UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

PROGRAMA DE MAESTRÍA Y DOCTORADO EN CIENCIAS MATEMÁTICAS Y DE LA ESPECIALIZACIÓN EN ESTADÍSTICA APLICADA

TESIS

"Una parametrización de diseños simétricos con un grupo de automorfismos transitivo en banderas y primitivo en puntos con acción producto."

Que para obtener el título de

"Maestro en ciencias"

Presenta:

Lic. José Emanuel Rodríguez Fitta

Asesora:

Dra. Eugenia O'Reilly Regueiro

Mayo 2017

Índice

CAPÍTULO 1

Introducción

Quince alumnas salen formadas de tres en tres durante siete días seguidos, se requiere formarlas cada día de manera que al terminar la semana no haya habido dos de ellas que hayan caminado en la misma fila más de una vez. Este es el famoso problema de las colegialas de Thomas Kirkman propuesto en 1850 en "The lady's and gentleman's diary" y cuya solución consiste en acomodar 15 alumnas en ternas de manera que cada par de alumnas estén en exactamente una terna. La solución es lo que hoy en día conocemos como un diseño de bloques incompleto balanceado o BIBD por sus siglas en inglés, de hecho la solución es un ejemplo de lo que hoy se le llama sistema triple de Steiner o STS por sus siglas en inglés. Los STS son un tipo de diseños de bloques que fueron nombrados así en honor al matemático Jakob Steiner, pues él propone en 1853 justamente el problema de arreglar n elementos en ternas de tal forma que cada par de elementos aparecen en exactamente una terna.

Este tipo de estructuras (BIBD) encuentran varias aplicaciones dentro de la estadística, por ejemplo Frank Yates en 1939 discute su importancia en diseños estadísticos de experimentos para variedades en el contexto de experimentos biológicos y de agricultura. Mientras que Raj Chandra Bose, igualmente en 1939, discute acerca de su construcción y algunas de sus propiedades, es decir, los BIBD ya no solo surgen como auxiliares en la resolución de problemas

como el de las colegialas, sino que empiezan a ser estudiados de manera más formal.

De hecho Ronald Fisher, estadístico y biólogo, también los utiliza al hacer diseños experimentales y estudiar la diferencia entre diversas variedades de plantas, cada una de ellas bajo un número de diferentes condiciones de cultivo a lo que él nombró bloques. De esto surgió la desigualdad de Fisher la cual es fundamental dentro del estudio de los diseños de bloques. Dicha desigualdad nos dice que el número de bloques es mayor o igual que el número de variedades, es decir, traducido al lenguaje de teoría de diseños, el número de bloques es mayor o igual que el número de puntos del diseño.
También es Fisher quien da la siguiente propiedad, el número de variedades que hay en cada bloque es menor que el número de variedades, de aquí el hecho de que los bloques son incompletos.

En la primera parte de este trabajo nos concentramos en dar algunas características importantes de los diseños, en particular nos concentramos en los llamados diseños simétricos, que ocurren justamente cuando el número de bloques coincide con el número de puntos del diseño, estas características son utilizadas en los resultados obtenidos en este trabajo y en general son resultados de suma importancia dentro de la teoría de diseños.

Dada la estructura de los diseños simétricos uno puede definir para ellos lo que en álgebra se conoce como automorfismos, de hecho, dada la naturaleza finita de los también conocidos como SBIBD, por sus siglas en inglés, los automorfismos forman un grupo igualmente finito. Este actúa de manera natural sobre el conjunto de parejas punto-bloque con el punto dentro del bloque, a esta pareja se le conoce como bandera.

Los grupos transitivos finitos, se clasifican en primitivos e imprimitivos de acuerdo a como sea la acción del grupo, de hecho Leonard Scott y Michael O'Nan en un artículo escrito para la conferencia de Santa Cruz en grupos finitos en 1979 dan una clasificación de los grupos primitivos en cinco tipos, grupos afines, grupos casi simples, acción diagonal simple, acción producto y acción de corona torcida.

En la segunda parte de este trabajo damos la definición de automorfismos de diseños y algunas nociones básicas sobre acciones de grupo, en particular damos la definición de lo que es una acción transitiva en banderas, que es un concepto básico que utilizamos dentro de este trabajo. Así mismo introducimos las ideas de los grupos imprimitivos y primitivos y hablamos acerca de la clasificación hecha por O'Nan-Scott antes mencionada. Liebeck, Praeger y Saxl en [3] dan una demostración de tan importante teorema de clasificación.

Antes de estudiar diseños simétricos cuyo grupo de automorfismos es transitivo en banderas y primitivo, damos un resultado que nos dice cuáles son las posibles ternas de los diseños simétricos que admiten un grupo de automorfismos transitivo en banderas e imprimitivo y cuyo parámetro λ es menor o igual que 20.

