $\mathcal{A}_{\mathcal{P}_l}$ es un plano Afín.*

Demostración. Verifiquemos que efectivamente cumple con los axiomas de un plano Afín:

A_1 Por P_1 tenemos que cualquier par de puntos están en una única línea y eso es válido para los puntos P_l y las líneas L_l.

A_2 Sea $p \in P_l$ y $m \in L_l$. De la Proposición 2.2.1 tenemos que l y m se intersectan en un único punto q, y de P_1 sabemos que la línea l_{pq}, que contiene a p y q, es única. Además $m \cap l_{pq} = q \in l$ por lo que en $\mathcal{A}_{\mathcal{P}_l}$, sus respectivas líneas asociadas son paralelas.

A_3 Por el Corolario 2.2.1 tenemos que existen cuatro puntos $\{p, q, r, s\}$ tales que no existe una línea que contenga a almenos tres de ellos, por lo que $|\{p, q, r, s\} \cap l| = 0, 1$ ó 2. Si es 0 ó 1 ya tenemos tres puntos no-colineales en $\mathcal{A}_{\mathcal{P}_l}$. Si es 2 por el Lema 2.2.2 existe un punto fuera de l y la línea que pasa por los otros dos puntos, por lo que tenemos tres puntos no-colineales en $\mathcal{A}_{\mathcal{P}_l}$.

□

Teorema 2.2.4 *Dado un plano Proyectivo $\mathcal{P}$ existe un plano Afín $\mathcal{A}$ tal que $\mathcal{P} = \mathcal{P}_{\mathcal{A}}$.*

Demostración. Sea $\mathcal{A} = \mathcal{A}_{\mathcal{P}_l}$ para alguna $l \in \mathcal{P}$. Entonces l es la línea al infinito en $\mathcal{A}$. Y así; $\mathcal{P} = \mathcal{P}_{\mathcal{A}}$.

□

Teorema 2.2.5 *Dado un plano Afín $\mathcal{A}$ existe un plano Proyectivo $\mathcal{P}$ tal que $\mathcal{A} = \mathcal{A}_{\mathcal{P}_l}$ para alguna línea l en $\mathcal{P}$.*

Demostración. Sea $\mathcal{P} = \mathcal{P}_{\mathcal{A}}$, entonces, $\mathcal{A} = \mathcal{A}_{\mathcal{P}_{l_\infty}}$.

□

Debido a esta relación tan fuerte del plano Proyectivo y del plano Afín; definimos el **orden** de un plano Afín como el orden del plano Proyectivo asociado a él.

Teorema 2.2.6 *Sea $\mathcal{A}$ un plano Afín de orden n con $P_{\mathcal{A}}$ como su conjunto de puntos y $L_{\mathcal{A}}$ como su conjunto de líneas. Entonces:*

i) $|l| = n \ \forall l \in L_{\mathcal{A}}$,

ii) $|L_p| = n + 1 \ \forall p \in P_{\mathcal{A}}$,

iii) $|[l]| = n \ \forall l \in L_{\mathcal{A}}$,

iv) $|\{[l]\}_{l \in L_{\mathcal{A}}}| = n + 1$,

v) $|P_{\mathcal{A}}| = n^2$,

vi) $|L_{\mathcal{A}}| = n^2 + n$.

Demostración. Consideramos a $\mathcal{P}_{\mathcal{A}}$ y el Teorema 2.2.1. Entonces para llegar de $\mathcal{P}_{\mathcal{A}}$ a $\mathcal{A}$, quitamos la línea l_∞ (vi) con $n+1$ puntos $(iv$ y $v)$, ésto hace que a cada línea, distinta de l_∞, se le quite sólo el punto en el que se intersectan (i). A los puntos fuera de l_∞ no les afectamos su incidencia (ii) excepto a los puntos al infinito que les quitamos l_∞ (iii).

□

Los siguientes ejemplos son muy importantes y motivan definiciones más amplias.

Ejemplo 5 *Sea $\mathbb{F}$ un campo, consideramos el espacio $\mathcal{A}$ donde sus puntos son $P = \mathbb{F}^2$ y cada línea l es de la forma*

$l = [a, b, c] = \{(x, y) \in \mathbb{F}^2 : ax + by + c = 0, \quad con \quad (a, b, c) \neq (0, 0, 0)\}$. *Nótese que para toda $\lambda \in \mathbb{F} \setminus \{0\}$; $[a, b, c] = [\lambda a, \lambda b, \lambda c]$. Además, a y b no pueden ser cero al mismo tiempo porque c sería cero. Y sabemos que el sistema de ecuaciones*

$$ax + by = c,$$
$$a'x + b'y = c',$$

tiene solución única si y sólo si (a, b) y (a', b') son linealmente independientes, es decir, $[a, b, c]$ y $[a', b', c']$ son paralelas si y sólo si
$a' = \lambda a$ y $b' = \lambda b$ con $\lambda \in \mathbb{F} \setminus \{0\}$. Lo que acabamos de demostrar es;

Lema 2.2.3 *Dos líneas $[a, b, c]$ y $[a', b', c']$ son paralelas si y sólo si*

1) $a = 0$ *entonces* $a' = 0$,

ó

2) $a \neq 0$ *entonces* $a' \neq 0$ *y* $\dfrac{b}{a} = \dfrac{b'}{a'}$.

Demostremos que $\mathcal{A}$ *es un plano Afín:*

A_1 *Sean* $\bar{x}_1 = (x_1, y_1)$ *y* $\bar{x}_2 = (x_2, y_2)$ *dos puntos diferentes en* $\mathcal{A}$*, entonces la línea* $[y_2 - y_1, x_1 - x_2, y_1(x_1 - x_2) + x_1(y_2 - y_1)]$ *pasa por* $\bar{x}_1$ *y por* $\bar{x}_2$.

Ahora si $\bar{x}_1$ *y* $\bar{x}_2$ *pertenecen a dos líneas* $l_1 = [a, b, c]$ *y* $l_2 = [a', b', c']$ *entonces tenemos las siguientes igualdades:*

i) $ax_1 + by_1 + c = 0$, *ii)* $a'x_1 + b'y_1 + c' = 0$,
iii) $ax_2 + by_2 + c = 0$, *iv)* $a'x_2 + b'y_2 + c' = 0$.

Entonces,

v) $a(x_1 - x_2) + b(y_1 - y_2) = 0$,

vi) $a'(x_1 - x_2) + b'(y_1 - y_2) = 0$.

Si $a = 0 \Longrightarrow b \neq 0 \Longrightarrow y_1 = y_2 \Longrightarrow a' = 0 \Longrightarrow b' \neq 0$*, por lo que siempre existe* $\lambda \in \mathbb{F} \setminus \{0\}$ *tal que* $b' = \lambda b$*, al multiplicar por* λ *en i) resulta que* $\lambda b y_1 + \lambda c = 0$ *y de ii) implica que* $c' = \lambda c$*. Por lo tanto* $l_1 = l_2$*. Hacemos el mismo razonamiento si* $b = 0$*,* $a' = 0$ *ó* $b' = 0$ *y obtendremos las mismas conclusiones.*

En el caso de que a, b, a' *y* b' *sean todas distintas de cero; como* $\bar{x}_1$ *y* $\bar{x}_2$ *son diferentes, sin pérdida de generalidad podemos suponer que* $x_1 \neq x_2$*, entonces, sea* $\lambda \in \mathbb{F} \setminus \{0\}$ *tal que;* $b' = \lambda b$*, entonces de v) y de vi) tenemos que* $(a' - \lambda a)(x_1 - x_2) = 0 \Longrightarrow a' = \lambda a$ *y por i) y ii)* $\Longrightarrow c' = \lambda c$*, entonces,* $l_1 = l_2$.

Por lo tanto dos puntos pertenecen a una única línea.

A_2 *Sean* $l = [a, b, c]$ *una línea y* $\bar{x}_1 = (x_1, y_2)$ *un punto, entonces la línea* $l' = [a, b, -(ax_1 + bx_2)]$ *es paralela a* l *y pasa por* $\bar{x}_1$*. Si suponemos que otra línea* $l'' = [a''.b'', c'']$ *es paralela a* l *(y a* l'*) y pasa por* $\bar{x}_1$*, entonces existe una* $\lambda \in \mathbb{F} \setminus \{0\}$ *tal que* $a'' = \lambda a'$ *y* $b'' = \lambda b'$*; y como pasan por* $\bar{x}_1$*;*

$a'x_1 + b'y_1 + c' = 0$,

$a''x_1 + b''y_1 + c'' = 0$,

resultando que $c'' = \lambda c'$ *y* $l' = l''$.

A_3 *consideremos los puntos* $\bar{x}_1 = (1,0), \bar{x}_2 = (0,1)$ *y* $\bar{x}_3 = (1,1)$. *Si existiera* $l = [a,b,c]$ *que pasa por* $\bar{x}_1, \bar{x}_2$ *y* $\bar{x}_3$, *tendriía que suceder;*

1) $a1 + b0 + c = 0 \Longrightarrow a + c = 0$,

2) $a0 + b1 + c = 0 \Longrightarrow b + c = 0$,

3) $a1 + b1 + c = 0 \Longrightarrow a + b + c = 0$,

de 1) *y* 3) *implica que* $b = 0$ *y de* 2) *y* 3) *implica que* $a = 0$ *contradiciendo que* l *sea una línea. Por lo tanto, los puntos* $\bar{x}_1, \bar{x}_2$ *y* $\bar{x}_3$ *son no-colineales.*

Por lo tanto $\mathcal{A}$ *es un plano Afín.*

Ejemplo 6 *Sea* $\mathbb{F}$ *un campo, consideramos el espacio* $\mathcal{P}$ *donde sus puntos* P *son el haz de rectas en* $\mathbb{F}^3$ *por el origen, sin el origen, y sus líneas* L *son los planos en* $\mathbb{F}^3$ *que pasan por el origen, sin el origen. Reprecentamos a los puntos de* $\mathcal{P}$ *por medio de coordenadas que dependen de las rectas por el origen en* $\mathbb{F}^3$ *de la siguiente manera: en* $\mathbb{F}^3$, *sea* l *una recta por el origen y* $(x_1, x_2, x_3) \neq (0,0,0)$ *un vector en* l, *entonces, cualquier otro elemento en* l *se puede ver como múltiplo de* (x_1, x_2, x_3), *es decir,* $(0,0,0) \neq (x'_1, x'_2, x'_3) \in l \Leftrightarrow \exists \lambda \in \mathbb{F} \setminus 0$ *tal que* $x'_i = \lambda x_i$ *para* $i = 1,2,3$. *Entonces al punto que representa a la recta* l, *le asignamos las* ***coordenadas homogéneas*** $[x_1 : x_2 : x_3]$, *y a cada línea en* $\mathcal{P}$, *le asignamos coordenadas por medio de los parámetros de la ecuación del plano que representan; sea* π *un plano por el origen en* $\mathbb{F}^3$, *entonces* π *tienen una ecuación de la forma* $ax_1 + bx_2 + cx_3 = 0$ *con* $(a,b,c) \neq (0,0,0)$, *por lo que a la línea que representa a* π *le asignamos las coordenadas* $[a : b : c]$. *En estos términos tenemos que:*

$\mathcal{P} = \mathbb{F}^3 \setminus \{\bar{0}\} / \sim$ *donde* $\bar{u} \sim \bar{v} \Leftrightarrow \bar{u} = \lambda \bar{v}$, *para alguna* $\lambda \in \mathbb{F} \setminus 0$

$P = \{[x_1 : x_2 : x_3] : (x_1, x_2, x_3) \in \mathbb{F}^3 \setminus (0,0,0)\}$,

$L = \{[a : b : c] : (a,b,c) \in \mathbb{F}^3 \setminus (0,0,0)\}$.

Demostremos que $\mathcal{P}$ *es un plano Proyectivo.*

P_1 *En* $\mathbb{F}^3$, *se sabe que por cualquier par de rectas por el origen distintas, pasa un único plano y es justo el generado por cualquier par de vectores representantes, por esta razón en* $\mathcal{P}$ *por dos puntos distintos pasa una única línea.*

P_2 *Análogamente, en* $\mathbb{F}^3$*, se sabe que cualquier par de planos por el origen distintos* $[a:b:c]$ *y* $[a':b':c']$*, se intersectan en una única recta por el origen y es justo la generada por* $(a,b,c)\times(a',b',c')$*.*

P_3 *Sean* $a=[1:0:0]$*,* $b=[0:1:0]$ *y* $c=[1:1:1]$*, si suponemos que* a*,* b *y* c *pertenecen a la línea* $l=[a,b,c]$*, entonces se tiene que satisfacer el siguiente sistema de ecuaciones;*

1) $a1+b0+c0=0\Longrightarrow a=0$,

2) $a0+b1+c0=0\Longrightarrow b=0$,

3) $a1+b1+c1=0\Longrightarrow a+b+c=0\Longrightarrow c=0$.

Por lo tanto, a*,* b *y* c *son no-colineales.*

P_4 *Como* $\mathbb{F}$ *es un campo tiene al menos dos puntos (el neutro aditivo y el neutro multiplicativo), entonces, en* $\mathbb{F}^3$ *cada plano tiene al menos cuatro puntos, por lo que cada línea de* $\mathcal{P}$ *tiene almenos tres puntos.*

Por lo tanto, $\mathcal{P}$ *es un plano Proyectivo.*

Además, teniendo en cuenta el Lema 2.2.3 podemos asociarle a cada línea $[a:b:c]$ su respectivo punto al infinito $P_{\{a,b\}}$;

$$P_{a,b}:=\begin{cases}[\frac{b}{a}] & \text{si } a\neq 0,\\ \infty & \text{si } a=0.\end{cases}$$

Teorema 2.2.7 *Sea* $\mathcal{A}$ *el plano Afín del Ejemplo 5 y* $\mathcal{P}$ *el plano Proyectivo del Ejemplo 6, entonces,* $\mathcal{P}_{\mathcal{A}}$ *es isomorfo a* $\mathcal{P}$*.*

Demostración. Sea $\phi:\mathcal{P}\longrightarrow\mathcal{P}_{\mathcal{A}}$

$$\phi([x_1:x_2:x_3]):=\begin{cases}\left(\frac{x_1}{x_3},\frac{x_2}{x_3}\right) & \text{si } x_3\neq 0,\\ P_{x_2,-x_1} & \text{si } x_3=0.\end{cases}$$

Chequemos que;

(i) ϕ está bien definida; sea $(x_1,x_2,x_3)\in\mathbb{F}^3$,

$$\text{si } x_3\neq 0,\text{ entonces } \left(\frac{\lambda x_1}{\lambda x_3},\frac{\lambda x_2}{\lambda x_3}\right)=\left(\frac{x_1}{x_3},\frac{x_2}{x_3}\right),\text{ para toda } \lambda\in\mathbb{F}\setminus\{0\},$$

si $x_3 = 0$ y

$x_2 \neq 0$ entonces $\dfrac{-\lambda x_1}{\lambda x_2} = \dfrac{-x_1}{x_2}$, para toda $\lambda \in \mathbb{F} \setminus \{0\}$,
$x_2 = 0$ entonces $\lambda x_2 = 0$, para toda $\lambda \in \mathbb{F} \setminus \{0\}$.

(ii) ϕ es inyectiva; sean $[x_1 : x_2 : x_3]$ y $[y_1 : y_2 : y_3]$ tales que:
$\phi([x_1 : x_2 : x_3]) = \phi([y_1 : y_2 : y_3])$, entonces $y_3 = \lambda x_3$ con $\lambda \neq 0$,

si $x_3 \neq 0$, como $\left(\dfrac{x_1}{x_3}, \dfrac{x_2}{x_3}\right) = \left(\dfrac{y_1}{y_3}, \dfrac{y_2}{y_3}\right), \Longrightarrow \dfrac{x_1}{x_3} = \dfrac{y_1}{\lambda x_3}$ y $\dfrac{x_2}{x_3} = \dfrac{y_2}{\lambda x_3}$,
entonces $y_1 = \lambda x_1$ y $y_2 = \lambda x_2$, por lo que
$[x_1 : x_2 : x_3] = [y_1 : y_2 : y_3]$,

si $x_3 = 0$, entonces, $\phi([x_1 : x_2 : x_3]) = \phi([y_1 : y_2 : y_3]) = P_{a,b}$;

si $a \neq 0$, entonces $\left(\dfrac{-x_1}{x_2}\right) = \left(\dfrac{b}{a}\right) = \left(\dfrac{-y_1}{y_2}\right)$ entonces $y_1 = \lambda x_1$,
$y_2 = \lambda x_2$ y $[x_1 : x_2 : x_3] = [y_1 : y_2 : y_3]$,
si $a = 0$, entonces $\phi([x_1 : x_2 : x_3]) = \phi([y_1 : y_2 : y_3]) = \infty$, por
tanto $x_2 = y_2 = y_3 = x_3 = 0$ y así, $[x_1 : x_2 : x_3] = [y_1 : y_2 : y_3]$.

(iii) ϕ es suprayectiva, por que;

si $(x, y) \in \mathcal{A}$, entonces $\phi([x : y : 1]) = \left(\dfrac{x}{1}, \dfrac{y}{1}\right) = (x, y)$,

si $P_{a,b}$ es un punto al infinito asociado a una línea $[a : b : c]$, entonces
$(a, b) \neq (0, 0)$, luego, $\phi([-b : a : 0]) = P_{a,b}$.

Nos falta verificar que ϕ manda líneas de $\mathcal{P}$ en líneas de $\mathcal{P}_{\mathcal{A}}$. Sea $l = [a : b : c]$ una línea en $\mathcal{P}$, entonces cualquier punto $[x_1 : x_2 : x_3]$ que pertenezca a l tiene que satisfacer:

$$ax_1 + bx_2 + cx_3 = 0.$$

Si $(a, b) \neq (0, 0)$,entonces las imágenes de los puntos $[x_1 : x_2 : x_3]$ que pertenecen a l, con $x_3 \neq 0$, satisfacen la ecuación

$$a\left(\frac{x_1}{x_3}\right) + b\left(\frac{x_2}{x_3}\right) + c = 0,$$

y el $[x_1 : x_2 : x_3]$ que pertenece a l, con $x_3 = 0$, es justamente $[-b : a : 0]$ y como $\phi([-b : a : 0]) = P_{a,b}$, es colineal con los puntos de la línea $ax + by + c = 0$.