Más adelante, y utilizando la clasificación de O'Nan-Scott aplicada a los grupos de automorfismos de diseños, Eugenia O'Reilly Regueiro estudia en particular aquellos diseños simétricos cuyos grupos de automorfismos son primitivos y transitivos en banderas y encuentra en [2] que para $\lambda \leq 4$, dichos grupos solo pueden ser afines o casi simples.
En un intento por generalizar dicho resultado Tian y Zhou en [4] trabajan sobre el mismo problema pero para $\lambda \leq 100$. Dentro de su artículo, encuentran que en el caso de la acción producto, se obtienen algunas posibles ternas (v, k, λ) que cumplen todas las condiciones aritméticas que surgen al hacer la suposición de que dichos diseños con este tipo de grupo de automorfismos existen. En el caso particular en que v es el cuadrado de un número par, las ternas resultantes son lo que se llaman diseños de Menon [5], gran parte de este trabajo se centra en generalizar este resultado.

Así, en la última parte de esta tesis nos concentramos en la acción producto, es decir, suponemos que existe un diseño simétrico con grupo de automorfismo primitivo y transitivo en banderas y cuya acción es la acción producto, con base en condiciones aritméticas que surgen y con un método distinto al usado en [4] obtenemos para $\lambda \leq 20$ las mismas posibles ternas (v, k, λ) que obtienen Tian y Zhou. Después, al darnos cuenta que la mayor cantidad de posibles ternas surgen cuando $v = m^2$ nos concentramos en este caso e intentamos generalizar lo que Tian y Zhou hicieron en su artículo, es decir, que para cualquier λ siempre que m es

par las posibles ternas que se surgen son las de Menon. En este intento nos concentramos en el parámetro m y obtenemos una condición suficiente y necesaria para que el diseño resulte ser de Menon. Esta condición da como consecuencia que cuando $m-1$ es una potencia de primo mayor o igual que tres, los parámetros del diseño resultan ser los de un diseño de Menon. Todo lo anterior surge de la idea de concentrarnos en $m-1$ en lugar de λ y gracias a este cambio se obtiene que para $m \leq 210$ además de los diseños de Manon correspondientes surgen tres ternas que no son de Menon pero cumplen todas las condiciones aritméticas.

Posteriormente obtenemos dos posibles casos, que surgen de las hipótesis sobre el diseño y su grupo de automorfismos, en ambos casos es posible descartar dos de las tres ternas. La terna restante sirve como posible contraejemplo de la generalización del resultado de Tian y Zhou, en el sentido de querer obtener diseños de Menon para un λ arbitrario ($v = m^2$, m par), pues cumple todas las condiciones aritméticas y además cumple con la consecuencia de uno de estos dos casos y no es una terna de Menon, más aún el caso en el que entra esta terna, arroja una parametrización sobre v, k, λ que es generalización de los diseños de Menon. Al trabajar con el otro caso obtenemos como consecuencia solo los diseños de Menon.

Como resultado central de esta tesis obtenemos un teorema que generaliza lo hecho por Tian y Zhou pero en el sentido de que obtenemos una parametrización para los posibles diseños simétricos que admiten un grupo de automorfismos primitivo, transitivo en banderas con la acción producto, que depende ahora de dos parámetros s y t. Además concluimos que dicha parametrización sólo puede ser posible cuando $s \geq 1$ es impar, si $s = 1$ se reduce a la parametrización de los diseños de Menon y si $s > 1$ entonces t sólo puede ser par.

Por último en la parte final del trabajo se da un resultado sobre el complemento de un diseño simétrico con la acción producto, cuando $v = m^l$ se obtiene que dicho complemento no puede ser transitivo en banderas.

CAPÍTULO 2

Diseños

En la introducción hicimos mención acerca de que los diseños son estructuras de incidencia que constan de puntos y bloques, además de eso debemos introducir una propiedad de balance. De hecho la definición formal de un diseño es la siguiente:

Definición 1. Sean v, k y λ enteros positivos tales que $v > k \geq 2$. Sea X un conjunto finito de elementos o puntos y A una familia de subconjuntos de X, llamados bloques. Un $(v, k, \lambda)-$diseño de bloques inclompletos balanceados (BIBD por sus siglas en inglés) es un par (X, A) tal que se cumplen las siguientes propiedades

1. $|X| = v$,

2. cada bloque contiene k puntos y

3. cada par de puntos distintos está contenido en exactamente λ bloques

La propiedad 3 en la definición es la propiedad de balanceo. Un BIBD es llamado un diseño de bloques incompleto porque $k < v$ así que todos los bloques son bloques incompletos, pues ningún bloque contiene a todos los puntos.