Si $(a, b) = (0, 0)$, entonces $c \neq 0$ y la línea l tiene la ecuación $x_3 = 0$. Por lo tanto, l , bajo ϕ, tiene como imagen a la línea al infinito de $\mathcal{A}$.

Entonces, ϕ manda líneas de $\mathcal{P}$ en líneas de $\mathcal{P}_{\mathcal{A}}$. Como por cualquier par de puntos distintos p_1 y p_2 de $\mathcal{P}_{\mathcal{A}}$ pasa una única línea l y ϕ es biyectiva, la imagen de la única línea, en $\mathcal{P}$, que pasa por las imágenes inversas de p_1 y p_2 es justamente l. Por lo tanto ϕ es un isomorfismo de $\mathcal{P}$ a $\mathcal{P}_{\mathcal{A}}$.

□

Sólo por mensionarlo, cuando tomamos a $\mathbb{F} = \mathbb{R}$, nuestro plano Afín es el plano Euclidiano y a la proyectivización se le conoce como **Plano Proyectivo Real** $\mathbb{P}$.

Otro caso particular, de los Ejemplos 5 y 6, es cuando $\mathbb{F}$ es finito. En este contexto, generalizamos un poco más la definición de plano Afín y plano Proyectivo.

2.3. Espacio Afín

Consideramos el espacio vectorial $\mathbb{F}_q^n$, donde $\mathbb{F}_q$ es un campo finito con q elementos y q es un número primo elevado a alguna potencia. A los vectores de $\mathbb{F}_q^n$ les nombramos *puntos afines*, y si S es cualquier subespacio de $\mathbb{F}_q^n$ con dimensión i; un *i-plano afín* es el traslado $\bar{v} + S$ para cualquier $\bar{v} \in \mathbb{F}_q^n$; por lo que un punto afín es un 0-plano, un 1-plano es una *línea afín*,..., un $(n-1)$-plano es un **hiperplano afín**. A todos los i-planos afines, con $i = 0, 1, ..., n-1$, los definimos como **subespacios afines**. Decimos que dos subespacios afines, $(\bar{v} + S_1)$ y $(\bar{u} + S_2)$, son *paralelos* si $S_1 \subseteq S_2$ o $S_2 \subset S_1$. Entonces definimos al **Espacio Afín** $AG(n, q)$ de dimensión n sobre $\mathbb{F}_q$, como el conjunto de subespacios afines, con la estructura de incidencia determinada por la contención y la relación de paralelismo dada para subespacios afines.

Definición 2.3.1 *Sean V_j y V_k dos subespacios afines en el $AG(n, q)$, de dimensión j y k repectivamente, definimos al subespacio afín en el $AG(n, q)$ generado por V_j y V_k, denotado por $\langle V_j, V_k \rangle$, como el i-plano afín V_i del $AG(n, q)$ más pequeño que contiene a V_j y V_k.*

Definición 2.3.2 *Sea V_m un m-plano afín en el $AG(n, q)$, definimos el espacio afín generado por V_m, denotado como $AG(V_m)$, como el conjunto de todos los i- planos afines del $AG(n, q)$ contenidos en V_m, con la estructura de incidencia dada por la contención y la relación de paralelismo en el $AG(n, q)$.*

Definición 2.3.3 *Sean V y W dos espacios vectoriales de dimensión finita sobre el mismo campo $\mathbb{F}_q$. Decimos que el $AG(V)$ y el $AG(W)$ son* ***isomorfos*** *si existe una transformación biyectiva $\phi : AG(V) \to AG(W)$, tal que, si $V_1, V_2 \in AG(V)$, entonces $V_1 \subseteq V_2$ si y sólo si $\phi(V_1) \subseteq \phi(V_2)$. En tal caso a ϕ le llamamos* ***isomorfismo****. Y en el caso de que $V = W$ diremos que ϕ es un* ***automorfismo*** *de V.*

Proposición 2.3.1 *Sean V_m y W_m dos m-planos afines del $AG(n, q)$ entonces, el $AG(V_m)$ es isomorfo al $AG(W_m)$.*

Demostración. Como V_m es un m-plano afín; $V_m = \bar{u} + S_1$, donde S_1 es un subespacio vectorial de $\mathbb{F}_q^n$ con dimensión m, en consecuencia cualquier i-plano afín U' contenido en $AG(V_m)$ es de la forma $U' = \bar{u}+U$ con U un i-plano afín en S_1, por tanto $AG(V_m)$ es isomorfo a $AG(S_1)$. Identicamente $AG(W_m)$ es isomorfo a $AG(S_2)$, donde $V_m = \bar{v} + S_1$ y S_2 es un subespacio vectorial de $\mathbb{F}_q^n$ con dimensión m. Además, como S_1 y S_2 son subespacios de dimensión m cada uno tiene una base con m vectores; sean $B_1 = \{a_1, a_2, ..., a_m\}$ base de S_1 y $B_2 = \{b_1, b_2, ..., b_m\}$ base de S_1, entonces si consideramos la función

$$\begin{array}{rcl} \phi : & S_1 & \longrightarrow S_2 \\ & \sum_{i=1}^{m} \lambda_i a_i & \mapsto \sum_{i=1}^{m} \lambda_i b_i. \end{array}$$

es claro que ϕ es una función lineal y biyectiva.

Ahora si tenemos un k-plano afín U en S_1, entonces $U = \bar{u}+V$, donde V es un subespacio de S_1 con dimensión k, entonces existen $a_{v1}, a_{v2}, ..., a_{vk} \in B_1$ tal que $V = \langle a_{v1}, a_{v2}, ..., a_{vk}\rangle$, como ϕ es lineal el conjunto $\{\phi(a_{v1}), \phi(a_{v2}), ..., \phi(a_{vk})\}$ es linealmente independiente en S_2. Entonces si

$$\begin{array}{rcl} \Phi : & AG(S_1) & \longrightarrow AG(S_2) \\ & \bar{u} + \langle a_{v1}, a_{v2}, ..., a_{vk}\rangle & \mapsto \phi(\bar{u}) + \langle \phi(a_{v1}), \phi(a_{v2}), ..., \phi(a_{vk})\rangle, \end{array}$$

es inmediato verificar que Φ es un isomorfismo.

Por lo tanto $AG(V_m)$ y $AG(W_m)$ son isomorfos.

□

Corolario 2.3.1 *Sea V_i un m-plano afín en el $AG(n, q)$ entonces, el $AG(V_m)$ isomorfo al $AG(m, q)$ sobre el mismo campo $\mathbb{F}_q$.*

Demostración. Como V_m es un m-plano afín, $V_m = \bar{v}+S$, con S un subespacio de $\mathbb{F}_q^n$ con dimensión m. De la demostración anterior se infiere que $AG(V_m)$ es isomorfo a $AG(S)$ que a su vez es isomorfo a $AG(\mathbb{F}_q^m) = AG(m,q)$.

□

Por este motivo, si V_m es un m-plano afín en el $AG(n,q)$, decimos que el $AG(V_m)$ es un $AG(m,q)$ contenido en el $AG(n,q)$.

Teorema 2.3.1 *Sea $\mathbb{F}_q^n$ un espacio vectorial, entonces el número de subespacios de $\mathbb{F}_q^n$ de dimensión i, con $i = 1, 2, ..., n$, está determinado por el* ***polinomio de Gauss****:*

$$\mathcal{G}(n,i) := \prod_{k=0}^{i-1} \frac{q^{n-k}-1}{q^{i-k}-1}.$$

Demostración. Un subespacio de dimensión i se determina por una base de i vectores linealmente independientes, para escoger los vectores; tenemos (q^n-1) para escoger el primero distinto de $\bar{0}$, el segundo no puede ser $\bar{0}$ ni estar en el subespacio generado por el primero, entonces tenemos (q^n-q) para el segundo, y en general el k-ésimo vector no puede estar en el subespacio generado por los $k-1$ vectores anteriores entonces tiene (q^n-q^{k-1}). Por lo tanto, podemos escoger una base con i elementos linealmente independientes de $(q^n-1)(q^n-q)\cdots(q^n-q^{i-1})$ formas. Pero cada subespacio de dimensión i se puede generar con distintas bases. Para escoger una base dentro de un subespacio de dimensión i, tenemos (q^i-1) para escoger el primero distinto de $\bar{0}$, el segundo no puede ser $\bar{0}$ ni estar en el subespacio generado por el primero, entonces tenemos (q^i-q) para el segundo, y en general el k-ésimo vector no puede estar en el subespacio generado por los $k-1$ vectores anteriores entonces tiene (q^i-q^{k-1}). Por lo que tenemos $(q^i-1)(q^i-q)\cdots(q^i-q^{i-1})$ bases distintas dentro de un espacio de dimensión i. Entonces el número de subespacios de dimensión i,con $i = 1, 2, ...n$, es:

$$\frac{(q^n-1)(q^n-q)\cdots(q^n-q^{i-1})}{(q^i-1)(q^i-q)\cdots(q^i-q^{i-1})} = \frac{(q^{n-0}-1)q(q^{n-1}-1)\cdots q^{i-1}(q^{n-(i-1)}-1)}{(q^{i-0}-1)q(q^{i-1}-1)\cdots q^{i-1}(q^{i-(i-1)}-1)}$$

$$= \prod_{k=0}^{i-1} \frac{q^{n-k}-1}{q^{i-k}-1}.$$

□

Teorema 2.3.2 *El número de Espacios Afines $AG(m,q)$ en un Espacio Afín $AG(n,q)$ es:*

$$q^{n-m}\mathcal{G}(n,m) = q^{n-m}\prod_{i=0}^{m-1}\frac{q^{n-i}-1}{q^{m-i}-1}.$$

Demostración. En $\mathbb{F}_q^n$, podemos trasladar a un subespacio vectorial de dimensión m de q^n maneras, pero hay q^m vectores que nos generan el mismo traslado (ya que q^m es la cantidad de puntos en el subespacio), por lo que hay $\frac{q^n}{q^m} = q^{n-m}$ formas distintas de trasladar a cada subespacio vectorial de dimensión m. Por lo tanto, el número de Espacios Afines $AG(m,q)$, es:

$$q^{n-m}\mathcal{G}(n,m).$$

□

Teorema 2.3.3 *Sean l, m y n números naturales tales que $l < m < n$. Entonces, dentro de un $AG(n,q)$, el número de $AG(m,q)$ que contienen a un $AG(l,q)$ dado es:*

$$\mathcal{G}(n-l, m-l) = \prod_{i=l+1}^{m}\frac{q^{n-i+1}-1}{q^{m-i+1}-1}.$$

Demostración. Sea $\bar{v}+U$ un l-plano afín, entonces cada m-plano afín que lo contenga se puede escribir como $\bar{v}+V$, donde U es subespacio vectorial de V. Por lo que el número de m-planos afines que contienen al l-plano dado es igual al número de $(m-l)$-subespacios en un $(n-l)$-subespacio.

□

Teorema 2.3.4 *La estructura de incidencia conformada por los puntos y las líneas afines del $AG(n,3)$ es un $STS(3^n)$ para toda $n \in \mathbb{N}$.*

Demostración. Considerando el espacio vectorial $\mathbb{F}_p^n$, con $p = 3$, y el $AG(n,3)$, tenemos que cada línea afín tiene 3 puntos, y como los puntos en el $AG(n,3)$ son vectores de $\mathbb{F}_3^n$; cualquier línea que pase por dos puntos diferentes está contenida en el subespacio de $\mathbb{F}_3^n$, generado por los vectores correspondientes a esos puntos; si es una línea, esa es la única que pasa por esos dos puntos, y si es un plano, ese plano es isomorfo al $AG(2,3)$ y, por el Ejemplo 5; el $AG(2,3)$ es un plano Afín, y en él existe una única línea que pasa por dos puntos diferentes. Además, $|AG(n,3)| = |\mathbb{F}_3^n| = 3^n$. Entonces los puntos y líneas afines de $AG(n,3)$ son un $STS(3^n)$.

□

Corolario 2.3.2 *Sea V un i-plano afín del $AG(n,3)$ con $0 < i < n$, entonces, la subestructura de incidencia conformada por los puntos y las líneas afines del $AG(n,3)$ contenidas en V, es un $STS(3^i)$.*

Demostración. De la Proposición 2.3.1; el $AG(V)$ es isomorfo al $AG(i,q)$, y por el Teorema anterior tenemos el resultado.

□

2.4. Espacio Proyectivo

Consideremos el espacio vectorial $\mathbb{F}_q^{n+1}$. También tomemos en cuenta la siguiente relación de equivalencia en $\mathbb{F}_q^{n+1} \setminus \{\bar{0}\}$:

$$\bar{u} \sim \bar{v} \Leftrightarrow \bar{u} = \lambda\bar{v}, \text{ para alguna } \lambda \in \mathbb{F}_q \setminus 0.$$

A las clases de equivalencia les llamamos *puntos proyectivos*. Estos puntos son los subespacios de dimensión 1, sin el $\bar{0}$, de $\mathbb{F}_q^{n+1}$. A los subespacios de dimensión 2, sin el $\bar{0}$, en $\mathbb{F}_q^{n+1}$, les llamamos *líneas proyectivas*, a los de dimensión n, sin el $\bar{0}$, les llamamos **hiperplanos proyectivos**, y en general a los subespacios de dimensión $i+1$, sin el $\bar{0}$, les llamamos *i-planos proyectivos*. A todos los i-planos proyectivos, con $i = 1, 2, ..., n$, los definimos como **subespacios proyectivos**. Entonces definimos al **Espacio Proyectivo** $PG(n,q)$ como el cociente $\mathbb{F}_q^{n+1} \setminus \{\bar{0}\}/\sim$, cuyos elementos son los subespacios proyectivos, junto con la estructura de incidencia que determina la contención. La dimensión de $PG(n,q)$ se define como n, igualmente se define la **dimensión proyectiva** de un subespacio proyectivo determinado por un i-plano proyectivo; como i.

Definición 2.4.1 *Sean V_j y V_k dos subespacios proyectivos en $PG(n,q)$, de dimensión j y k respectivamente, definimos al subespacio proyectivo en $PG(n,q)$ generado por V_j y V_k, denotado por $\langle V_j, V_k \rangle$, como el i-plano proyectivo V_i de $PG(n,q)$ más pequeño que contiene a V_j y V_k.*

Definición 2.4.2 *Sea V_m un m-plano proyectivo en $PG(n,q)$, definimos al espacio proyectivo generado por V_m, denotado como $PG(V_m)$, como el conjunto de todos los i- planos proyectivos de $PG(n,q)$ contenidos en V_m, con la estructura de incidencia determinada por la contención.*

Definición 2.4.3 *Sean V y W dos espacios vectoriales de dimensión finita sobre el mismo campo $\mathbb{F}_q$. Decimos que el $PG(V)$ y el $PG(W)$ son **isomorfos** si existe una transformación biyectiva $\psi : PG(V) \to PG(W)$, tal que, si $V_1, V_2 \in PG(V)$, entonces $V_1 \subseteq V_2$ si y sólo si $\psi(V_1) \subseteq \psi(V_2)$. En tal caso a ψ le llamamos **isomorfismo**. Y en el caso de que $V = W$ diremos que ψ es un **automorfismo** de V.*

Proposición 2.4.1 *Sean V_m y W_m dos m-planos proyectivos del $PG(n, q)$ entonces, el $PG(V_m)$ es isomorfo al $PG(W_m)$.*

Demostración. Como V_m y W_m m-planos proyectivos, entonces V_m y W_m son subespacios vectoriales de $\mathbb{F}_q^{n+1}$ sin el $\bar{0}$ con dimensión $m+1$, cada uno tiene una base con $m+1$ vectores: sean $B_1 = \{a_1, a_2, ..., a_{m+1}\}$ y $B_2 = \{b_1, b_2, ..., b_{m+1}\}$ sus respectivas bases, entonces es obvio que

$$\begin{array}{rcl} \psi : V_m & \longrightarrow & W_m \\ \sum_{i=1}^{m+1} \lambda_i a_i & \mapsto & \sum_{i=1}^{m+1} \lambda_i b_i. \end{array}$$

es una función lineal y biyectiva.

Ahora, si V es un k-plano proyectivo en V_m, entonces existen $a_{v1}, a_{v2}, ..., a_{v(k+1)} \in B_1$, tal que $V = \langle a_{v1}, a_{v2}, ..., a_{v(k+1)} \rangle \setminus \{\bar{0}\}$; como ψ es lineal el conjunto $\{\psi(a_{v1}), \psi(a_{v2}), ..., \psi(a_{v(k+1)})\} \in W_m$ es linealmente independiente. Entonces si

$$\begin{array}{rcl} \Psi : AG(V_m) & \longrightarrow & AG(V_m) \\ \langle a_1, a_2, ..., a_{k+1} \rangle \setminus \{\bar{0}\} & \mapsto & \langle \phi(a_{v1}), \phi(a_{v2}), ..., \phi(a_{v(k+1)}) \rangle \setminus \{\bar{0}\}, \end{array}$$

resulta que Ψ es un isomorfismo.

□

Corolario 2.4.1 *Sea V_i un i-plano proyectivo del $PG(n, q)$ entonces, el $PG(V_i)$ isomorfo al $PG(i, q)$ sobre el mismo campo $\mathbb{F}_q$.*

Demostración. La demostración es análoga a la anterior tomando en cuenta que el $PG(\mathbb{F}_q^{m+1} \setminus \{\bar{0}\}) = PG(m, q)$.

□

Por esta razón decimos que si V_m es un m-plano proyectivo en $PG(n, q)$ entonces el $PG(V_m)$ es un $PG(m, q)$ contenido en el $PG(n, q)$.

Teorema 2.4.1 *El número de Espacios Proyectivos $PG(l,q)$ en un Espacio Proyectivo $PG(n,q)$ es:*

$$\mathcal{G}(n+1,l+1)=\prod_{i=0}^{l}\frac{q^{n-i+1}-1}{q^{l-i+1}-1}.$$

Demostración. Como a los i-planos proyectivos los estamos asociando con los subespacios vectoriales de dimensión $i+1$, entonces el número de Espacios Proyectivos $PG(l,q)$ es:

$$\mathcal{G}(n+1,l+1).$$

□

Teorema 2.4.2 *Sean l,m y n números naturales tales que $l<m<n$. Entonces, dentro de un $PG(n,q)$, el número de $PG(m,q)$ que contienen a un $PG(l,q)$ dado es:*

$$\mathcal{G}(n-l,m-l)=\prod_{i=l+1}^{m}\frac{q^{n-i+1}-1}{q^{m-i+1}-1}.$$

Demostración. Es la misma que para espacios afines, con $\bar{v}=\bar{0}$.

□

Teorema 2.4.3 *La estructura de incidencia conformada por los puntos y las líneas proyectivas de $PG(n,2)$ es un $STS(2^{n+1}-1)$ para toda $n\in\mathbb{N}$.*

Demostración. Si consideramos al Espacio Proyectivo $PG(n,2)$, entonces, según el Teorema 2.4.1; cada línea proyectiva tiene $\mathcal{G}(2,1)=\frac{2^2-1}{2^1-1}=3$ puntos y ya sabemos que entre cualquier par de puntos proyectivos, existe una única línea proyectiva que los contiene. Por lo tanto, $PG(n,2)$ es un $STS(v)$ donde;

$$v=\mathcal{G}(n+1,1)=\frac{2^{n+1}-1}{2^1-1}=2^{n+1}-1.$$

□

Corolario 2.4.2 *Sea V un i-plano proyectivo del $PG(n,2)$ con $0<i<n$, entonces, la subestructura de incidencia conformada por los puntos y las líneas proyectivas del $PG(n,2)$ contenidas en V, es un $STS(2^{i+1}-1)$.*

Demostración. De la Proposición 2.4.1; el $PG(V)$ es isomorfo al $PG(i,q)$, y por el Teorema anterior tenemos el resultado.

□

Capítulo 3

Códigos lineales

Imaginemos la siguiente estructura de comunicación; tenemos una *fuente emisora* que envía mensajes, por medio de un *canal* de comunicación, a un cierto destino que llamaremos *receptor*. En la práctica es común que dicho canal no sea lo suficientemente seguro y estable, es decir, pudiera ser que la privacidad de los mensajes se vea afectada y que en el canal pudiera haber *ruido* por lo que el mensaje recibido no sea precisamente el que se envió, entonces hay un error en la información reciba; le daremos prioridad a la detección y corrección de errores. Lo que queremos pues, es que los mensajes estén codificados de tal manera que podamos detectar y corregir los errores que se pudieran haber cometido por el ruido en el canal; para éllo es necesario enviar información extra que llamaremos *redundancia* y así confirmar si hubo errores. Trabajaremos con **palabras** de la forma (p, a, l, a, b, r, a).

Entonces, con números, tenemos la siguiente situación:

mensaje		*mensaje codificado*	*canal*	*mensaje con error*		*mensaje corregido*		*mensaje decodificado*
1010	$\rightarrow$	10101011	$\rightarrow$	10001011	$\rightarrow$	10101011	$\rightarrow$	1010

.

3.1. Conceptos básicos

Primero fijemos un *alfabeto* finito $\mathcal{A}$ del cual se van a formar las palabras de los mensajes, donde $\mathcal{A}$ un conjunto de símbolos diferentes y $|\mathcal{A}| = p$ para algún $p \in \mathbb{N}$. Ahora definamos a $M := \mathcal{A}^k$ como el conjunto de todas las posibles palabras de longitud k, que se forman con el alfabeto $\mathcal{A}$.

Definición 3.1.1 *Si $k < n$ y $C \subseteq \mathcal{A}^n$ es tal que $|C| = |M| = |\mathcal{A}^k|$, entonces decimos que C es un* ***código*** *de longitud n sobre el alfabeto $\mathcal{A}$, para alguna biyección entre M y C. A los elementos de C les llamaremos* ***palabras codificadas****.*

Definición 3.1.2 *Sean $\bar{a}, \bar{b} \in C$, con $\bar{a} = (a_1, a_2, ..., a_n)$ y $\bar{b} = (b_1, b_2, ..., b_n)$. Definimos la* ***distancia de Hamming*** *entre las palabras $\bar{a}$ y $\bar{b}$, como:*

$$d(\bar{a}, \bar{b}) := |\{i : a_i \neq b_i\}|.$$

Definición 3.1.3 *La* ***distancia mínima*** *de un código C se define como:*

$$d := d(C) := mín\{d(\bar{a}, \bar{b}) : \bar{a}, \bar{b} \in C, \bar{a} \neq \bar{b}\}.$$

El caso especial es cuando $\mathcal{A} = \mathbb{F}_q$, $M = \mathbb{F}_q^k$ y $C \leq \mathbb{F}_q^n$, es decir, las palabras son vectores sobre el campo $\mathbb{F}_q$ y el código es un subespacio vectorial de $\mathbb{F}_q^n$. Observemos antes que si $C \subset \mathbb{F}_q^n$ es un subespacio con dimensión k, siempre existe $\phi : \mathbb{F}_q^k \to C$ lineal biyectiva.

Definición 3.1.4 *Sean $k, n \in \mathbb{N}$, con $k < n$ y $\phi : \mathbb{F}_q^k \to \mathbb{F}_q^n$ una función lineal inyectiva. Decimos que $C := \phi[\mathbb{F}_q^k]$ es un $[n, k, d]_q$* ***código lineal*** *de longitud n, dimensión k y distancia mínima d, sobre el campo $\mathbb{F}_q$. En caso de que no conozcamos a d sólo diremos que C es un $[n, k]_q$ código lineal.*

En este contexto;

Definición 3.1.5 *Decimos que dos códigos lineales C_1 y C_2 son* ***equivalentes*** *si C_2 si se obtiene de C_1 intercambiando coordenadas y multiplicándolas por un elemento de $\mathbb{F}_q \setminus \{0\}$.*

Nótese que si C_1 y C_2 son equivalentes, entonces, $dim(C_1) = dim(C_2)$ en el mismo campo.

De la Definición 3.1.4 tenemos que ϕ es nuestro codificador, aparte, a cada palabra recibida $\bar{y}$ la podemos ver como la palabra codificada $\bar{x}$ más un error $\bar{e}$, es decir; $\bar{y} = \bar{x} + \bar{e}$, donde $\bar{e}$ tiene entradas todas cero, excepto en donde ocurren los errores en $\bar{x}$. Llamamos a $\bar{e}$ **vector error**. Así cuando $\bar{e} = \bar{0}$; afirmamos que no ocurren errores en la transmisión de $\bar{x}$.

Definición 3.1.6 *El* ***peso de Hamming*** *w de una palabra $\bar{a} \in C$ es el número de entradas distintas de cero en $\bar{a}$, o dicho de otra forma:*

$$w(\bar{a}) := d(\bar{a}, \bar{0}).$$

Siendo C un código lineal y $\bar{a}, \bar{b} \in C$ sucede que:

$$d(\bar{a}, \bar{b}) = d(\bar{a} - \bar{b}, 0) = w(\bar{a} - \bar{b}),$$

entonces $d = \text{mín}\{w(\bar{a}) : \bar{a} \in C, \bar{a} \neq \bar{0}\}$, es decir, la distancia mínima es igual al **peso mínimo**.

Proposición 3.1.1 *Si C_1 y C_2 son dos códigos lineales equivalentes, entonces $d(C_1) = d(C_2)$.*

Demostración. Las palabras de C_1 son las mismas que las de C_2, salvo por un intercambio de coordenadas, en particular; las palabras de peso mínimo. □

Proposición 3.1.2 *En un código lineal la distancia de Hamming es una métrica.*

Demostración. Es claro que es no-negativa y simétrica, además $d(\bar{a}, \bar{b}) = 0$ si y sólo si $a_i = b_i$ para toda $i = 1, 2, ..., n$, y así $\bar{a} = \bar{b}$. Ahora, sean $\bar{a}, \bar{b}, \bar{c} \in C$, tenemos que demostrar que $d(\bar{a}, \bar{b}) \leq d(\bar{a}, \bar{c}) + d(\bar{c}, \bar{b})$. Veamos antes que si $\bar{x} = (x_1, x_2, ..., x_n)$ y $\bar{y} = (y_1, y_2, ..., y_n)$, entonces si x_i es distinto de cero, tenemos dos casos; y_i es cero o y_i es distinto de cero, en ambos casos;

$$w(\bar{x}) \leq w(\bar{x} - \bar{y}) + w(\bar{y}).$$

Haciendo el cambio $\bar{x} = \bar{a} - \bar{b}$, $\bar{y} = \bar{c} - \bar{b}$ tenemos que:

$$w(\bar{a} - \bar{b}) \leq w(\bar{a} - \bar{c}) + w(\bar{c} - \bar{b}).$$

Por lo tanto,

$$d(\bar{a}, \bar{b}) \leq d(\bar{a}, \bar{c}) + d(\bar{c}, \bar{b}).$$

□

Como C es un código lineal con dimensión k, lo podemos describir por medio de una base. Si $C = \phi[\mathbb{F}_q^k]$, sean $\bar{e}_1, \bar{e}_2, ..., \bar{e}_k \in \mathbb{F}_q^k$ tal que el vector $\bar{e}_i$ tiene 1 en la entrada i y ceros en las demás entradas, para cada $i = 1, 2, ..., k$. Sean $\bar{v}_i := \phi(\bar{e}_i)$ para toda $i = 1, 2, ..., k.$, entonces como C es lineal; el conjunto $\mathcal{B} = \{\bar{v}_i\}_{i=1,2,...,k}$ es una base para C. Definimos a la matriz G de $k \times n$, que tiene como renglón i al vector $\bar{v}_i \in \mathcal{B}$ para cada $i = 1, 2, ..., k$, como **matriz generadora** del código C. Entoces tenemos que cada palabra

$\bar{m} = (m_1, m_2, ...m_k) = \sum_{i=1}^{k} m_i \bar{e}_i$, es codificada al aplicar la función ϕ, de la siguiente manera:

$$\phi(\bar{m}) = \sum_{i=1}^{k} m_i \phi(\bar{e}_i) = (m_1, m_2, ..., m_k)G = \bar{m}G.$$

Por lo tanto;

$$C = \{\bar{m}G : \bar{m} \in \mathbb{F}_q^k\}.$$

Otra cosa que inferimos de inmediato es que $dim(C) = Rango(G)$ sobre el mismo campo.

Así mismo podemos referirnos al complemento ortogonal a C en $\mathbb{F}_q^n$.

Definición 3.1.7 *Sea C un $[n,k]_q$ código lineal sobre $\mathbb{F}_q$. Definimos al espacio ortogonal a C, que denotaremos por $C^\perp$, como el* ***código dual*** *a C. Entonces;*

$$C^\perp = \{\bar{h} \in \mathbb{F}_q^n : \bar{h} \cdot \bar{a} = 0, \forall \bar{a} \in C\}.$$

Cómo la dimensión de $C^\perp$ es $n-k$, $C^\perp$ tiene una base con $n-k$ elementos. Entonces si H es una matriz que tiene como renglones a los vectores de una base para $C^\perp$, decimos que H es una **matriz de verificación** para el código C. Así, si definimos a $\bar{0}_{a\times b}$ como la matriz de $a \times b$ que en todas sus entradas tiene ceros, resulta que H es una matriz de $(n-k) \times n$ con la propiedad de que;

$$\bar{x} \in C \Leftrightarrow \bar{x} \cdot H^t = \bar{0}_{1\times n-k}.$$

Proposición 3.1.3 *Sea C un $[n,k]_q$ código lineal con matriz generadora G y matriz de verificación H, entonces $C^\perp$ es un $[n, n-k]_q$ código lineal con matriz generadora H y matriz de verificación G.*

Demostración. Justamente definimos a H como la matriz generadora de $C^\perp$, donde sus renglones son la base de un subespacio de dimensión $n-k$ entonces existe una función lineal inyectiva ψ tal que manda a los elementos de una base de $\mathbb{F}_q^{n-k}$ a los renglones de H, entonces $C^\perp = \psi[\mathbb{F}_q^{n-k}]$; por lo tanto $C^\perp$ es un $[n, n-k]_q$ código lineal. Ahora, sea $\bar{y} \in C^\perp$, entonces $\bar{y}$ es ortogonal a todos los elemtos de C, pero eso sucede si y sólo si $\bar{y}$ es ortogonal a la base de C, como los renglones de G son una base para C, tenemos que G es una matriz de verificación de $C^\perp$.

□

Corolario 3.1.1 *Sea C un $[n,k]_q$ código lineal con matriz generadora G y matriz de verificación H, entonces:*

$$HG^t = \bar{0}_{n-k\times k} \;\; y \;\; GH^t = \bar{0}_{k\times n-k}.$$

Definición 3.1.8 *Sea H una matriz de verificación de el código lineal C, para cada $\bar{x} \in \mathbb{F}_q^n$ definimos el **síndrome** de $\bar{x}$ como:*

$$S(\bar{x}) := \bar{x} \cdot H^t.$$

Por lo tanto, el código C queda caracterizado como:
$C = \{\bar{x} : S(\bar{x}) = \bar{0}_{1\times n-k}\}$. Siendo así, el receptor puede garantizar que si la palabra recibida $\bar{y}$, satisface $S(\bar{y}) \neq \bar{0}_{1\times n-k}$, entonces H detecta que hubo errores en la transmisión. Pero no necesariamente se están detectando todos los errores; ya que si al enviar $\bar{x}$, llega $\bar{y}$ con $\bar{y} \neq \bar{x}$, pero $\bar{y} \in C$, aunque hubo error en la transmisión de $\bar{x}$ no fué detectado. Dado que H depende de C; decimos que es C quien detecta los errores.

Lema 3.1.1 *El síndrome es lineal.*

Demostración. Si $\bar{x}$ y $\bar{y}$ son dos palabras codificadas y $\lambda \in \mathbb{F}_q\backslash\{0\}$, entonces;

$$S(\bar{x} + \lambda\bar{y}) = (\bar{x} + \lambda\bar{y}) \cdot H^t = \bar{x} \cdot H^t + \lambda\bar{y} \cdot H^t = S(\bar{x}) + \lambda S(\bar{y}).$$

□

Debido a ésto; si enviamos $\bar{x}$ y recibimos $\bar{y}$, tenemos que $\bar{y} = \bar{x} + \bar{e}$, donde $\bar{e}$ es el vector error, entonces

$$S(\bar{y}) = S(\bar{x} + \bar{e}) = S(\bar{x}) + S(\bar{e}) = S(\bar{e}).$$

Además, como $\bar{e}$ tiene entradas distintas de cero sólo en donde ocurren los errores, resulta ser que el peso de $\bar{e}$ nos dice cuantos errores hubo en la transmisión de $\bar{x}$.

Teorema 3.1.1 *Sea C un $[n,k,d]_q$ código lineal, entonces el código es capaz de detectar errores de transmisión de peso $\leq l$ si y sólo si $l+1 \leq d$.*

Demostración. Sea $\bar{x} \in C$ tal que; al enviar $\bar{x}$ se recibe $\bar{y} = \bar{x} + \bar{e}$ con $w(\bar{e}) = t \leq l$ (con $w(\bar{e}) \leq w(\bar{y})$), entonces el código detecta este error, de manera que $\bar{e}$ no pertenece a C, y así; $t = w(\bar{e}) < d$ por lo que $l + 1 \leq d$. Recíprocamente; como la distancia mínima es al menos $l+1$, cualquier palabra

con peso $\leq l$, no pertenecerá al código, por tanto, cualquier error $\bar{e}$, que ocurra en una palabra $\bar{x}$, tendra síndrome distinto de cero.

□

Analicemos un poco más al error. Si nos fijamos en cada entrada de $\bar{e}$ y $P(b|a)$ denota la probabilidad de que se reciba b dado que se envió a en alguna entrada fija, entonces $P(b|a) = p$ con $0 < p < \frac{1}{2}$ porque la probabilidad de cometer un error, en cada entrada, debe ser menor a $\frac{1}{2}$, ya que si no fuera así el canal no sería útil para transmitir y si $p = 0$ en el canal no se cometerían errores, y ese caso no nos interesa. Así las cosas, para cada entrada tenemos: $P(b|a) = p$ y $P(a|a) = (1-p)$ donde $0 < p < \frac{1}{2}$.

En el mismo sentido, si $P[\bar{e} = \bar{v}]$ denota la probabilidad de que el error cometido sea igual a la palabra $\bar{v}$; tenemos que $P[\bar{e} = a\bar{e}_i]$ (donde $\bar{e}_i$ es el vector con ceros en todas las entradas distintas de i y 1 en la entrada i con $a \in \mathbb{F}_q$), denota la probabilidad de que se cometa un error en la entrada i con error igual a a. Entonces:

$$P[\bar{e} = \bar{0}] = (1-p)^n$$

y

$$P[\bar{e} = a\bar{e}_i] = P[\bar{e} = b\bar{e}_j] = p(1-p)^{n-1}, \forall i, j = 1, 2, ..., n, \forall a, b \in \mathbb{F}_q \setminus 0,$$

ya que no nos interesa en donde se cometió el error y cuál fue dicho error. En general tenemos que

$$P[\bar{e} = \bar{v}] = p^{w(\bar{v})}(1-p)^{n-w(\bar{v})},$$

y como $p < \frac{1}{2}$ entonces

$$(1-p)^n > p(1-p)^{n-1} > p^2(1-p)^{n-2} > p^3(1-p)^{n-3} > \cdots$$

Ésto nos dice que los errores más probables de cometer son aquellos con los pesos más pequeños, razón por la que, al decodificar buscamos la palabra del código más cercana a la palabra recibida.