Dada la definición anterior podemos calcular cuantos puntos hay en cada bloque, lo que queda expresado en el siguiente:

Teorema 1. *En un $(v, k, \lambda)-$ BIBD, cada punto se encuentra en exactamente*

$$r = \frac{\lambda(v-1)}{k-1}$$

bloques.

Demostración. Sea (X, A) un $(v, k, \lambda)-$ BIBD, supongamos $x \in X$ y sea r_x el número de bloques que contienen a x. Así mismo definamos el conjunto

$$I = \{(y, C) : y \in X, y \neq x, C \in A, \{x, y\} \subseteq C\},$$

obtengamos el número de elementos de I.
Primero, sabemos que hay $v-1$ maneras de elegir $y \in X$ tal que $y \neq x$ y para cada una de estas y hay λ bloques C tales que $\{x, y\} \subseteq C$, por lo que $|I| = \lambda(v-1)$.
Por otro lado, hay r_x maneras de elegir un bloque C tal que $x \in C$, para cada uno de estos bloques C, hay $k-1$ maneras de elegir $y \in C$ tal que $y \neq x$, con lo que $|I| = r_x(k-1)$.
Por lo tanto

$$\lambda(v-1) = r_x(k-1).$$

Dado que $r_x = \frac{\lambda(v-1)}{k-1}$ es independiente de x, se obtiene el resultado deseado. □

Además también podemos hacer el cálculo de cuántos bloques exactamente tiene nuestro diseño.

Teorema 2. *Un $(v, k, \lambda)-$ BIBD tiene*

$$b = \frac{vr}{k} = \frac{\lambda(v^2 - v)}{k^2 - k}$$

bloques.

Demostración. Sea (X, A) un $(v, k, \lambda)-$ BIBD y sea $b = |A|$, definamos el conjunto

$$I = \{(x, C) : x \in X, C \in A, x \in C\},$$

obtengamos el número de elementos de I.
Primero, hay v maneras de elegir $x \in X$, para cada uno de ellos hay r bloques C que los

contienen, así que $|I| = vr$.
Por otro lado, hay b maneras de elegir un bloque $C \in A$, para cada uno de esos bloques hay k maneras de elegir $x \in C$, así que $|I| = bk$.
Por lo tanto

$$bk = vr,$$

que es lo que se buscaba probar. □

Algo que es muy importante dentro de la teoría de diseños es el hecho de que a cada diseño podemos asignarle una matriz llamada matriz de incidencia, la cual tiene dentro de sí toda la información acerca de cómo los puntos inciden dentro de los bloques.

Definición 2. Sea (X, A) un diseño donde $X = \{x_1, ..., x_v\}$ y $A = \{A_1, ..., A_b\}$. La matriz de incidencia de (X, A) es la matriz $M = (m_{i,j})$ de tamaño $v \times b$ definida por:

$$m_{i,j} = \begin{cases} 1 & \text{si } x_i \in A_j, \\ 0 & \text{si } x_i \notin A_j. \end{cases}$$

Los renglones corresponden a los puntos y las columnas a los bloques.
Esta satisface las siguientes propiedades

1. cada columna de M tiene k "1"s,
2. cada renglón de M tiene r "1"s,
3. dos renglones distintos de M contienen "1"s en λ columnas.

Más aún una pregunta que surge en es Â¿Cuándo una matriz es la matriz de incidencia de un diseño? Las condiciones suficientes y necesarias para que esto suceda son las siguientes:

Teorema 3. *Sea M una matriz $v \times b$ con entradas 0 y 1 y sea $2 \leq k < v$. Entonces M es la matriz de incidencia de un (v, b, r, k, λ)-BIBD si y sólo si $MM^T = \lambda J_v + (r - \lambda)I_v$ y $u_v M = k u_b$. Donde I_v es la matriz identidad y J_v es la matriz $v \times v$ cuyas entradas son sólo 1, y u_v denota al vector de longitud v en el que cada coordenada es 1.*

Demostración. Supongamos (X, A) es un (v, k, λ)-BIBD, donde $X = \{x_1, ..., x_v\}$ y $A = \{A_1, ..., A_b\}$. Sea M su matriz de incidencia. La entrada (i, j) de MM^T es

$$\sum_{h=1}^{b} m_{i,h} m_{j,h} = \begin{cases} r & \text{si } i = j, \\ \lambda & \text{en otro caso .} \end{cases}$$