Definición 3.1.9 *Definimos la* ***esfera*** *de radio r con centro en $\bar{x} \in \mathbb{F}_q^n$ como el conjunto:*

$$B(\bar{x}, r) := \{\bar{y} \in \mathbb{F}_q^n : d(\bar{x}, \bar{y}) \leq r\}.$$

Teorema 3.1.2 *Sea C un $[n, k, d]_q$ código lineal, entonces C tiene la capacidad de corregir errores de transmisión con peso $\leq \lfloor \frac{d-1}{2} \rfloor$*

Demostración. Tenemos dos casos $d = 2r + 1$ ó $d = 2r + 2$, en ambos $r = \lfloor \frac{d-1}{2} \rfloor$; consideramos las esferas de radio r con centro en cada elemento de C, afirmamos que dichas esferas son ajenas; sean $\bar{x}$ y $\bar{y} \in C$ palabras distintas, supongamos que existe $\bar{v} \in B(\bar{x}, r) \cap B(\bar{y}, r)$, entonces
$d(\bar{x}, \bar{y}) \leq d(\bar{x}, \bar{v}) + d(\bar{y}, \bar{v}) \leq 2r$ contradiciendo que d es la distancia mínima.

Ahora, si se envía $\bar{x}$ y se recibe $\bar{y} = \bar{x} + \bar{e}$, donde $w(\bar{e}) \leq r$, entonces $\bar{y} \in B(\bar{x}, r)$, es decir, $\bar{x}$ es la palabra codificada más cercana a $\bar{y}$, entonces el código corrige el error de peso a lo más r.

□

Lo que en escencia estamos haciendo es empaquetar a las palabras en esferas de radio r. Para ver cuantas palabras tiene cada esfera, contemos las formas en que podemos tener i entradas distintas de la palabra codificada con $0 \leq i \leq r$; para las que están a distancia i de una palabra codificada fija, , tenemos $\binom{n}{i}$ formas de escoger estas i entradas y en cada entrada podemos tener $q-1$ letras distintas de la original, entonces tenemos $\binom{n}{i}(q-1)^i$ palabras a distancia i de una palabra codificada. Cada esfera de radio r centradas en alguna palabra codificada $\bar{v}$, corrige los errores que contiene, es decir, su volumen:

$$|B(\bar{v}, r)| = \sum_{i=0}^{r} \binom{n}{i} (q-1)^i.$$

Proposición 3.1.4 *Sean C un $[n, k, d]_q$ código lineal y $r = \lfloor \frac{d-1}{2} \rfloor$ entonces:*

$$q^k \sum_{i=0}^{r} \binom{n}{i} (q-1)^i \leq q^n.$$

Demostración. Cuando $r = \lfloor \frac{d-1}{2} \rfloor$, ya vimos que las esferas centradas en las palabras codificadas de radio r, son ajenas; entonces para cualquier palabra $\vec{v}$ fija:

$$|C||B(\vec{v}, r)| = q^k \sum_{i=0}^{r} \binom{n}{i} (q-1)^i \leq q^n.$$

□

Definición 3.1.10 *Sean C un $[n, k, d]_q$ código lineal y $r = \lfloor \frac{d-1}{2} \rfloor$. Si las esferas de radio r con centro en los elementos de C son ajenas y su unión*

contiene a $\mathbb{F}_q^n$*, entonces decimos que* C *es un código* ***perfecto****. En otras palabras;* C *es un código perfecto si:*

$$q^k \sum_{i=0}^{r} \binom{n}{i} (q-1)^i = q^n.$$

Para la decodificación existe una forma general para cualquier código lineal, utilizando el síndrome, pero no es muy práctica porque implica enlistar (de manera adecuada) todas las palabras del código. Dado que los códigos lineales no son el interés central de este trabajo; nos enfocaremos a los códigos asociados a $STS(v)$.

3.2. Códigos lineales asociados a estructuras de incidencia

Observemos que, en una estructura de incidencia S, una vez que numeramos a los puntos y los mantenemos fijos; el orden de los renglones de dos matrices de incidencia de S, es lo que hace que sean diferentes. En este contexto; los renglones de cualquier matriz de incidencia generan el mismo espacio.

Definición 3.2.1 *Sean* $S = (\mathcal{P}, \mathcal{B})$ *una estructura de incidencia, con* $\mathcal{P} = \{p_1, p_2, ..., p_v\}$*, y* $\mathbb{F}_q$ *un campo, entonces definimos el* ***código asociado a*** S ***sobre el campo*** $\mathbb{F}_q$*,* $C_q(S)$*, como el espacio generado por los vectores de incidencia de los bloques de* S*,es decir:*

$$C_q(S) = \langle \chi(B) : B \in \mathcal{B} \rangle_q.$$

Debemos notar dos cosas. Si M es una matriz que tiene por renglones a los vectores de incidencia de los bloques de S, entonces $dim(C_q(S)) = Rango_q(M)$. Y que el orden de las columnas (es decir, la forma en que numeramos a los puntos), es lo que hace que dos códigos asociados a la misma estructura de incidencia, sean equivalentes.

Teorema 3.2.1 *Si dos estructuras de incidencia finitas* S_1 *y* S_2 *son isomorfas, entonces,* $C_q(S_1)$ *es equivalente a* $C_q(S_2)$*.*

Demostración. Como S_1 y S_2 son isomorfas entonces existe una función biyectiva ϕ de los puntos de S_1 a los puntos de S_2, entonces, si en la matriz de incidencia asociada a S_1 tenemos acomodadas las columnas de acuerdo al orden de los puntos como $p_1, p_2, ..., p_v$ y reacomodamos las columnas de la matriz asociada a S_2 de tal manera que se encuetren ordenadas como $\phi(p_1), \phi(p_2), ..., \phi(p_v)$, tenemos entonces que estas dos matrices tienen los mismos renglones debido a que ϕ manda bloques de S_1 a los bloques de S_2. Por lo tanto, $C_q(S_1)$ es equivalente a $C_q(S_2)$ porque llegamos de $C_q(S_2)$ a $C_q(S_1)$ intercambiando coordenadas.

□

Teorema 3.2.2 *Si dos estructuras de incidencia S_1 y S_2 son isomorfas y $\mathbb{F}_q$ es un campo, entonces, sus matrices de incidencia tienen el mismo rango sobre $\mathbb{F}_q$.*

Demostración. Por el Teorema anterior; $C_q(S_1)$ es equivalente a $C_q(S_2)$, entonces, $dimC_q(S_1) = dimC_q(S_2)$. Pero, $dimC_q(S_1) = Rango_q(M)$ para toda matriz de incidencia M de S_1, y lo mismo sucede con $dimC_q(S_2)$. Por lo tanto cualquier par de matrices de incidencia de S_1 y S_2 tienen el mismo rango sobre $\mathbb{F}_q$.

□

Sea S una estructura de incidencia, consideremos una de sus matrices de incidencia $M_{b\times v}$ con b renglones y v columnas. Debido a que $M_{b\times v}$ es una matriz de $0's$ y $1's$, observamos que el rango de $M_{b\times v}$ sobre el campo $\mathbb{F}_{p^n}$ es el mismo que sobre el campo $\mathbb{Z}_p$; que llamaremos $p - rango$ de $M_{b\times v}$ y lo denotaremos por $Rango_pM$. Además, ya vimos que el rango es independiente de como numeremos a los puntos y bloques de S, es decir, es el mismo rango para cualquier matriz de incidencia relacionada con S, y tenemos que:

$$Rango_pM = dim(C_p(S)).$$

Estas observaciones nos dan pie para el siguiente capítulo.

Capítulo 4

El p-rango de un $STS(v)$

Definición 4.0.2 *Definimos el* ***p-rango*** $Rango_pS$ *de el Sistema Triple de Steiner* S *como el* $p-rango$ *de cualquiera de sus matrices de incidencia.*

Si S un Sistema Triple de Steiner con v puntos, como el $Rango_pS$ es igual al $Rango_pM$ de cualquier matriz de incidencia relacionada con S, entonces;

$$Rango_pS \leq v.$$

En el caso de que $Rango_pM < v$, tenemos que existe una combinación lineal no-trivial, de las columnas de M, igual a $\bar{0}_{b\times 1}$, es decir, denotando como C_i a la columna i de la matriz M, que representa el vector de incidencia del punto i, tenemos que existen $w_1, w_2, ..., w_v \in \mathbb{Z}_p$, no todos cero, tal que:

$$\sum_{i=1}^{v} w_i C_i = \bar{0}_{b\times 1}.$$

Entonces la **distribución de peso** a cada punto como a continuación se muestra:

$$\begin{aligned} w : S &\longrightarrow \mathbb{Z}_p \\ i &\mapsto w_i \end{aligned}$$

asigna a cada punto su peso correspondiente. De esta manera obtenemos que los bloques cumplen con la propiedad de que si $B_x = \{i, j, k\}$ es un bloque de S, entonces $w_i + w_j + w_k = 0$, ya que en el *lugar* x los únicos elementos con entradas distintas de cero son i, j y k. Así para cada $\alpha \in \mathbb{Z}_p$ distinguimos al conjunto S_α como el subconjunto de puntos de S con peso α. Por comodidad, para dos puntos distintos i y j, denotaremos por $i * j$

al tercer punto del bloque que los contiene. En este contexto exponemos los siguientes lemas.

Lema 1 *S_0 es un subsistema de S.*

Demostración. Sean i y j dos puntos distintos en S_0 entonces el bloque $\{i, j, i * j\}$ es tal que $w_i + w_j + w_{i*j} = 0$, como $i, j \in S_0$, implica que $w_i = w_j = 0$, entonces $w_{i*j} = 0$, por lo tanto $i * j \in S_0$.

□

Lema 2 *Si $S_0 \neq \emptyset$ entonces $|S_\alpha| = |S_{-\alpha}|$ para cada $\alpha \in \mathbb{Z}_p \setminus \{0\}$.*

Demostración. Sea $\alpha \in \mathbb{Z}_p \setminus \{0\}$ e $i \in S_0$. Entonces consideramos la biyección entre los puntos de S_α y $S_{-\alpha}$ que se establece por el mapeo que asigna a cada punto $j \in S_\alpha$, el punto $(i * j) \in S_{-\alpha}$.

□

Lema 3 *Si $p \neq 2$ y $S_0 \neq \emptyset$, entonces $S_\alpha \neq \emptyset$ implica que $|S_\alpha| = |S_0|$, $\forall \alpha \in \mathbb{Z}_p \setminus \{0\}$.*

Demostración. como $p \neq 2$ implica que $S_\alpha \neq S_{-\alpha}$ y por el Lema 2 sabemos que $|S_\alpha| = |S_{-\alpha}|$, entonces $S_{-\alpha} \neq \emptyset$. Análogamente a la demostración anterior; fijamos un punto $i \in S_{-\alpha}$ y consideramos la biyección entre S_α y S_0 que se determina por la operación $*$ con el punto i.

□

Lema 4 *Si $p \neq 3$ y $|S_\alpha| \geq 2$ con $\alpha \neq 0$, entonces $|S_\alpha|$ es par y $|S_{-2\alpha}| = |S_\alpha| - 1$.*

Demostración. Como $p \neq 3$ tenemos que $S_\alpha \neq S_{-2\alpha}$, entonces fijando un punto $i \in S_\alpha$, obtenemos la biyección entre $S_\alpha \setminus \{i\}$ y $S_{-2\alpha}$ tal que a cada punto $j \in S_\alpha \setminus \{i\}$ le coincidimos el punto $(j * i) \in S_{-2\alpha}$. Entonces $|S_{-2\alpha}| = |S_{-2\alpha}| + 1$. Ahora, como $|S_\alpha| \geq 2$, tenemos que $S_{-2\alpha}$ es no vacío. Sea $i \in S_{-2\alpha}$, entonces el mapeo que manda cada punto $j \in S_\alpha$ en el punto $(j * i)$ que también pertenece a S_α, además dicho mapeo no puede tener puntos fijos ya que los bloques tienen exáctamente tres puntos. Por lo tanto, $|S_\alpha|$ es par.

□

Teorema 4.0.3 *Para cada primo $p > 3$,*

$$Ranro_pM = v.$$

Demostración. Si $Rango_pM < v$. Entonces existe $\alpha \in \mathbb{Z}_p \setminus \{0\}$ tal que $S_\alpha \neq \emptyset$. Definamos pues el conjunto $\Gamma := \{\alpha \in \mathbb{Z}_p : S_\alpha \neq \emptyset\}$, obviamente $|\Gamma| \geq 2$.

caso 1. $|S_0| > 1$.

Por el Lema 1 sabemos que S_0 es un subsistema, entonces $|S_0| \geq 3$. Y como existe otra $\alpha \in \Gamma$, por el Lema 3; $|S_\alpha| \geq 3$, y así por el Lema 4 $|S_\alpha|$ es par y $|S_{-2\alpha}| = |S_\alpha| - 1$ es *impar*. Sin embargo, el hecho de que $|S_\alpha| \geq 3$ implica que $|S_{-2\alpha}| \geq 2$, y nuevamente por el Lema 4, $|S_{-2\alpha}|$ debe ser par, lo cual es una contradicción.

caso 2. $|S_0| = 1$.

Por el Lema 3 tenemos que $\forall \alpha \in \Gamma$, $|S_\alpha| = 1$. Por lo que podemos renombrar a los puntos de S e identificarlos con su peso. Como $v > 3$, el sistema S contiene al menos dos bloques $\{0, \alpha, -\alpha\}$ y $\{0, \beta, -\beta\}$ distintos. Pero de esta manera quedan determinados los bloques $\{\alpha, \beta, -\alpha - \beta\}$ y $\{-\alpha, \beta, \alpha - \beta\}$, que a su vez determiman al bloque $\{\alpha - \beta, -\alpha - \beta, 2\beta\}$. Ahora, como $\beta \neq 0$ y $p \neq 3$, $-\beta \neq 2\beta$. Entonces el bloque que pasa por $-\beta$ y 2β tiene otro punto con peso $-\beta$, contradiciendo el hecho de que $|S_{-\beta}| = 1$.

caso 3. $S_0 = \emptyset$.

Primero veamos que pasa si $|S_\alpha| = 1$ $\forall \alpha \in \Gamma$. Entonces igual que en el caso anterior, identificamos a los puntos de S con su peso y también tenemos al menos dos bloques distintos $\{\alpha, \beta, -\alpha - \beta\}$ y $\{\alpha, \gamma, -\alpha - \gamma\}$, por lo que también tendremos a los bloques $\{\beta, -\alpha - \gamma, \alpha - \beta + \gamma\}$ y $\{\gamma, -\alpha - \beta, \alpha + \beta - \gamma\}$. Como $\beta \neq \gamma$ y cada peso es distinto a su inverso aditivo, ya que $p \neq 2$; entonces $\alpha - \beta + \gamma \neq \alpha + \beta - \gamma$, y establecen el bloque $\{\alpha - \beta + \gamma, \alpha + \beta - \gamma, -2\alpha\}$. Como $p \neq 3$; 2α y α son distintos y determinan un bloque que tiene un tercer punto de peso α; lo que contradice que $|S_\alpha| = 1$.

Ahora supongamos que existe $\alpha \in \mathbb{Z}_3$ con $|S_\alpha| \geq 2$. Si $|S_\alpha| > 2$, por el Lema 4 tenemos que $|S_\alpha|$ es par y $|S_{-2\alpha}| = |S_\alpha| - 1$ es impar, pero $|S_{-2\alpha}| \geq 2$ y otra vez por el Lema 4 tenemos que $|S_{-2\alpha}|$ es par; contradicción. Entonces $|S_\alpha| = 2$ y $|S_{-2\alpha}| = 1$, por lo que, $S_\alpha \cup S_{-2\alpha}$

es un bloque de S, sean a y a' los elementos de S_α y consideremos a cualquier otro elemento $b \in S \setminus (S_\alpha \cup S_{-2\alpha})$ tal que $b \in S_\beta$, entonces se determina el bloque $\{a, b, c\}$ donde $c \in S_{-\alpha-\beta}$, y por consiguiente también el bloque $\{a', c, b'\}$ donde $b' \in S_\beta$, como $a \neq a'$, entonces $b \neq b'$. Por lo tanto, $|S_\beta| \geq 2$, igualmente, como lo hicimos para α, mostramos que $|S_\beta| = 2$ y $|S_{-2\beta}| = 1$ Entonces, si d es el elemento en $S_{-2\beta}$, y $d \in S \setminus (S_\alpha \cup S_{-2\alpha})$ igual que para b, probamos que $|S_{-2\beta}| \geq 2$, contradiciendo lo anterior. Así las cosas; $d \in S_\alpha \cup S_{-2\alpha}$ como $|S_\alpha| = 2$ entonces $d \in S_{-2\alpha}$, implica que $-2\beta = -2\alpha$ dado que $p \neq 2$, concluimos que $\beta = \alpha$; contracción.

Por lo tanto no puede suceder que $Rango_p M < v$ cuando $p \neq 2, 3$ y ya sabemos que $Rango_p M \leq v$, entonces $Rango_p M = v$.

□

El Teorema anterior es muy fuerte, ya que el $p - rango$ resulta ser un invariante, cuando $p \geq 3$, independiente de la estructura de los Sistemas Triples de Steiner. No así, cuando $p = 2$ ó $p = 3$.

4.1. El 2-rango

Definición 4.1.1 *Decimos que un subsistema propio S' de un Sistema Triple de Steiner S, es un* ***hiperplano proyectivo****, si cada bloque de S tiene una intersección no vacía con S'.*

La definición, en abstracto, no tiene mucho que ver con la definición que tenemos de *hiperplano proyectivo* para Espacios Proyectivos pero al ocuparnos de $\mathbb{F}_p^{n+1}$ con $p = 2$, por el Teorema 2.4.3, la estructura de incidencia conformada por los puntos y las líneas proyectivas del Espacio Proyectivo $PG(n, 2)$ es un $STS(2^{n+1} - 1)$ y por el Teorema 2.4.1, cada hiperplano proyectivo de $PG(n, 2)$ tiene $\mathcal{G}(n, 1)$ puntos, donde;

$$\mathcal{G}(n, 1) = 2^n - 1 = \frac{2(2^n - 1)}{2} = \frac{(2^{n+1} - 1) - 1}{2} = \frac{v - 1}{2}.$$

Teorema 4.1.1 *Un subsistema S' de un Sistema Triple de Steiner S, es un hiperplano proyectivo si y sólo si*

$$|S'| = \frac{(v - 1)}{2}.$$

Demostración. Si S' es un subsistema propio, entonces existe $x \in S \setminus S'$; consideramos los r bloques que pasan por x. Sea $y \in S'$ sabemos que existe un único bloque que contiene a x y y, sea $\{x, y, z\}$ tal bloque. Entonces si $z \in S'$, por definición de subsistema, implica que $x \in S'$; contradicción. Entonces $z \notin S'$, ésto quiere decir que los bloque que pasan por x intersectan a S' en a lo más un punto.

Si S' es hiperplano proyectivo; todo bloque que pasa por x intersecta a S'. Por lo que tenemos una relación biyectiva entre los elementos S' y los bloques que pasan por x. Por lo tanto

$$|S'| = r = \frac{(v-1)}{2}.$$

Ahora, si S' es un subsistema con $|S'| = \dfrac{(v-1)}{2}$; ya tenemos que intersecta a los r bloques que pasan por cualquier elemento fuera de él. Por lo que S' es un hiperplano proyectivo.

□

Sabemos que $Rango_2 M < v$ si y sólo si existe, entre las columnas de M, una combinación lineal, no-trivial igual a $\bar{0}_{b\times 1}$. Y como $p = 2$, sólo tememos los posibles pesos 0 y 1, ésto nos dice que $|S_0| + |S_1| = v$ y $|S_1| \geq 2$, entonces por el Lema 4; $|S_0| = |S_1| - 1$. Por lo tanto, $|S_0| + |S_0| + 1 = v$ y así $|S_0| = \frac{v-1}{2}$ y como S_0 es un subsistema; S_0 es un hiperplano proyectivo.

Inversamente, si S contiene un hiperplano proyectivo H, entonces definimos la distribución de peso w_H para cada elemento en S de la siguiente manera;

$$w_H(i) = \begin{cases} 0 & \text{si } i \in H, \\ 1 & \text{si } i \notin H. \end{cases}$$

Esta distribución de peso; origina una combinación lineal, no-trivial igual a $\bar{0}_{b\times 1}$, de las columnas de M, ya que H intersecta a todos los bloques en uno o tres puntos, razón por la que; en las entradas consernientes a cada bloque, la suma de los pesos, es igual a cero. En consecuencia, $Rango_2 M < v$.

Entonces tenemos una biyección entre los hiperplanos proyectivos y las combinaciones lineales no-triviales, de los vectores columna de M, iguales a $\bar{0}_{b\times 1}$, con coeficientes en $\mathbb{Z}_2$. Caractericemos pues, a los hiperplanos proyectivos por medio de sus distribuciones de peso.

Teorema 4.1.2 *Sean w_1 y w_2 dos distribuciones de peso distintas. Si a cada elemento $i \in S$ le asignamos el peso $w(i) := w_1(i) + w_2(i)$, entonces w determina otro hiperplano proyectivo.*

Demostración. Sean H_1 y H_2 los hiperplanos proyectivos que determinan las distribuciones de peso w_1 y w_2. Consideremos el conjunto

$$H = (H_1 \cap H_2) \cup (S \setminus (H_1 \cup H_2)).$$

Veamos que H es un subsistema de S. Sean i y j dos elementos en H y $B = \{i, j, k\}$ el bloque que contiene a i y j; si $i, j \in (H_1 \cap H_2)$, debido a que H_1 y H_2 son subsistemas, implica que $B \subset (H_1 \cap H_2) \subset H$. Si $i, j \in (S \setminus (H_1 \cup H_2))$ entonces, por ser H_1 y H_2 hiperplanos proyectivos, intersectan a todos los bloques, y así $k \in (H_1 \cap H_2)$. Ahora, si $i \in (H_1 \cap H_2)$ y $j \in (S \setminus (H_1 \cup H_2))$, ocurre que $k \notin (H_1 \cup H_2)$ porque de lo contrario $j \notin (S \setminus (H_1 \cup H_2))$, ya que H_1 y H_2 son hiperplanos proyectivos, entonces $k \in (S \setminus (H_1 \cup H_2))$ y por lo tanto, $B \subset H$. Como $S \setminus H = S \setminus ((H_1 \cap H_2) \cup (S \setminus (H_1 \cup H_2))) = (H_1 \cup H_2) \setminus (H_1 \cap H_2)$, y $H_1 \neq H_2$, entonces $S \setminus H \neq \emptyset$, por lo que H es un subsistema propio. Tomemos $x \in S \setminus H = (H_1 \cup H_2) \setminus (H_1 \cap H_2)$, sin pérdida de generalidad supongamos que $x \in H_1$, y sea $B = \{x, y, z\}$ un bloque que pasa por x, como H_2 es hiperplano proyectivo, intersecta a B, pero no puede ser en x por no estar en la intersección. Otra vez, sin pérdida de generalidad supongamos que $y \in H_2$; entonces $z \notin H_2$ porque si no fuera así x estaría en H_2. Entonces; si $z \in H_1$ tenemos que $y \in (H_1 \cap H_2)$ y se tiene que H intersecta a B, y si $z \notin H_2$ tenemos que $z \in (S \setminus (H_1 \cup H_2))$. Por lo tanto H es un hiperplano proyectivo de S. Ahora, sea $i \in S$ un punto, y w la distribución de peso correspodiente a H. Entonces por un lado, si $i \in H = (H_1 \cap H_2) \cup (S \setminus (H_1 \cup H_2))$ con $i \in (H_1 \cap H_2)$, tenemos que $w(i) = 0 = 0 + 0 = w_1(i) + w_2(i)$, y si $i \in H$ con $i \in (S \setminus (H_1 \cup H_2))$, tenemos que $w(i) = 0 = 1 + 1 = w_1(i) + w_2(i)$. Por otro lado, si $i \notin H$, ésto es, $i \in S \setminus H = (H_1 \cup H_2) \setminus (H_1 \cap H_2)$ entonces $i \in H_1$ o $i \in H_2$ en cualquiera de los dos casos tenemos que $w(i) = 1 = 1 + 0 = w_1(i) + w_2(i)$. Por lo tanto, H_1 y H_2 determinan al hiperplano proyectivo que tiene como distribución de peso a la suma de w_1 y w_2.

□

Obsevación 1. Consideramos el espacio $\mathcal{W}$ que consiste de todas las distribuciones de peso asociadas con los hiperplanos proyectivos de S, junto con la distribución w_0 que le asigna el peso 0 a cada punto de S; como los escalares en $\mathbb{Z}_2$ son 0 y 1, y por el Teorema anterior tenemos que $\mathcal{W}$ tiene estructura de espacio vectorial sobre $\mathbb{Z}_2$. Por lo tanto, el conjunto de todas las distribuciones de peso, asociadas a hiperplanos proyectivos, tienen estructura de Espacio Proyectivo sobre $\mathbb{Z}_2$. Que es lo mismo decir; que el conjunto $\mathcal{H}$,

compuesto de todos hiperplanos proyectivos de S, tiene estructura de Espacio Proyectivo. Definimos la **dimensión proyectiva** $d_{\mathcal{P}}$ como la dimensión de $\mathcal{H}$.

Teorema 4.1.3 *Dado un Sistema Triple de Steiner S, con $v \geq 3$;*

$$Rango_2 S = v - (d_{\mathcal{P}} + 1).$$

Demostración. Sea M una matriz de incidencia de S con columnas $C_1, C_2, ..., C_v$, entonces $Rango_2 S = Rango_2 M$. De la Defínción 1.0.6; $Rango_2 M = Rango_2(L_M)$, donde $L_M : \mathbb{Z}_2^v \longrightarrow \mathbb{Z}_2^b$ es la transformación de multiplición por la izquierda de M. Por el *Teorema de la dimensión* [1];

$$Rango_2(L_M) = dim(\mathbb{Z}_2^v) - dim(kernel(L_M)) = v - dim(kernel(L_M)),$$

donde el
$kernel(L_M) = \{\bar{x} \in \mathbb{Z}_2^v : M\bar{x} = \bar{0}_{b\times 1}\}$
$= \{(x_1, x_2, ..., x_v) \in \mathbb{Z}_2^v : x_1C_1 + x_2C_2 + \cdots + x_vC_v = \bar{0}_{b\times 1}\} = \mathcal{W}$,
$\Longrightarrow Rango_2 S = v - dim(\mathcal{W}) = v - (dim(\mathcal{H}) + 1) = v - (d_{\mathcal{P}} + 1)$.

□

4.2. El 3-rango

Sea S' un subsistema propio de un Sistema Triple de Steiner S, y un punto $x \in S \setminus S'$. Consideremos al espacio $\mathcal{B}_x$ que tiene los mismos puntos de S pero sólo los bloques que pasan por x. Entonces denotemos por S'' al espacio que resulta de quitar los puntos de los bloques de $\mathcal{B}_x$ que intersectan a S'. Así, resulta que $S' \cap S'' = \emptyset$.

Definición 4.2.1 *Decimos que un subsistema propio S' de un Sistema Triple de Steiner S, es un **hiperplano afín**, si S'' es un subsistema, y cada bloque intersecta a S' en exáctamente un punto si y sólo si intersecta a S'' en un solo punto.*

Por como generamos a $\mathcal{B}_x$, pareciera que S'' depende del elemento x que se toma fuera de S'. Veamos que S'' no depende de la $x \in S''$; sea $y \in S''$ con $y \neq x$. Tomemos en cuenta al conjunto $\mathcal{B}_y$. Los bloques que intersectan a S' lo hacen en un solo punto, ya que si fuera en dos; y estaría en S'. Entonces estos bloques no pertenecen a S'', coincidiendo con la estructura inicial. Si

un bloque no intersecta a S' entonces tienen dos puntos en S'' (por que si sólo fuera y tendríamos que ese bloque intersecta a S' en un punto), de modo que el bloque queda contenido en S'', ya que S'' es subsistema de S. Por lo tanto, la construcción a partir de y de S'', no quita ni aporta nuevos bloques.

Proposición 4.2.1 *Sea S' un hiperplano afín del Sistema Triple de Steiner S, entonces el espacio $S''' = S \setminus (S' \cup S'')$, es un subsistema.*

Demostración. Sean $x, y \in S''' = S \setminus (S' \cup S'')$, y sea $B = \{x, y, z\}$ el único bloque que contiene a x y y, entonces $z \notin (S' \cup S'')$, de lo contrario querría decir que B intersecta a $(S' \cup S'')$ y por definición tenemos que intersecta a ambos en diferentes puntos, entonces x o y pertenecen a $(S' \cup S'')$, siendo que los tomamos en $S''' = S \setminus (S' \cup S'')$. Por lo tanto, $z \in S''' = S \setminus (S' \cup S'')$, y entonces S''' es un subsistema.

□

Lo que hemos hecho es partir a S en tres subsistemas ajenos (S',S'',S''').

Proposición 4.2.2 *Sea S' un hiperplano afín, entonces los subsistemas S'' y S''' son hiperplanos afines.*

Demostración. Sea $x \in S \setminus S''$ entonces $x \in S'$ o $x \in S'''$, en cualquiera de los dos casos tenemos que S' (o S''') es un subsistema y contiene a los bloques que pasan por x que no intersectan a S''. Entonces S'' es un hiperplano. La prueba para S''' es análoga que para S''.

□

Entonces S'' y S''' quedan determinados por S' salvo que les intercambiemos el nombre. Aún más, cualquiera de estos tres (S',S'',S''') hiperplanos afines, determina a los otros dos.

Definición 4.2.2 *Sea S' un hiperplano afín, al conjunto de hiperplanos afines $\mathcal{H} := \{S', S'', S'''\}$, diremos que es una* ***familia de hiperplanos afines paralelos****.*

Corolario 4.2.1 *Sea $\mathcal{H} := \{S', S'', S'''\}$ una familia de hiperplanos afines paralelos, entonces:*

$$|S'| = |S''| = |S'''| = \frac{v}{3}.$$

Demostración. Si entre cualquier par de (S',S'',S'''), consideramos un punto x fuera de ellos y los bloques que pasan por x y todos los puntos de uno de ellos; tendríamos una biyección de los puntos de un hiperplano afín al otro, es decir: $|S'| = |S''| = |S'''|$ y como la unión $S' \cup S'' \cup S''' = S$ es ajena;

$$|S'| = |S''| = |S'''| = \frac{v}{3}.$$

□

Nuevamente la noción de hiperplano afín y paralelismo, no es exáctamente la que teníamos en los Espacios Afines, pero considerando el espacio vectorial $\mathbb{F}_p^n$, con $p = 3$; por el Teorema 2.3.4, la estructura de incidencia conformada por los puntos y las líneas afines del Espacio Afín $AG(n, 3)$ es un $STS(3^n)$. Además, cada hiperplano afín de $AG(n, 3)$ tiene $|\mathbb{F}_3^{n-1}| = 3^{n-1} = \frac{v}{3}$ puntos y dado un hiperplano afín, existen exáctamente dos hiperplanos afines paralelos a él, ya que su *complemento ortogonal* tiene tres puntos. Y al revés, si tenemos tres hiperplanos afines disjuntos, entonces son paralelos.

Teorema 4.2.1 *En un Sistema Triple de Steiner S, tres subsistemas disjuntos tal que su unión es S, forman una familia de hiperplanos afines paralelos.*

Demostración. Sean S_1,S_2 y S_3 dichos subsistemas. Como la unión resulta ser S y son ajenos, sucede que $S_3 = S \setminus (S_1 \cup S_2)$, además, cualquier bloque que intersecte a un subsistema en un solo punto; tiene que intersectar a los tres en exáctamente un punto, por que de lo contrario, intersectaría a otro en dos puntos y el bloque completo le pertenecería; contradiciendo que son ajenos.

Sea $x \in S_2$ y consideremos al conjunto S_1'' generado por S_1 y x. Como S_1 y S_2 son ajenos, y S_2 es subsistema; S_2 no puede tener a los puntos de los bloques que pasan por x e intersectan a S_1, por lo tanto; $S_2 \subseteq S_1''$. Ahora, si existe $y \in S_1'' \setminus S_2$, y $B = \{x, y, z\}$ es el bloque que contiene a x y y, entonces z tampoco pertenece a S_2, y así, B intersecta a S_2 en un solo punto, por lo que debería intersectar a S_1, pero esos bloques los descartamos en la construcción de S_1''. Por lo tanto $S_2 = S_1''$. entonces S_1'' es subsistema. Entonces S_1 es un hiperplano afín, y por las Proposiciones 4.2.1 y 4.2.2; $S_2 = S_1''$ y $S_3 = S \setminus (S_1 \cup S_2)$ también son hiperplano afines.

□

Regresemos con la matriz de incidencia M del Sistema Triple de Steiner S. Dado que cada renglón representa la incidencia en los bloques; tenemos

tres $1's$ en cada renglón, entonces en $\mathbb{Z}_3$:

$$\sum_{i=1}^{v} C_i = 0 = \sum_{i=1}^{v} 2C_i,$$

por lo que $Rango_3 M \leq v - 1$.

Sean w_0, w_1 y w_2 las distribuciones de peso que les asignan, a todos los puntos, el peso constante 0,1 y 2 respectivamente. Entonces, si $Rango_3 M < v - 1$, existe una distribución de peso w que; para algún par de elementos distintos i y j, les asigna pesos distintos w_i y w_j. Si este $\{i, j, k\}$ es el bloque que contiene a i y j, entonces tenemos la ecuación: $w_i + w_j + w_k = 0$. Como w_i y w_j son distintos y $p = 3$ entonces $\{w_i, w_j w_k\} = \{0, 1, 2\}$, por lo que los conjuntos S_0, S_1 y S_2 son no-vacíos y la suma de sus elementos es el total. Entonces por los lemas 2 y 3, $|S_0| = |S_1| = |S_2| = \frac{v}{3}$, y si nos fijamos en la demostración del Lema 1, dado que $p = 3$, deducimos que S_0, S_1 y S_2 son subsistemas. Por lo tanto S_0, S_1 y S_2 forman una *familia de hiperplanos afines paralelos* en S.

Por otro lado; si S contiene una familia $\mathcal{H}$ de hiperplanos afines paralelos H_0, H_1 y H_2, entonces definimos la distribución de peso $w_{\mathcal{H}}$ para cada elemento en S; de la siguiente manera:

$$w_{\mathcal{H}}(i) = \begin{cases} 0 & \text{si } i \in H_0, \\ 1 & \text{si } i \in H_1, \\ 2 & \text{si } i \in H_2. \end{cases}$$

Esta distribución de peso corresponde a una combinación lineal no-trivial, de los vectores columna de M, iguales al vector cero, por lo que $Rango_3 M < v - 1$.

Por lo tanto, tenemos una biyección entre los hiperplanos afines y las combinaciones lineales (distintas de w_0, w_1 y w_2), de las columnas de M, iguales al vector cero, con coeficientes en $\mathbb{Z}_3$.