Lo an, de las propiedades 2 y 3 mencionadas antes, cada entrada en la diagonal de MM^T es igual a r, y cada entrada fuera de la diagonal es igual a λ, entonces $MM^T = \lambda J_v + (r-\lambda)I_v$. Más aún, la i-ésima entrada de $u_v M$ es igual al número de 1's en la columna i de M. Por la propiedad 1, esto es igual a k, entonces $u_v M = ku_b$.
Supongamos ahora que M es una matriz $v \times b$ con entradas 0 y 1 tal que $MM^T = \lambda J_v + (r-\lambda)I_v$ y $u_v M = ku_b$. Sea (X, A) el diseño cuya matriz de incidencia es M. Claramente $|X| = v$ y $|A| = b$. Luego, de $u_v M = ku_b$ se sigue que cada bloque de A contiene k puntos. De $MM^T = \lambda J_v + (r-\lambda)I_v$ se sigue que cada par de puntos están en λ bloques, y cada punto está en r bloques, por lo tanto podemos concluir con lo visto con anterioridad que (X, A) es un BIBD. Con lo que se prueba lo que se quería. □

En esta tesis trabajaremos específicamente con los denominados diseños simétricos, es decir, aquellos en los que el número de puntos coincide con el número de bloques. La definición formal es como sigue:

Definición 3. Un (v, k, λ)-BIBD en el cual $b = v$ es llamado un BIBD simétrico. En este caso decimos que el diseño es un (v, k, λ)-SBIBD.

Notemos que la condición $b = v$ en la definición anterior es equivalente a que $r = k$. Luego notamos del Teorema 1 que para un diseño simétrico se cumple:

$$\lambda(v-1) = k(k-1). \tag{2.1}$$

La ecuación anterior es de suma importancia para el trabajo realizado en la presente tesis pues nos da interesantes condiciones aritméticas con las cuáles obtenemos resultados importantes.

Más aun, este resultado nos arroja otra interesante condición sobre los parámetros de un diseño simétrico, y esta condición a su vez nos ayudará a descartar posibles ternas que surgen en el desarrollo del trabajo, y por lo tanto nos ayuda a acercarnos más al resultado que deseamos probar.

Lema 1. *Si D es un $(v, k, \lambda)-$ diseño simétrico, entonces*

$$4\lambda(v-1) + 1 \tag{2.2}$$

es un cuadrado.

Demostración.

$$k = \frac{1 + \sqrt{1 + 4\lambda(v-1)}}{2} \in \mathbb{Z}. \tag{2.3}$$

Se obtiene al resolver la ecuación

$$k(k-1) = \lambda(v-1) \tag{2.4}$$

para k. □

Definición 4. El complemento D' de un (v, k, λ) diseño simétrico $D = (X, A)$ es un $(v, v - k, v - 2k + \lambda)$ diseño simétrico cuyo conjunto de puntos es el mismo que para D y cuyos bloques son los complementos de los bloques de D con respecto a X.

Nótese que al ser D' un diseño simétrico se cumple una relación análoga a (2.1), en particular como D' es un $(v, v - k, v - 2k + \lambda)$ diseño simétrico se debe cumplir:

$$(v-k)(v-k-1) = (v-2k+\lambda)(v-1). \tag{2.5}$$

Definición 5. Si D es un (v, k, λ) diseño simétrico llamamos $n = k - \lambda$ al orden de D.

Nótese que el orden del complemento del diseño D de la definición anterior es $n' = v - k - (v - 2k + \lambda) = k - \lambda$, es decir, el orden es el mismo para el diseño que para su complemento.
Algunos tipos de diseños que son de suma importancia dentro de la teoría son los siguientes:

Definición 6. Sea D un (v, k, λ) diseño simétrico, entonces

1. si $v = 4n - 1$, $k = 2n - 1$ y $\lambda = n - 1$ diremos que D es un diseño de Hadamard.
2. si $\lambda = 2$ diremos que el diseño es un biplano.
3. si $v = 4t^2$, $k = (2t-1)t$ y $\lambda = (t-1)t$ para algún natural t diremos que D es un diseño de Menon.

En este trabajo nos interesamos sobre todo en estos últimos, pues estudiamos el caso en que el diseño es simétrico con grupo de automorfismos primitivo y transitivo en banderas con la acción producto (más adelante veremos a detalle el significado de estos conceptos). Al

imponer estas condiciones sobre el grupo de automorfismos del diseño y ciertas condiciones aritméticas sobre v, entonces el diseño que obtenemos resulta ser de Menon, lo cual podría facilitar más adelante un teorema de clasificación generalizado análogo al dado por Eugenia O'Reilly en [2].

Otra importante definición con la cual trabajeremos en los resultados centrales de esta tesis es la siguiente:

Definición 7. Sea D un (v, k, λ)-SBIBD, una bandera de D es un par ordenado (p, B) donde p es un punto de D, B es un bloque de D y ellos son incidentes, es decir, $p \in B$.

Cuando desarrollamos este trabajo, encontramos muchas posibles ternas que cumplían con las condiciones aritméticas que surgían de las hipótesis hechas sobre el diseño y su grupo de automorfismos. Sin embargo al estar concentrados específicamente en que el parámetro v fuese par, muchas de estas ternas se descartaron mediante los siguientes importantes resultados de la teoría de diseños simétricos.