Teorema 4.2.2 *Sean $w_{\mathcal{H}}$ y $w_{\mathcal{H}'}$ distribuciones de peso asociadas a las familias de hiperplanos afines paralelos $\mathcal{H}$ y $\mathcal{H}'$ respectivamente, entonces las distribuciones de peso $w_1 := w_{\mathcal{H}} + w_{\mathcal{H}'}$ y $w_2 := w_{\mathcal{H}} + 2w_{\mathcal{H}'}$ determinan otras dos familias de hiperplanos afines paralelos.*

Demostración. Sean $\mathcal{H} = \{H_0, H_1, H_2\}$ y $\mathcal{H}' = \{H'_0, H'_1, H'_2\}$ las familias de hiperplanos afines paralelos determinadas por las distribuciones de peso $w_{\mathcal{H}}$

y $w_{\mathcal{H}'}$; antes que nada, advertimos que a S lo podemos expresar por medio de distintas uniones ajenas, a saber:

$$S = H_0 \cup H_1 \cup H_2 = (H_0 \cap S) \cup (H_1 \cap S) \cup (H_2 \cap S)$$

$$= (H_0 \cap (H'_0 \cup H'_1 \cup H'_2)) \cup (H_1 \cap (H'_0 \cup H'_1 \cup H'_2)) \cup (H_2 \cap (H'_0 \cup H'_1 \cup H'_2))$$

$$= \bigcup_{\alpha,\beta \in \mathbb{Z}_3} (H_\alpha \cap H'_\beta) \qquad (i)$$

$$= \left(\bigcup_{\alpha \in \mathbb{Z}_3} (H_\alpha \cap H'_{2\alpha}) \right) \cup \left(\bigcup_{\alpha \in \mathbb{Z}_3} (H_\alpha \cap H'_{2\alpha+1}) \right) \cup \left(\bigcup_{\alpha \in \mathbb{Z}_3} (H_\alpha \cap H'_{2\alpha+2}) \right) \qquad (ii)$$

$$= \left(\bigcup_{\alpha \in \mathbb{Z}_3} (H_\alpha \cap H'_{\alpha}) \right) \cup \left(\bigcup_{\alpha \in \mathbb{Z}_3} (H_\alpha \cap H'_{\alpha+2}) \right) \cup \left(\bigcup_{\alpha \in \mathbb{Z}_3} (H_\alpha \cap H'_{\alpha+1}) \right). \qquad (iii)$$

En general, fijándonos en los conjuntos de índices

$$\{i, j, k\} = \{0, 1, 2\} = \{x, y, z\},$$

si tenemos dos elementos a y b del bloque $\{a, b, c\}$ tal que $a, b \in H_i \cap H'_x$ dado que H_i y H'_x son subsistemas, el elemento c queda contenido en $H_i \cap H'_x$, pero si $a \in H_i \cap H'_x$ y $b \in H_j \cap H'_y$, como $\mathcal{H}$ y $\mathcal{H}'$ son familias de hiperplanos afines paralelos, sucede que $c \in H_k \cap H'_z$.

Con lo anterior, y la separación de conjuntos ajenos no-vacios de (ii) y (iii), por el Teorema 4.2.1, argumentamos la construcción de las familias de hiperplanos afines paralelos $\mathcal{H}'' = \{H''_0, H''_1, H''_2\}$ y $\mathcal{H}''' = \{H'''_0, H'''_1, H'''_2\}$, donde:

$$H''_0 := \bigcup_{\alpha \in \mathbb{Z}_3} (H_\alpha \cap H'_{2\alpha}),$$
$$H''_1 := \bigcup_{\alpha \in \mathbb{Z}_3} (H_\alpha \cap H'_{2\alpha+1}),$$
$$H''_2 := \bigcup_{\alpha \in \mathbb{Z}_3} (H_\alpha \cap H'_{2\alpha+2}),$$

$$H'''_0 := \bigcup_{\alpha \in \mathbb{Z}_3} (H_\alpha \cap H'_{\alpha}),$$
$$H'''_1 := \bigcup_{\alpha \in \mathbb{Z}_3} (H_\alpha \cap H'_{\alpha+1}),$$
$$H'''_2 := \bigcup_{\alpha \in \mathbb{Z}_3} (H_\alpha \cap H'_{\alpha+1}).$$

Así las cosas tenemos que:
$H''_i = \bigcup_{\alpha\in\mathbb{Z}_3} (H_\alpha \cap H'_{2\alpha+i})$ y $H'''_i = \bigcup_{\alpha\in\mathbb{Z}_3} (H_\alpha \cap H'_{\alpha+2i})$ para cada $i \in \{0,1,2\}$.
Si $x \in H''_i$ para alguna $i \in \{0,1,2\}$ entonces $x \in (H_\alpha \cap H'_{\alpha+i})$ para alguna $\alpha \in \mathbb{Z}_3$, razón por la cual, la distribución de peso en $\mathcal{H}''$, está dada por:

$$w_{\mathcal{H}''}(x) = i = \alpha + (2\alpha + i) = w_{\mathcal{H}}(x) + w_{\mathcal{H}'}(x), \forall x \in S.$$

Un razonamiento análogo nos lleva a la conclusión de que la distribución de peso en $\mathcal{H}'''$, es:

$$w_{\mathcal{H}'''}(x) = i = \alpha + 2(\alpha + 2i) = w_{\mathcal{H}}(x) + 2w_{\mathcal{H}'}(x), \forall x \in S.$$

Es claro que $w_{\mathcal{H}''}$ y $w_{\mathcal{H}'''}$ determinan a las familias de hiperplanos afines paralelos $\mathcal{H}''$ y $\mathcal{H}'''$ respectivamente.

□

Obsevación 2. Sea $\mathcal{H}$ una familia de hiperplanos afines paralelos en un $STS(v)$, notemos que el conjunto
$\mathcal{E}_{\mathcal{H}} = \{w_0, w_1, w_2, w_{\mathcal{H}}, w_{\mathcal{H}} + w_1, w_{\mathcal{H}} + w_2, 2w_{\mathcal{H}}, 2(w_{\mathcal{H}} + w_1), 2(w_{\mathcal{H}} + w_2)\}$, es un espacio vectorial de dimensión 2 sobre el campo $\mathbb{Z}_3$; ya que la suma de cualquier par de ellos y la multiplicación por escalares en $\mathbb{Z}_3$; es cerrada. De ahí que el espacio $\mathcal{W}$ que está constituido de todas las distribuciones de peso asociadas a todas las familias de hiperplanos afines paralelos de S, junto con las distribuciones constantes w_0,w_1 y w_2, es un espacio vectorial sobre $\mathbb{Z}_3$. Sea $d = dim(\mathcal{W})$. Entonces el conjunto de todas las familias de hiperplanos afines paralelos de S, tienen la misma estructura que el conjunto de todos los subespacios de de dimensión 2 en $\mathcal{W}$ que contienen a la línea $\{w_0, w_1, w_2\}$; que a su vez es isomorfa a la estructura de los subespacios de dimensión 1 (líneas) en el espacio cociente $\mathcal{W}/\{w_0, w_1, w_2\}$ de dimensión $d-1$, isomorfo a la estructura de los hiperplano afines en el Espacio Afín de dimensión $d-1$ (relacionando a cada línea afín con su hiperplano afín ortogonal). En este contexto, para un $STS(v)$, definimos la **dimensión Afín** $d_{\mathcal{A}} := d - 1$.

Teorema 4.2.3 *Dado un Sistema Triple de Steiner S, con $v \geq 3$;*

$$Rango_3 S = v - (d_{\mathcal{A}} + 1).$$

Demostración. Sea M una matriz de incidencia de S que tiene columnas $C_1, C_2, ..., C_v$. Análogamente a la demostración del $2 - rango$, resulta que:

$Rango_3 S = v - dim(kernel(L_M))$,
donde $kernel(L_M) = \{\bar{x} \in \mathbb{Z}_3^v : M\bar{x} = \bar{0}_{b\times 1}\}$
$= \{(x_1, x_2, ..., x_v) \in \mathbb{Z}_3^v : x_1C_1 + x_2C_2 + \cdots + x_vC_v = \bar{0}_{b\times 1}\} = \mathcal{W}$,
$\Longrightarrow Rango_3 S = v - dim(\mathcal{W}) = v - (dim(\mathcal{H}) + 1) = v - (d_{\mathcal{A}} + 1)$.

□

El siguiente Teorema resume este capítulo.

Teorema 4.2.4 *Dado un Sistema Triple de Steiner $S(2, 3, v)$ con $v > 3$, entonces:*

$Rango_p STS(v) = v \qquad \forall p \neq 2, 3,$

$Rango_2 STS(v) = v - (d_{\mathcal{P}} + 1),$

$Rango_3 STS(v) = v - (d_{\mathcal{A}} + 1).$

Capítulo 5

Construcción de Sistemas Triples de Steiner no-isomorfos

Sean S_1 y S_2 Sistemas Triples de Steiner con v puntos y matrices de incidencia M_1 y M_2 respectivamente. De la definición que tenemos de isomorfismo para estructuras de incidencia; es indudable que si M_1 y M_2 son iguales entonces S_1 y S_2 son isomorfos. En el mismo sentido; S_1 y S_2 son isomorfos si y sólo si podemos obtener M_2 a partir de M_1 intercambiando renglones y columnas. Aclarado este punto, es evidente el siguiente hecho;

Proposición 5.0.3 *Sean S_1 y S_2 Sistemas Triples de Steiner con v puntos y matrices de incidencia M_1 y M_2 respectivamente, entonces S_1 y S_2 son isomorfos si y sólo si existe una matriz M tal que podemos llegar de M_i a M intercambiando renglones y columnas, para $i = 1, 2$.*

De los Corolarios 1.1.1 y 1.1.2 sabemos que existe el $STS(2^{n+1} - 1)$ y el $STS(3^n)$ para cualquier $n \in \mathbb{N}$, entonces, por el momento, nos interesa saber si son únicos salvo isomorfismos o no.

Proposición 5.0.4 *Si $v = 3, 7$ ó 9, el $STS(v)$ es único salvo isomorfismos.*

Demostración. Cuando $v = 3$, es trivial el resultado.

Si $v = 7$, sea M_1 una matriz asociada a un $STS(7)$, entonces cosiderando que: por cada par de puntos pasa un único bloque, cada bloque tiene tres puntos y cada punto pertenece a 3 bloques, siempre podemos intercambiar renglones y columnas de M_1 de tal manera que coincida con esta primera parte de la estructura de una matriz general:

	p_1	p_2	p_3	p_4	p_5	p_6	p_7
l_1	1	1	1	0	0	0	0
l_2	1	0	0	1	1	0	0
l_3	1	0	0	0	0	1	1
l_4	0	1	0				
l_5	0	1	0				
l_6	0	0	1				
l_7	0	0	1				

Para continuar y con el fín de evitar argumentos repetitivos, es mejor que veamos como se obtiene una matriz general por medio pasos en los que se va determinando una estructura general. En cada paso de la siguiente construcción, las entradas de la matriz que están encerradas en cuadros quedan determinadas por las que están en negritas.

	p_1	p_2	p_3	p_4	p_5	p_6	p_7
l_1	1	1	1	0	0	0	0
l_2	1	0	0	**1**	**1**	0	0
l_3	1	0	0	0	0	1	1
$\mapsto$ l_4	0	1	0	$\boxed{1}$	$\boxed{0}$		
l_5	0	1	0	$\boxed{0}$	$\boxed{1}$		
l_6	0	0	1	$\boxed{1}$	$\boxed{0}$		
l_7	0	0	1	$\boxed{0}$	$\boxed{1}$		

$\mapsto$

	p_1	p_2	p_3	p_4	p_5	p_6	p_7
l_1	1	1	1	0	0	0	0
l_2	1	0	0	1	1	0	0
l_3	1	0	0	0	0	1	1
l_4	0	**1**	0	**1**	0	$\boxed{1}$	$\boxed{0}$
l_5	0	1	0	0	1		
l_6	0	0	1	1	0		
l_7	0	0	1	0	1		

	p_1	p_2	p_3	p_4	p_5	p_6	p_7
l_1	1	1	1	0	0	0	0
l_2	1	0	0	1	1	0	0
l_3	1	0	0	0	0	1	1
$\mapsto$ l_4	0	**1**	0	**1**	0	**1**	0
l_5	0	**1**	0	0	1	$\boxed{0}$	
l_6	0	0	1	**1**	0	$\boxed{0}$	
l_7	0	0	1	0	1	$\boxed{1}$	

$\mapsto$

	p_1	p_2	p_3	p_4	p_5	p_6	p_7
l_1	1	1	1	0	0	0	0
l_2	1	0	0	1	1	0	0
l_3	1	0	0	0	0	1	1
l_4	0	1	0	1	0	1	0
l_5	0	**1**	0	0	**1**	0	$\boxed{1}$
l_6	0	0	**1**	**1**	0	0	$\boxed{1}$
l_7	0	0	**1**	0	**1**	**1**	$\boxed{0}$

Entonces cualquier matriz de incidencia de un Sistema Triple de Steiner con 7 puntos puede llevarse a través de intercambios de renglones y columnas a una matriz general, entonces todos los Sistemas Triples de Steiner con 7 puntos son isomorfos.

Hagamos lo mismo cuando $v = 9$, ahora tomando en cuenta que por cada par de puntos pasa un único bloque, cada bloque tiene tres puntos y cada punto pertenece a 4 bloques.

	p_0	p_1	p_2	p_3	p_4	p_5	p_6	p_7	p_8
l_1	1	1	1	0	0	0	0	0	0
l_2	1	0	0	1	1	0	0	0	0
l_3	1	0	0	0	0	1	1	0	0
l_4	1	0	0	0	0	0	0	1	1
l_5	0	1	0						
l_6	0	1	0						
l_7	0	1	0						
l_8	0	0	1						
l_9	0	0	1						
l_{10}	0	0	1						
l_{11}	0	0	0						
l_{12}	0	0	0						

$\mapsto$

	p_0	p_1	p_2	p_3	p_4	p_5	p_6	p_7	p_8
l_1	1	1	1	0	0	0	0	0	0
l_2	1	0	0	1	1	0	0	0	0
l_3	1	0	0	0	0	1	1	0	0
l_4	1	0	0	0	0	0	0	1	1
l_5	0	**1**	0	1	0	0	1	0	0
l_6	0	**1**	0						
l_7	0	**1**	0						
l_8	0	0	1						
l_9	0	0	1						
l_{10}	0	0	1						
l_{11}	0	0	0						
l_{12}	0	0	0						

	p_0	p_1	p_2	p_3	p_4	p_5	p_6	p_7	p_8
l_1	1	1	1	0	0	0	0	0	0
l_2	1	0	0	1	1	0	0	0	0
l_3	1	0	0	0	0	1	1	0	0
l_4	1	0	0	0	0	0	0	1	1
l_5	0	**1**	0	**1**	0	0	**1**	0	0
l_6	0	**1**	0	0			0		
l_7	0	**1**	0	0			0		
l_8	0	0	**1**	1					
l_9	0	0	**1**	0					
l_{10}	0	0	**1**	0					
l_{11}	0	0	0	1					
l_{12}	0	0	0	0					

$\mapsto$

	p_0	p_1	p_2	p_3	p_4	p_5	p_6	p_7	p_8
l_1	1	1	1	0	0	0	0	0	0
l_2	1	0	0	1	1	0	0	0	0
l_3	1	0	0	0	0	1	1	0	0
l_4	1	0	0	0	0	0	0	1	1
l_5	0	1	0	**1**	0	0	**1**	0	0
l_6	0	1	0	0			0		
l_7	0	1	0	0			0		
l_8	0	0	1	1			0		
l_9	0	0	**1**	0			1		
l_{10}	0	0	**1**	0			0		
l_{11}	0	0	0	**1**			0		
l_{12}	0	0	0	0			1		

	p_0	p_1	p_2	p_3	p_4	p_5	p_6	p_7	p_8
l_1	1	1	1	0	0	0	0	0	0
l_2	1	0	0	1	1	0	0	0	0
l_3	1	0	0	0	0	1	1	0	0
l_4	1	0	0	0	0	0	0	**1**	**1**
l_5	0	1	0	1	0	0	1	0	0
l_6	0	**1**	0	0	1	0	0		
l_7	0	**1**	0	0	0	1	0		
l_8	0	0	1	1			0		
l_9	0	0	1	0			1		
l_{10}	0	0	1	0			0		
l_{11}	0	0	0	1			0		
l_{12}	0	0	0	0			1		

$\mapsto$

	p_0	p_1	p_2	p_3	p_4	p_5	p_6	p_7	p_8
l_1	1	1	1	0	0	0	0	0	0
l_2	1	0	0	**1**	**1**	0	0	0	0
l_3	1	0	0	0	0	1	1	0	0
l_4	1	0	0	0	0	0	0	1	1
l_5	0	1	0	1	0	0	1	0	0
l_6	0	1	0	0	1	0	0		
l_7	0	1	0	0	0	1	0		
l_8	0	0	1	**1**	0		0		
l_9	0	0	**1**	0			1		
l_{10}	0	0	**1**	0			0		
l_{11}	0	0	0	**1**	0		0		
l_{12}	0	0	0	0	1		1		

	p_0	p_1	p_2	p_3	p_4	p_5	p_6	p_7	p_8
l_1	1	1	1	0	0	0	0	0	0
l_2	1	0	0	1	1	0	0	0	0
l_3	1	0	0	0	0	**1**	**1**	0	0
l_4	1	0	0	0	0	0	0	1	1
l_5	0	1	0	1	0	0	1	0	0
$\mapsto$ l_6	0	1	0	0	1	0	0		
l_7	0	1	0	0	0	1	0		
l_8	0	0	1	1	0		0		
l_9	0	0	1	0	$\boxed{0}$	$\boxed{0}$	**1**		
l_{10}	0	0	1	0	$\boxed{1}$		0		
l_{11}	0	0	0	1	0		0		
l_{12}	0	0	0	0	**1**	$\boxed{0}$	**1**		

	p_0	p_1	p_2	p_3	p_4	p_5	p_6	p_7	p_8
l_1	1	1	1	0	0	0	0	0	0
l_2	1	0	0	1	1	0	0	0	0
l_3	1	0	0	0	0	1	1	0	0
l_4	1	0	0	0	0	0	0	1	1
l_5	0	1	0	1	0	0	1	0	0
$\mapsto$ l_6	0	**1**	0	0	**1**	0	0	$\boxed{1}$	$\boxed{0}$
l_7	0	1	0	0	0	1	0		
l_8	0	0	1	1	0		0		
l_9	0	0	1	0	0	0	1		
l_{10}	0	0	1	0	1		0		
l_{11}	0	0	0	1	0		0		
l_{12}	0	0	0	0	1	0	1		

	p_0	p_1	p_2	p_3	p_4	p_5	p_6	p_7	p_8
l_1	1	1	1	0	0	0	0	0	0
l_2	1	0	0	1	1	0	0	0	0
l_3	1	0	0	0	0	1	1	0	0
l_4	1	0	0	0	0	0	0	1	1
l_5	0	1	0	1	0	0	1	0	0
$\mapsto$ l_6	0	**1**	0	0	**1**	0	0	**1**	0
l_7	0	**1**	0	0	0	1	0	$\boxed{0}$	$\boxed{1}$
l_8	0	0	1	1	0		0		
l_9	0	0	1	0	0	0	1		
l_{10}	0	0	1	0	**1**		0	$\boxed{0}$	
l_{11}	0	0	0	1	0		0		
l_{12}	0	0	0	0	**1**	0	1	$\boxed{0}$	$\boxed{1}$

	p_0	p_1	p_2	p_3	p_4	p_5	p_6	p_7	p_8
l_1	1	1	1	0	0	0	0	0	0
l_2	1	0	0	1	1	0	0	0	0
l_3	1	0	0	0	0	1	1	0	0
l_4	1	0	0	0	0	0	0	1	1
l_5	0	1	0	1	0	0	1	0	0
$\mapsto$ l_6	0	1	0	0	1	0	0	1	0
l_7	0	1	0	0	0	1	0	0	1
l_8	0	0	1	1	0		0		
l_9	0	0	1	0	0	0	**1**	$\boxed{1}$	$\boxed{0}$
l_{10}	0	0	1	0	**1**	$\boxed{1}$	0	0	$\boxed{0}$
l_{11}	0	0	0	1	0		0		
l_{12}	0	0	0	0	**1**	0	**1**	0	**1**

	p_0	p_1	p_2	p_3	p_4	p_5	p_6	p_7	p_8
l_1	1	1	1	0	0	0	0	0	0
l_2	1	0	0	1	1	0	0	0	0
l_3	1	0	0	0	0	1	1	0	0
l_4	1	0	0	0	0	0	0	**1**	1
l_5	0	1	0	1	0	0	1	0	0
$\mapsto$ l_6	0	1	0	0	1	0	0	**1**	0
l_7	0	1	0	0	0	1	0	0	1
l_8	0	0	**1**	1	0	$\boxed{0}$	0	$\boxed{0}$	$\boxed{1}$
l_9	0	0	**1**	0	0	0	1	**1**	0
l_{10}	0	0	**1**	0	1	**1**	0	0	0
l_{11}	0	0	0	1	0	$\boxed{1}$	0		
l_{12}	0	0	0	0	1	0	1	0	1

	p_0	p_1	p_2	p_3	p_4	p_5	p_6	p_7	p_8
l_1	1	1	1	0	0	0	0	0	0
l_2	1	0	0	1	1	0	0	0	0
l_3	1	0	0	0	0	1	1	0	0
l_4	1	0	0	0	0	0	0	**1**	1
l_5	0	1	0	1	0	0	1	0	0
$\mapsto$ l_6	0	1	0	0	1	0	0	**1**	0
l_7	0	1	0	0	0	1	0	0	1
l_8	0	0	1	1	0	0	0	0	1
l_9	0	0	1	0	0	0	1	**1**	0
l_{10}	0	0	1	0	1	1	0	0	0
l_{11}	0	0	0	1	0	1	0	$\boxed{1}$	$\boxed{0}$
l_{12}	0	0	0	0	1	0	1	0	1

□

5.1. Dos $STS(2^{n+1}-1)$ no-isomorfos con $n > 2$

Consideremos la estructura de incidencia $\mathcal{S}^2$ conformada por los puntos y las líneas del Espacio Proyectivo $PG(n, 2)$, con $n > 2$. Por el Teorema 2.4.3, $\mathcal{S}^2$ es un $STS(2^{n+1}-1)$. Decimos que $\mathcal{S}^2$ es el $STS(2^{n+1}-1)$ **clásico** asociado a la Geometría Proyectiva. Como $v = 2^{n+1} - 1$; la cantidad de líneas es:

$$b = \frac{v(v-1)}{6} = \frac{(2^{n+1}-1)2(2^n-1)}{6} = \frac{(2^{n+1}-1)(2^n-1)}{3}.$$

Teorema 5.1.1 *Sean α, β y γ tres puntos diferentes dos a dos en $\mathcal{S}^2$ entonces; α, β y γ pertenecen a una línea en $\mathcal{S}^2$ si y sólo si $\alpha + \beta + \gamma = \bar{0}$ en el campo $\mathbb{Z}_2$.*

Demostración. Los puntos en $\mathcal{S}^2$ son puntos proyectivos en $PG(n, 2)$ que a su vez son rectas por el origen en $\mathbb{Z}_2^{n+1}$. Las líneas en $\mathcal{S}^2$ son líneas proyectivas en $PG(n, 2)$ que a su vez son planos por el origen en $\mathbb{Z}_2^{n+1}$. Pero en $\mathbb{Z}_2^{n+1}$ cada recta por el origen tiene a dos únicos puntos; el origen y otro distinto de él, y cualquier vector genera una recta por el origen en $\mathbb{Z}_2^{n+1}$, es decir, los puntos proyectivos de $PG(n, 2)$ son justamente todos los vectores diferentes del vector cero en $\mathbb{Z}_2^{n+1}$. Por esa razón, si un plano por el origen, en $\mathbb{Z}_2^{n+1}$, pasa por dos vectores $\bar{u}$ y $\bar{v}$, diferentes entre si y del vector cero; existe un único vector, diferente de $\bar{u}$, $\bar{v}$ y del vector cero, que pertenece a ese plano, y es justamante $\bar{u} + \bar{v}$. Recíprocamente, si $\bar{u}$, $\bar{v}$ y $\bar{w}$ son vectores diferentes dos a dos y del vector cero, y sucede que; $\bar{u} + \bar{v} + \bar{w} = \bar{0} \Longrightarrow \bar{w} = \bar{u} + \bar{v}$, es decir, $\bar{w}$ pertenece al plano generado por $\bar{u} + \bar{v}$.

□

Ya vimos que los puntos de $\mathcal{S}^2$ son los vectores de $\mathbb{Z}_2^{n+1}$ distintos del vector cero. Por ello, conviene ver a los puntos de $\mathcal{S}^2$ como la reprecentación de cada número natural del 1 al v en base 2, de manera que el punto p_i es el vector $(v_1, v_2, ..., v_{n+1})$ tal que $\sum_{k=1}^{n+1} v_k 2^{k-1} = i$.

Sea M^2 una matriz de incidencia de $\mathcal{S}^2$, que tiene ordenadas las columnas de acuerdo al orden del índice de los puntos . Entonces, el espacio generado por los renglones de M^2 en el campo $\mathbb{Z}_2$; es el código $C_2(\mathcal{S}^2)$.

Proposición 5.1.1 *Sean $p_1, p_2, ..., p_v$ los puntos de $\mathcal{S}^2$. Entonces, para cualquier*

palabra $\bar{a} = (a_1, a_2, ..., a_v) \in C_2(\mathcal{S}^2)$*, resulta que:*

$$\sum_{j=1}^{v} a_j p_j = \bar{0}.$$

Demostración. Sean $l_1, l_2, ..., l_b$ las líneas de $\mathcal{S}^2$, como $\bar{a} \in C_2(\mathcal{S}^2)$, ocurre que,

$$\bar{a} = \sum_{i=1}^{b} \lambda_i \chi(l_i),$$

con $\lambda_i \in \mathbb{Z}_2$, entonces, $a_j = \sum_{i=1}^{b} \lambda_i \chi_{p_j}(l_i)$ y así;

$$\sum_{j=1}^{v} a_j p_j = \sum_{j=1}^{v} \Big(\sum_{i=1}^{b} \lambda_i \chi_{p_j}(l_i) \Big) p_j = \sum_{i=1}^{b} \lambda_i \Big(\sum_{j=1}^{v} \chi_{p_j}(l_i) p_j \Big) = \bar{0}.$$

□

Corolario 5.1.1 $d(C_2(\mathcal{S}^2)) = 3$.

Demostración. Como todas las palabras en la matriz de incidencia tienen peso 3, entonces la distancia mínima es a lo más 3:

a) como ningún punto es el vector cero; no puede haber palabras de peso 1,

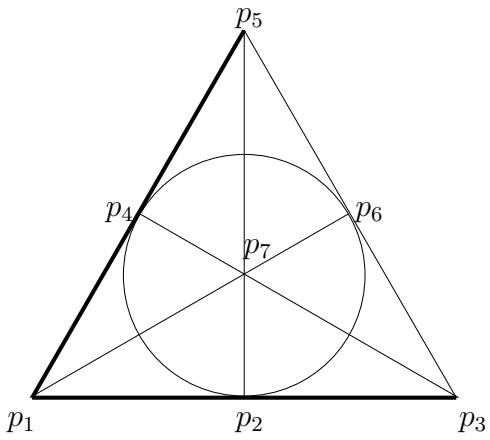
b) si hubiera una palabra $\bar{a}$ de peso 2; sumándole el vector de incidencia de la línea que pasa por los dos puntos en los que $\bar{a}$ tiene coeficientes diferentes de cero, obtenemos una palabra de peso 1. Por *a*), dicha palabra $\bar{a}$ no existe.

Por lo tanto, la distancia mínima $d = 3$.

□

Ahora, como
$p_1 + p_2 + p_3 = (1, 0, 0, 0, ..., 0) + (0, 1, 0, 0, ..., 0) + (1, 1, 0, 0, ..., 0) = \bar{0}$ y
$p_1 + p_4 + p_5 = (1, 0, 0, 0, ..., 0) + (0, 0, 1, 0, ..., 0) + (1, 0, 1, 0, ..., 0) = \bar{0}$,

tomemos las líneas proyectivas $\{p_1, p_2, p_3\}$ y $\{p_1, p_4, p_5\}$ en $PG(n, 2)$ entonces $\langle \{p_1, p_2, p_3\}, \{p_1, p_4, p_5\} \rangle$ es un plano proyectivo en $PG(n, 2)$, por el Corolario 2.4.1, $S^2 := PG(\langle \{p_1, p_2, p_3\}, \{p_1, p_4, p_5\} \rangle)$ es isomorfo a $PG(2, 2)$, luego, por el Corolario 2.4.2 es un Sistema Triple de Steiner con 7 puntos, es decir, S^2 es un subsistema de $\mathcal{S}^2$ con 7 puntos;



Subsistema de $\mathcal{S}^2$ con 7 puntos.

$S^2 = (P, L)$, donde:
$P = \{p_1, p_2, p_3, p_4, p_5, p_6, p_7\}$,
$L = \{p_1, p_2, p_3\}, \{p_1, p_4, p_5\}, \{p_1, p_6, p_7\}, \{p_2, p_4, p_6\}, \{p_2, p_5, p_7\}, \{p_3, p_4, p_7\}, \{p_3, p_5, p_6\}$.

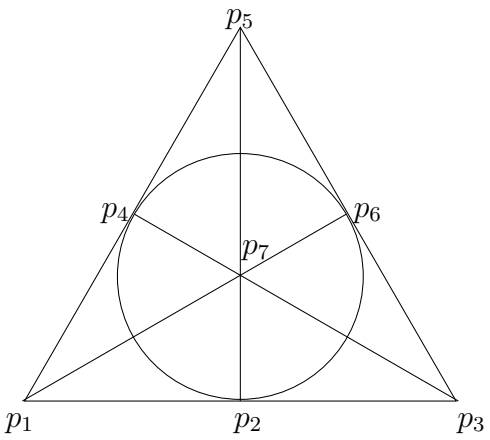
Nótese que la estructura de incidencia $S'^2 = (P', L')$, con;
$P' = \{p_1, p_2, p_3, p_4, p_5, p_6, p_7\}$,
$L' = \{\{p_1, p_2, p_3\}, \{p_1, p_4, p_5\}, \{p_1, p_6, p_7\}, \{p_3, p_4, p_6\}, \{p_3, p_5, p_7\}, \{p_2, p_4, p_7\}, \{p_2, p_5, p_6\}$

es isomorfa a S^2, debido a que;

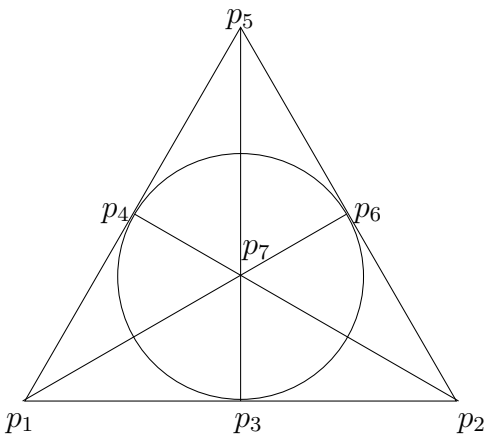
$$\begin{aligned} \phi : S^2 &\longrightarrow S'^2 \\ p_1 &\mapsto p_1 \\ p_2 &\mapsto p_3 \\ p_3 &\mapsto p_2 \\ p_4 &\mapsto p_4 \\ p_5 &\mapsto p_5 \\ p_6 &\mapsto p_6 \\ p_7 &\mapsto p_7 \end{aligned}$$

es un isomorfismo de S^2 en S'^2, ya que lo único que estamos haciendo; es un cambio de nombres, pero manteniendo la estructura del subsistema, como a continuación se muestra:

Sea $\mathcal{S}'^2$ la estructura de incidencia que consiste de los mismos puntos de $\mathcal{S}'^2$ y donde sus líneas son: las líneas de S'^2 y las líneas de $\mathcal{S}^2$ excepto las que se encuentran en S^2.



Subsistema original.



Subsistema con el cambio.

Teorema 5.1.2 *$\mathcal{S}'^2$ es un $STS(2^{n+1}-1)$.*

Demostración. $\mathcal{S}'^2$ tiene $2^{n+1}-1$ puntos y todas sus líneas tienen 3 puntos. Ahora, sean p_i y p_j dos puntos en S'^2:

si p_i y p_j pertenecen a S^2 en $\mathcal{S}^2$, entonces, por ser S^2 subsistema, la única línea que los contiene en $\mathcal{S}^2$ se encuentra en S^2, y como S^2 es isomorfo a S'^2, existe una única línea en $\mathcal{S}'^2$ que contiene a p_i y p_j,

si al menos uno de los puntos p_i y p_j no pertenece a S^2 en $\mathcal{S}^2$, entonces, por ser S^2 subsistema, no existe ninguna línea en S^2 a la que le pertenezcan por lo tanto no existe ninguna línea en S'^2 que los contenga, entonces, la única línea que los contiene se encuentra en las líneas de $\mathcal{S}'^2$ excepto las que están en S^2. Por lo tanto, existe una única línea en $\mathcal{S}'^2$ que contiene a p_i y p_j.

□

Teorema 5.1.3 *$\mathcal{S}'^2$ no es isomorfo a $\mathcal{S}^2$.*

Demostración. Sea $C_2(\mathcal{S}'^2)$ el código generado por alguna matriz de incidencia de $\mathcal{S}'^2$. Las líneas $\{p_1, p_2, p_3\}$ y $\{p_3, p_5, p_7\}$ pertenece a S'^2 y como;
$p_2 + p_8 + p_{10} = (0,1,0,0,...,0) + (0,0,0,1,0,...,0) + (0,1,0,1,...,0) = \bar{0}$,
$p_5 + p_8 + p_{13} = (1,0,1,0,...,0) + (0,0,0,1,0,...,0) + (1,0,1,1,0,...,0) = \bar{0}$ y
$p_7 + p_{10} + p_{13} = (1,1,1,0,...,0) + (0,1,0,1,0,...,0) + (1,0,1,1,0,...,0) = \bar{0}$,

tenemos que las líneas $\{p_2, p_8, p_{10}\}$ $\{p_5, p_8, p_{13}\}$ y $\{p_7, p_{10}, p_{13}\}$ de $\mathcal{S}^2$, no pertenecen a S^2, por lo tanto, pertenecen a $\mathcal{S'}^2$ y entonces cualquier combinación lineal de los vectores de incidencia correspondientes a estas líneas pertenece a $C_2(\mathcal{S'}^2)$, en particular la que se muestra;

	p_1	p_2	p_3	p_4	p_5	p_6	p_7	p_8	p_9	p_{10}	p_{11}	p_{12}	p_{13}	p_{14}	p_{15}	$\cdots$	$p_{2^{n+1}-1}$
2^0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	$\cdots$	1
2^1	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	$\cdots$	1
2^2	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	$\cdots$	1
2^3	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	$\cdots$	1
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\cdots$	$\vdots$
2^n	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	$\cdots$	1
$\chi(\{p_2, p_8, p_{10}\})$	0	**1**	0	0	0	0	0	**1**	0	**1**	0	0	0	0	0	$\cdots$	0
$+\chi(\{p_5, p_8, p_{13}\})$	0	0	0	0	**1**	0	0	**1**	0	0	0	0	**1**	0	0	$\cdots$	0
$+\chi(\{p_7, p_{10}, p_{13}\})$	0	0	0	0	0	0	**1**	0	0	**1**	0	0	**1**	0	0	$\cdots$	0
$+\chi(\{p_1, p_2, p_3\})$	**1**	**1**	**1**	0	0	0	0	0	0	0	0	0	0	0	0	$\cdots$	0
$+\chi(\{p_3, p_5, p_7\})$	0	0	**1**	0	**1**	0	**1**	0	0	0	0	0	0	0	0	$\cdots$	0
$=$	**1**	0	0	0	0	0	0	0	0	0	0	0	0	0	0	$\cdots$	0

Por lo que $C(\mathcal{S'}^2)$ tienen una palabra de peso 1, entonces

$$d(C_2(\mathcal{S'}^2)) = 1 \neq 3 = d(C_2(\mathcal{S}^2)),$$

por el Teorema 3.1.1 $C_2(\mathcal{S}^2)$ y $C_2(\mathcal{S'}^2)$ no son equivalentes y por el Teorema 3.2.1 los Sistemas Triples de Steiner $\mathcal{S'}^2$ y $\mathcal{S}^2$ no son isomorfos.