Teorema de Bruck-Ryser-Chowla para v par 1. *Supongamos que existe un* (v, k, λ)*-SBIBD con* v *par, entonces* $n = k - \lambda$ *es un cuadrado.*

Demostración. Sea M la matriz de incidencia de un (v, k, λ)-SBIBD con v par. Del teorema 3 y usando el hecho de que $r = k$ tenemos que $MM^T = \lambda J_v + (k - \lambda)I_v$. Ya que $b = v$, las matrices M y M^T son matrices $v \times v$. Luego, como $det(MM^T) = (detM)(detM^T) = (detM)^2$ para cualquier matriz M, en particular, en nuestro caso, esto implica que $(detM)^2 = det(\lambda J_v + (k - \lambda)I_v)$.
Notemos que la matriz $\lambda J_v + (k - \lambda)I_v$ es

$$\begin{pmatrix} k & \lambda & \lambda & \dots & \lambda \\ \lambda & k & \lambda & \dots & \lambda \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ \lambda & \lambda & \lambda & ,..., & k \end{pmatrix}$$

Restemos la primera fila a las demás entonces tenemos

$$\begin{pmatrix} k & \lambda & \lambda & \dots & \lambda \\ \lambda-k & k-\lambda & 0 & \dots & 0 \\ \lambda-k & 0 & k-\lambda & \dots & 0 \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ \lambda-k & 0 & 0 & ,..., & k-\lambda \end{pmatrix}$$

Sumando todas las columnas a la primera tenemos

$$\begin{pmatrix} k+(v-1)\lambda & \lambda & \lambda & \dots & \lambda \\ 0 & k-\lambda & 0 & \dots & 0 \\ 0 & 0 & k-\lambda & \dots & 0 \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ 0 & 0 & 0 & ,..., & k-\lambda \end{pmatrix} \tag{2.6}$$

como lo que hicimos fueron operaciones elementales sobre las filas y columnas de $\lambda J_v+(k-\lambda)I_v$ entonces $det(\lambda J_v + (k-\lambda)I_v)$ será el determinante de (2.6) que al ser una matriz triangular, este se obtiene multiplicando los elementos de la diagonal, por lo que tendremos

$$(detM)^2 = det(\lambda J_v + (k-\lambda)I_v) = (k+(v-1)\lambda)(k-1)^{v-1} = k^2(k-\lambda)^{v-1},$$

es decir, $detM = k\sqrt{(k-\lambda)^{v-1}}$ y como la matriz M tiene entradas enteras, entonces $detM$ debe ser entero y por lo tanto si v es par se debe tener $k-\lambda$ es un cuadrado para que la raÃz sea entera. □

Para complementar el teorema anterior con su contraparte impar necesitaremos los siguientes dos lemas.

Lema 2. *Para cualquier entero $n \geq 0$ existen enteros $a_0, a_1, a_2, a_3 \geq 0$ tales que $n = a_0^2 + a_1^2 + a_2^2 + a_3^2$*

Demostración. Ver[1] □

Lema 3. *Sea C la matriz 4×4*

$$\begin{pmatrix} a_0 & a_1 & a_2 & a_3 \\ -a_1 & a_0 & a_3 & a_2 \\ -a_2 & a_3 & a_0 & -a_1 \\ -a_3 & -a_2 & a_1 & a_0 \end{pmatrix} \tag{2.7}$$

y sea $n = a_0^2 + a_1^2 + a_2^2 + a_3^2$ entonces $C^{-1} = \frac{1}{n}C^T$.

Demostración. Ver[1] □

Ahora presentamos el complemento del Teorema de Bruck- Ryser- Chowla, antes mencionado, es decir, cuando v es impar, que aunque en este trabajo no nos centramos en diseños con esa condición, es importante mencionar este resultado.

Teorema de Bruck-Ryser-Chowla para v impar 1. *Supongamos que existe un (v, k, λ)-SBIBD con v impar. Entonces existen enteros x, y, z, no todos cero tales que*

$$x^2 = (k - \lambda)y^2 + (-1)^{(v-1)/2}\lambda z^2. \tag{2.8}$$

Demostración. Supongamos que existe un (v, k, λ)- SBIBD y sea $v \equiv 1 \pmod 4$, denotemos $v = 4w + 1$. Sea M su matriz de incidencia. Sean $x_1, ..., x_v$ indeterminadas. Para $1 \leq i \leq v$ definimos

$$L_i = \sum_{j=1}^{v} m_{j,i}x_j,$$

cada L_i es una función lineal de las x_i y con coeficientes enteros. Tenemos que

$$L_i^2 = \sum_{j=1}^{v}\sum_{h=1}^{v} m_{j,i}m_{h,i}x_jx_h.$$

Sumando sobre i obtenemos

$$\sum_{i=1}^{v} L_i^2 = \sum_{i=1}^{v}\sum_{j=1}^{v}\sum_{h=1}^{v} m_{j,i}m_{h,i}x_jx_h = \sum_{j=1}^{v}\sum_{h=1}^{v}\sum_{i=1}^{v} m_{j,i}m_{h,i}x_jx_h. \tag{2.9}$$

De la definición de diseño simétrico y de matriz de incidencia observamos que:

$$\sum_{i=1}^{v} m_{j,i}m_{h,i} = \begin{cases} \lambda & \text{si } j \neq h, \\ k & \text{si } j = h. \end{cases}$$

Sustituyendo en (2.9) obtenemos:

$$\begin{aligned}\sum_{i=1}^{v} L_i^2 &= \sum_{j,h:j\neq h} \lambda x_j x_h + \sum_{j=1}^{v} k x_j^2 \\ &= \sum_{j=1}^{v}\sum_{h=1}^{v} \lambda x_j x_h + \sum_{j=1}^{v} (k-\lambda) x_j^2 \\ &= \lambda \left(\sum_{j=1}^{v} x_j \right)^2 + (k-\lambda) \sum_{j=1}^{v} x_j^2.\end{aligned}$$

Con lo que concluimos que:

$$\sum_{i=1}^{v} L_i^2 = \lambda \left(\sum_{j=1}^{v} x_j \right)^2 + (k-\lambda) \sum_{j=1}^{v} x_j^2. \tag{2.10}$$

Transformando las variables $x_1, ..., x_v$ en nuevas variables $y_1, ..., y_v$, donde cada y_i es alguna combinación lineal entera de las x_i. Por el Lema 2 existen a_0, a_1, a_2, a_3 enteros tales que $a_0^2 + a_1^2 + a_2^2 + a_3^2 = k - \lambda$ y sea la matriz C como en (2.7).

Para $1 \leq h \leq w$, sean $(y_{4h-3}, y_{4h-2}, y_{4h-1}, y_{4h}) = (x_{4h-3}, x_{4h-2}, x_{4h-1}, x_{4h})C$, $y_v = x_v$, y $y_0 = \sum_{i=1}^{v} x_i$. Debido al Lema 3 tenemos

$$\sum_{j=1}^{v-1} y_j^2 = (k-\lambda) \sum_{j=1}^{v-1} x_j^2.$$

De aquí tenemos que

$$\sum_{i=1}^{v} L_i^2 = \lambda y_0^2 + \sum_{j=1}^{v-1} y_j^2 + (k-\lambda) y_v^2. \tag{2.11}$$

Por el Lema 3, podemos expresar x_j y y_0 como combinación lineal racional de $y_1, ..., y_v$, pero además L_i fue definida como combinación lineal entera de las x_i. Por lo que la anterior ecuación puede ser vista como una identidad en las indeterminadas $y_1, ..., y_v$ en la cual todos los coeficientes son racionales.

Ahora, supongamos que $L_1 = \sum_{i=1}^{v} e_i y_i$, si e_1 no es 1, entonces $y_1 = L_1$, y si $e_1 = 1$, entonces $y_1 = -L_1$, hemos expresado y_1 como combinación lineal racional de $y_2, ..., y_v$ de tal forma que $L_1^2 = y_1^2$. Entonces la ecuación (2.11) se transforma en

$$\sum_{i=2}^{v} L_i^2 = \lambda y_0^2 + \sum_{j=2}^{v-1} y_j^2 + (k-\lambda) y_v^2.$$

Continuando de esta forma, escribimos y_j como combinación lineal racional de $y_{j+1}, ..., y_v$ tal que $y_j^2 = L_j^2$, con lo que eliminamos las variables $y_2, ..., y_{v-1}$ y al final se obtiene

$$L_v^2 = \lambda y_0^2 + (k - \lambda) y_v^2,$$

donde L_v y y_0 son múltiplos racionales de y_v. Supongamos que $L_v = s y_v$ y $y_0 = t y_v$ con s, t racionales. Sea $y_v = 1$, entonces $s^2 = \lambda t^2 + k - \lambda$, luego podemos escribir $s = s_1/s_2$ y $t = t_1/t_2$ con s_1, s_2, t_1, t_2 enteros y s_2, t_2 distintos de cero. Con lo anterior tendremos $(s_1 t_2)^2 = \lambda(s_2 t_1)^2 + (k - \lambda)(s_2 t_2)^2$. Si $x = s_1 t_2, y = s_2 t_2$ y $z = s_2 t_1$, tendremos una solución entera a la ecuación $x^2 = (k - \lambda) y^2 + (-1)^{(v-1)/2} \lambda z^2$ en la que x, y, z no todos cero y $(-1)^{(v-1)/2} = 1$ pues $v \equiv 1 \pmod 4$.