□

5.2. Dos $STS(3^n)$ no-isomorfos con $n > 2$

Consideremos la estructura de incidencia $\mathcal{S}^3$ conformada por los puntos y las líneas del Espacio Afín $AG(n, 3)$, con $2 < n$. Por el Teorema 2.3.4 sabemos que $\mathcal{S}^3$ es un $STS(3^n)$. Decimos que $\mathcal{S}^3$ es el $STS(3^n)$ **clásico** asociado a la Geometría Afín. Dado que $v = 3^n$; la cantidad de líneas es:

$$b = \frac{v(v-1)}{6} = \frac{3^n(3^n-1)}{6} = \frac{3^{n-1}(3^n-1)}{2}.$$

Teorema 5.2.1 *Sean α, β y γ tres puntos diferentes dos a dos en $\mathcal{S}^3$ entonces; α, β y γ pertenecen a una línea en $\mathcal{S}^3$ si y sólo si $\alpha + \beta + \gamma = \bar{0}$ en el campo $\mathbb{Z}_3$.*

Demostración. Los puntos en $\mathcal{S}^3$ son puntos afines en $AG(n,3)$, es decir, son los vectores de $\mathbb{Z}_3^n$. Las líneas en $\mathcal{S}^3$ son líneas afines en $AG(n,3)$ que a su vez son las rectas por el origen y sus trasladadas; una recta por el origen es el subespacio generado por un vector diferente de cero, por lo que una línea que no pase por el origen se puede expresar como un subespacio generado por un vector, diferente de cero, más un vector fijo. Pero en $\mathbb{Z}_3^n$ cada recta por el origen tiene a tres únicos puntos; el origen y otro distinto de él y su doble. Y cualquier vector genera una recta por el origen en $\mathbb{Z}_3^n$. Por esa razón, si una línea pasa por dos vectores $\bar{u}$ y $\bar{v}$, diferentes entre si; existe un único vector, diferente de $\bar{u}$, $\bar{v}$, que pertenece a esa línea, y es justamante $2(\bar{u}+\bar{v})$. Recíprocamente, si $\bar{u}$, $\bar{v}$ y $\bar{w}$ son vectores diferentes dos a dos, y sucede que; $\bar{u}+\bar{v}+\bar{w}=0 \Longrightarrow \bar{w}=2(\bar{u}+\bar{v})$, es decir, $\bar{w}$ pertenece a la línea que pasa por $\bar{u}+\bar{v}$.

□

Sabemos que los puntos de $\mathcal{S}^3$ son los vectores de $\mathbb{Z}_3^n$. Análogamente a la sección anterior, veamos a los puntos de $\mathcal{S}^3$ como la representación de cada número natural del 0 al $v-1$ en base 3, de manera que el punto p_i es el vector $(v_1, v_2, ..., v_n)$ tal que $\sum_{k=1}^{n} v_k 3^{k-1} = i$.

Sea M^3 una matriz de incidencia de $\mathcal{S}^3$, que tiene en la columna i las incidencias del punto $i+1$. Entonces, el espacio generado por los renglones de M^3 en el campo $\mathbb{Z}_3$; es el código $C_3(\mathcal{S}^3)$.

Proposición 5.2.1 *Sean $p_0, p_1, ..., p_{v-1}$ los puntos de $\mathcal{S}^3$. Entonces, para cualquier palabra $\bar{a} = (a_0, a_1, ..., a_{v-1}) \in C_3(\mathcal{S}^3)$, resulta que:*

i) $\sum_{j=0}^{v-1} a_j = 0,$

ii) $\sum_{j=0}^{v-1} a_j p_j = \bar{0}.$

Demostración. Sean $l_1, l_2, ..., l_b$ las líneas de $\mathcal{S}^3$, como $\bar{a} \in C_3(\mathcal{S}^3)$ se tiene que;

$$\bar{a} = \sum_{i=1}^{b} \lambda_i \chi(l_i),$$

con $\lambda_i \in \mathbb{Z}_3$, entonces, $a_j = \sum_{i=1}^{b} \lambda_i \chi_{p_j}(l_i)$ y así;

1) $\sum_{j=0}^{v-1} a_j = \sum_{j=0}^{v-1} \Big(\sum_{i=1}^{b} \lambda_i \chi_{p_j}(l_i) \Big) = \sum_{i=1}^{b} \lambda_i \Big(\sum_{j=0}^{v-1} \chi_{p_j}(l_i) \Big) = 0,$

2) $\sum_{j=0}^{v-1} a_j p_j = \sum_{j=0}^{v-1} \Big(\sum_{i=1}^{b} \lambda_i \chi_{p_j}(l_i) \Big) p_j = \sum_{i=1}^{b} \lambda_i \Big(\sum_{j=0}^{v-1} \chi_{p_j}(l_i) p_j \Big) = \bar{0}.$

□

Corolario 5.2.1 $d(C_3(\mathcal{S}^3)) = 3$.

Demostración. Como todas las palabras en la matriz de incidencia tienen peso 3, entonces la distancia mínima es a lo más 3:

a) Por 1) de la Proposición anterior, no puede haber palabras de peso 1.

b) Si hubiera una palabra $\bar{a}$ de peso 2 con coeficientes iguales; sumandole el doble del vector de incidencia de la línea que pasa por los dos puntos en los que $\bar{a}$ tiene coeficientes diferentes de cero, obtenemos una palabra de peso 1. Por *a*), dicha palabra $\bar{a}$ no existe.

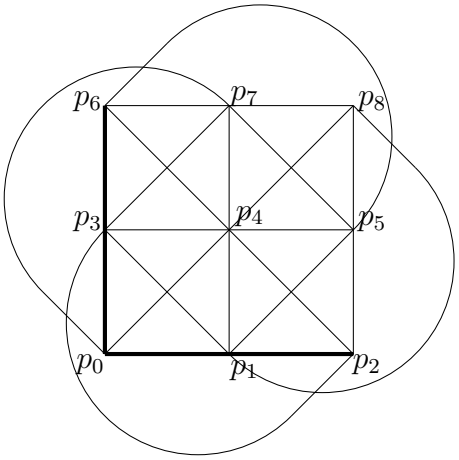
c) Si hubiera una palabra $\bar{a}$ de peso 2 con coeficientes diferentes, digamos $a_i = 1$ y $a_j = 2$; por 2) de la Proposición anterior;
$a_i p_i + a_j p_j = p_i + 2p_j = \bar{0} \Longrightarrow p_i = p_j \Longrightarrow i = j \Longrightarrow a_i = a_j$, contradiciendo nuestro caso.

Por lo tanto, $d(C_3(\mathcal{S}^3)) = 3$.

□

Como,
$p_0 + p_1 + p_2 = (0,0,0,0,...,0) + (1,0,0,0,...,0) + (2,0,0,0,...,0) = \bar{0}$ y
$p_0 + p_3 + p_6 = (0,0,0,0,...,0) + (0,1,0,0,...,0) + (0,2,0,0,...,0) = \bar{0},$

$\{p_1, p_2, p_3\}$ y $\{p_1, p_4, p_5\}$ son líneas de $\mathcal{S}^3$ y, por tanto, líneas de $AG(n,2)$, entonces $\langle \{p_0, p_1, p_2\}, \{p_0, p_3, p_6\} \rangle$ es un plano afín en $AG(n,2)$, por el Corolario 2.3.1; $S^3 := AG(\langle \{p_0, p_1, p_2\}, \{p_0, p_3, p_6\} \rangle)$ es isomorfo a $AG(2,2)$, luego, por el Corolario 2.3.2 es un Sistema Triple de Steiner con 9 puntos, es decir, S^3 es un subsistema de $\mathcal{S}^3$ con 9 puntos;



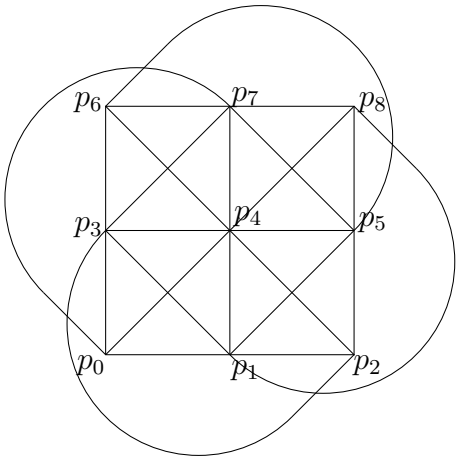
Subsistema de $\mathcal{S}^3$ con 9 puntos.

$S^3 = (P, L)$, donde:
$P = \{p_0, p_1, p_2, p_3, p_4, p_5, p_6, p_7, p_8\}$,
$L = \{\{p_0, p_1, p_2\}, \{p_0, p_3, p_6\}, \{p_0, p_4, p_8\}, \{p_0, p_5, p_7\}, \{p_1, p_3, p_8\}, \{p_1, p_5, p_6\},$
$\{p_1, p_4, p_7\}, \{p_2, p_3, p_7\}, \{p_2, p_5, p_8\}, \{p_2, p_4, p_6\}, \{p_3, p_4, p_5\}, \{p_6, p_7, p_8\}\}$.

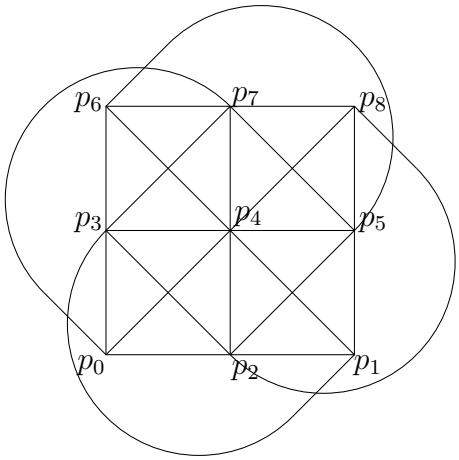
Nótese que la estructura de incidencia $S'^3 = (P', L')$, con;
$P' = \{p_0, p_1, p_2, p_3, p_4, p_5, p_6, p_7, p_8\}$,
$L' = \{\{p_0, p_1, p_2\}, \{p_0, p_3, p_6\}, \{p_0, p_4, p_8\}, \{p_0, p_5, p_7\}, \{p_2, p_3, p_8\}, \{p_2, p_5, p_6\},$
$\{p_2, p_4, p_7\}, \{p_1, p_3, p_7\}, \{p_1, p_5, p_8\}, \{p_1, p_4, p_6\}, \{p_3, p_4, p_5\}, \{p_6, p_7, p_8\}\}$,
es isomorfa a S^3, debido a que;

$$\begin{aligned}
\psi : S^3 &\longrightarrow S'^3 \\
p_0 &\mapsto p_0 \\
p_1 &\mapsto p_2 \\
p_2 &\mapsto p_1 \\
p_3 &\mapsto p_3 \\
p_4 &\mapsto p_4 \\
p_5 &\mapsto p_5 \\
p_6 &\mapsto p_6 \\
p_7 &\mapsto p_7 \\
p_8 &\mapsto p_8
\end{aligned}$$

es un isomorfismo de S^3 en S'^3, por que lo único que estamos haciendo es un cambio de nombres pero manteniendo la estructura del subsistema, como se ilustra a continuación:



Subsistema original.



Subsistema con el cambio.

Entonces, consideremos a la estructura de incidencia $\mathcal{S}'^3$ que tiene los mismos puntos de $\mathcal{S}^3$ y tal que sus líneas son las líneas de S'^3 y las líneas de $\mathcal{S}^3$ excepto las que están en S^3.

Teorema 5.2.2 *$\mathcal{S}'^3$ es un $STS(3^n)$.*

Demostración. $\mathcal{S}'^3$ tiene 3^n puntos y todas sus líneas tiene 3 puntos. Ahora, sean p_i y p_j dos puntos en $\mathcal{S}'^3$:

si p_i y p_j pertenecen a S^3 en $\mathcal{S}^3$, entonces, por ser S^3 subsistema, la única línea que los contiene en $\mathcal{S}^3$ se encuentra en S^3, y como S^3 es isomorfo a S'^3, existe una única línea en $\mathcal{S}'^3$ que contiene a p_i y p_j,

si al menos uno de los puntos p_i y p_j no pertenece a S^3 en $\mathcal{S}^3$, entonces, por ser S^3 subsistema, no existe ninguna línea en S^3 que los contenga por lo tanto, no existe ninguna línea en S'^3 que los contenga, entonces, la única línea que los posee se encuentra en las líneas de $\mathcal{S}'^3$ excepto las que están en S^3. Por lo tanto, existe una única línea en $\mathcal{S}'^3$ a la que le pertenecen p_i y p_j.

□

Teorema 5.2.3 *$\mathcal{S}'^3$ no es isomorfo a $\mathcal{S}^3$.*

Demostración. Sea $C_3(\mathcal{S}'^3)$ el código generado por una matriz de incidencia de $\mathcal{S}'^3$. Una de las líneas que obtuvimos al hacer el cambio es $\{p_2, p_4, p_7\}$. Y como;

$p_4 + p_9 + p_{26} = (1,1,0,0,...,0) + (0,0,1,0,...,0) + (2,2,2,0,...,0) = \bar{0}$,
$p_1 + p_{15} + p_{23} = (1,0,0,0,...,0) + (0,2,1,0,...,0) + (2,1,2,0,...,0) = \bar{0}$,
$p_7 + p_{15} + p_{26} = (1,2,0,0,...,0) + (0,2,1,0,...,0) + (2,2,2,0,...,0) = \bar{0}$ y
$p_7 + p_9 + p_{23} = (1,2,0,0,...,0) + (0,0,1,0,...,0) + (2,1,2,0,...,0) = \bar{0}$,

tenemos que las líneas, $\{p_4, p_9, p_{26}\}, \{p_1, p_{15}, p_{23}\}, \{p_7, p_{15}, p_{26}\}$ y $\{p_7, p_9, p_{23}\}$ de $\mathcal{S}^3$, no pertenecen a S^3, por lo tanto, pertenecen a $\mathcal{S}'^3$ y entonces, cualquier combinación lineal los vectores de incidencia correspodientes a estas líneas pertenece a $C_3(\mathcal{S}'^3)$, en particular la que se muestra en el siguiente arreglo;

	p_0	p_1	p_2	p_3	p_4	p_5	p_6	p_7	p_8	p_9	p_{10}	p_{11}	p_{12}	p_{13}	p_{14}	p_{15}	p_{16}	p_{17}	p_{18}	p_{19}	p_{20}	p_{21}	p_{22}	p_{23}	p_{24}	p_{25}	p_{26}	$\cdots$	p_{3^n-1}
3^0	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	$\cdots$	2
3^1	0	0	0	1	1	1	2	2	2	0	0	0	1	1	1	2	2	2	0	0	0	1	1	1	2	2	2	$\cdots$	2
3^2	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	$\cdots$	2
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\cdots$	$\vdots$
$3^n - 1$	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	$\cdots$	2
$2\chi(\{\vec{4},\vec{9},\vec{26}\})$	0	0	0	0	**2**	0	0	0	0	**2**	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	**2**	$\cdots$	0
$+2\chi(\{\vec{1},\vec{15},\vec{23}\})$	0	**2**	0	0	0	0	0	0	0	0	0	0	0	0	0	**2**	0	0	0	0	0	0	0	**2**	0	0	0	$\cdots$	0
$+\chi(\{\vec{7},\vec{15},\vec{26}\})$	0	0	0	0	0	0	0	**1**	0	0	0	0	0	0	0	**1**	0	0	0	0	0	0	0	0	0	0	**1**	$\cdots$	0
$+\chi(\{\vec{7},\vec{9},\vec{23}\})$	0	0	0	0	0	0	0	**1**	0	**1**	0	0	0	0	0	0	0	0	0	0	0	0	0	**1**	0	0	0	$\cdots$	0
$+\chi(\{\vec{2},\vec{4},\vec{7}\})$	0	0	**1**	0	**1**	0	0	**1**	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	$\cdots$	0
$=$	0	**2**	**1**	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	$\cdots$	0

Por lo que $C_3(\mathcal{S}'^3)$ tiene una palabra de peso 2, entonces $d(C_3(\mathcal{S}'^3)) \leq 2$, luego, $d(C_3(\mathcal{S}'^3)) \neq 3 = d(C_3(\mathcal{S}^3))$ por el Teorema 3.1.1 los códigos $C_3(\mathcal{S}'^3)$ y $C_3(\mathcal{S}^3)$ no son equivalentes, entonces por el Teorema 3.2.1 los Sistemas Triples de Steiner $\mathcal{S}^3$ y $\mathcal{S}'^3$ no son isomorfos.

□

Conclusiones

Como se podrá advertir, el método que utilizamos no sólo nos sirve para encontrar un par de Sistemas Triples de Steiner con $2^{n+1}-1$ y 3^n puntos; ya que, en cada caso, el cambio que hicimos lo podemos hacer en subsistemas más grandes, es decir, generados por más de dos líneas, más aún, podemos realizar más de un cambio en el mismo subsistema o en subsistemas diferentes e igualmente podría suceder que obtuvieramos más sistemas no isomorfos. Entonces una pregunta interesante es; ¿cuantos Sistemas Triples de Steiner no isomorfos podemos construir a partir de los sistemas clásicos con este método?. De igual manera; el argumento que utilizamos para saber si los sistemas que obtuvimos eran no isomorfos a los clásicos, fue a por medio de la no equivalencia de sus códigos asociados, pero se ha visto que pueden existir sistemas que no son isomorfos pero sus códigos asociados si resultan ser equivalentes, entonces; ¿cuantos códigos no equivalentes podemos obtener de los $STS(2^{n+1}-1)$ y de los $STS(3^n)$?. Ya se demostró que los $STS(2^{n+1}-1)$ con el mismo 2-rango deben tener códigos equivalentes; ¿será cierto que los $STS(3^n-1)$ con el mismo 3-rango tienen códigos equivalentes?. Bueno, pues todas estas cuestiones son parte de mí proyecto de maestría y doctorado.

Bibliografía

[1] Friedberg, Stephen H., Insel, Arnold J. and Spence Lawrence E. *Linear Algebra*. Prentice Hall, Fourth edition, 2003.

[2] T. Berth, D. Jungnickel, H Lenz. *Desings Theory*. Cambridge University Press, V. I and II, 1999.

[3] Marshall Hall, JR. *Combinatorial Theory*. Emory University, Second edition 1983.

[4] Van Lint, J.H. and Wilson, R.M. *A course in combinatorics*. Cambridge University Press, Second edition, 2001.

[5] Hartshorne, R. *Foundations of Proyective Geometry*. Lecture Notes, Harvard University, 1967.

[6] Bierbrauer, J. *Introduction to Coding Theory*. Chapman and Hall/CRC, 2004.

[7] Van Lint, J.H. *Introduction to Coding Theory*. GTM, Springer, 1998.

[8] Doyen, J., Hubaut, X., and Vandensavel, M. *Rank of incidence matrices of Steiner Triple Sistems*. Math. Z.163, 251-259, 1978.