Consideremos el caso en que $v \equiv 3 \pmod 4$, denotamos $v = 4w - 1$, introducimos la indeterminada x_{v+1} y agregamos el término $(k - \lambda) x_{v+1}^2$ a la ecuación (2.10) para obtener

$$\sum_{i=1}^{v} L_i^2 + (k - \lambda) x_{v+1}^2 = \lambda \left(\sum_{j=1}^{v} x_j \right)^2 + (k - \lambda) \sum_{j=1}^{v+1} x_j^2. \tag{2.12}$$

Para $1 \leq h \leq w$, sean $(y_{4h-3}, y_{4h-2}, y_{4h-1}, y_{4h}) = (x_{4h-3}, x_{4h-2}, x_{4h-1}, x_{4h}) C$, $y_v = x_v$, y $y_0 = \sum_{i=1}^{v} x_i$ y sea $y_0 = \sum_{i=1}^{v} x_i$, entonces tenemos

$$\sum_{i=1}^{v} L_i^2 + (k - \lambda) x_{v+1}^2 = \lambda y_0^2 + \sum_{j=1}^{v+1} y_j^2.$$

Procediendo como en el caso en que $v \equiv 1 \pmod 4$, eliminando las L_i tenemos la siguiente ecuación

$$(k - \lambda) x_{v+1}^2 = \lambda y_0^2 + y_{v+1}^2,$$

y tendremos una solución a la ecuación $x^2 = (k - \lambda) y^2 + (-1)^{(v-1)/2} \lambda z^2$ con x, y y z no todos cero, y $(-1)^{(v-1)/2} = -1$ pues $v \equiv 3 \pmod 4$. □

Lema 4. *Sea D un (v, k, λ)-diseño simétrico con $n = k - \lambda$, entonces*

$$4n - 1 \leq v \leq n^2 + n + 1.$$

Demostración. Sabemos que $\lambda(v - 1) = k(k - 1)$ podemos reescribirla en función de n

$$v - 1 = \frac{k(k-1)}{\lambda} = \lambda + 2n + \frac{n(n-1)}{\lambda} - 1.$$

Resolviendo la anterior ecuación para λ tenemos que

$$\lambda = \frac{1}{2}\left(v - 2n \pm \sqrt{(v-2n)^2 - 4n(n-1)}\right).$$

Ya que como vimos el orden es el mismo para D que para D' entonces estas dos ecuaciones valen para ambos diseños. Como $\lambda \geq 1$ entonces se debe cumplir $v - 2n - 2 \geq \sqrt{(v-2n)^2 - 4n(n-1)}$ de donde obtenemos

$$\begin{aligned} v^2 - 4(n+1)v + 4(n+1)^2 &\geq v^2 - 4nv + 4n^2 - 4n(n-1) \\ -4v + 4(n+1)^2 &\geq 4n^2 - 4n(n-1) \\ n^2 + n + 1 &\geq v. \end{aligned}$$

Probemos ahora la otra desigualdad, notemos primero que se debe cumplir $\sqrt{(v-2n)^2 - 4n(n-1)} \neq 0$ pues si $\sqrt{(v-2n)^2 - 4n(n-1)} = 0$ entonces $\lambda = \frac{v}{2} - n = \frac{v}{2} + \lambda - k$ lo que implicaría que $v = 2k$. Además tendríamos que $(v-2n)^2 = 4n(n-1)$ y como $v = 2k$ entonces $(2k-2n)^2 = 4n(n-1)$ y con ello $\lambda^2 = n(n-1)$ lo que no puede ser pues λ es entero y $n(n-1)$ no es un cuadrado. Por lo tanto $\sqrt{(v-2n)^2 - 4n(n-1)} \geq 1$.
Ahora, dado que $(v-2n)^2 - 4n(n-1) \geq 1$ entonces $(v-2n)^2 \geq 4n(n-1)+1$, afirmamos que $4n(n-1)+1 \geq (2n-1)^2$. En efecto, procedemos a hacer la demostración por inducción. Para $n = 1$ tenemos que $4n(n-1)+1 = 1$ y $(2n-1)^2 = 1$ por lo que se cumple el resultado para $n = 1$. Ahora supongamos la desigualdad cierta para cualquier natural $n \geq 1$ y probémosla para $n+1$.

$$4(n+1)n + 1 = 4(n-1)n + 8n + 1$$

Y por la hipótesis inductiva tendremos

$$\begin{aligned} 4(n+1)n + 1 = 4(n-1)n + 8n + 1 &\geq (2n-1)^2 + 8n = \\ &= 4n^2 + 4n + 1 = (2n+1)^2 = (2(n+1)-1)^2. \end{aligned}$$

Es decir, $4(n+1)n + 1 \geq (2(n+1)-1)^2$, con lo que se demuestra la desigualdad para $n+1$ y entonces hemos probado que $4n(n-1)+1 \geq (2n-1)^2$ es válida para todo número natural n. Luego, $(v-2n)^2 \geq 4n(n-1)+1 \geq (2n-1)^2$ y por lo tanto $v - 2n \geq 2n - 1$ de donde tenemos $v \geq 4n - 1$. Con lo que hemos probado el lema. □

La cota superior para v en el Lema anterior se alcanza si y sólo si D o D' es un plano proyectivo mientras que la cota inferior se alcanza cuando D o D' son diseños de Hadamard.

CAPÍTULO 3

Grupos de automorfismos de diseños simétricos

Hemos dado hasta este punto, las definiciones y resultados más importantes dentro de la teoría de diseños que son necesarios para el desarrollo de los resultados centrales de esta tesis. Ahora, en esta parte, trabajaremos con la estructura algebraica de los diseños y de igual manera daremos las definiciones y resultados más importantes que son fundamentales en este trabajo.

Definición 8. Supongamos (X, A) y (Y, B) son dos diseños con $|X| = |Y|$. (X, A) y (Y, B) son isomorfos si existe una biyección $\alpha : X \to Y$ tal que

$$[\{\alpha(x) : x \in C\} : C \in A] = B.$$

Es decir, si renombramos a cada punto $x \in X$ como $\alpha(x)$ entonces la colección de bloques de A se transforma en la colección de bloques de B.

Como dijimos, con esta definición podemos saber cuándo dos diseños son algebraicamente iguales. Con ello se busca poder hacer una clasificación de los diseños simétricos de acuerdo con su grupo de automorfismos, donde un automorfismo de un diseño se define como a continuación:

Definición 9. En la definición anterior si $(Y, B) = (X, A)$ decimos que α es un automorfismo del diseño (X, A).

Notemos que como los automorfismos de diseños simétricos preservan la relación de incidencia, entonces un automorfismo de un diseño simétrico es también un automorfismo del complemento. Todo el conjunto de autormofismos de un diseño simétrico forma una estructura algebraica denominada grupo y un grupo se define como:

Definición 10. Un conjunto no vacío de elementos G se dice que forma un grupo si en G está definida una operación binaria $(\cdot)$ tal que:

1. $a, b \in G$ implica que $a \cdot b \in G$. (Cerradura).
2. $a, b, c \in G$ implica que $a \cdot (b \cdot c) = (a \cdot b) \cdot c$. (Asociatividad).
3. Existe un elemento $e \in G$ tal que $a \cdot e = e \cdot a = a$ para todo $a \in G$. (Existencia del elemento neutro o identidad).
4. Para todo $a \in G$ existe un elemento $a^{-1} \in G$ tal que $a^{-1} \cdot a = a \cdot a^{-1} = e$. (Existencia elementos inversos).

Si la operación es conmutativa decimos que el grupo es abeliano.

Hay subconjuntos del grupo que tienen las propiedades algebraicas derivadas del mismo, a estos se les denominan subgrupos.

Definición 11. Un subconjunto H de un grupo G se le llamará subgrupo de G si respecto a la operación de G, H forma un grupo. En este caso escribimos $H < G$.

Tenemos el siguiente criterio para ver si un subconjunto de un grupo dado es un subgrupo [6].

Lema 5. *Un subconjunto no vacío H de un grupo G es un subgrupo de G si y sólo si*

1. *$a, b \in H$ implica que $ab \in H$*
2. *$a \in H$ implica que $a^{-1} \in H$.*

Demostración. Si H es un subgrupo de G entonces es claro que se cumplen las condiciones (1) y (2). Supongamos que H es un subconjunto de G y que se verifican (1) y (2), para probar que H es subgrupo de G resta probar que la identidad e está en H y que se cumple la asociatividad para los elementos de H. Pero está última es claro que se cumple para los elementos de H, pues se cumple para todos los elementos de G. Luego por (2) tenemos que $a, a^{-1} \in H$ y también están en G que es un grupo, por lo que $aa^{-1} = e$ luego por (1) tenemos que $aa^{-1} \in H$ y entonces $e \in H$. □

El hecho de que los automorfismos de un diseño sean un grupo es importante, pues más adelante se dará una clasificación de un tipo especial de diseño. Dicha clasificación se basa en el teorema de O'Nan-Scott el cuál clasifica los grupos de permutación primitiva finitos. Por ello debemos primero dar el siguiente lema donde se prueba que el conjunto de automorfismos de un diseño forman un grupo.

Lema 6. *Sea $D = (X, A)$ un diseño y sea $Aut(D)$ el conjunto de todos los automorfismos de D, entonces $Aut(D)$ es un grupo con la composición de funciones.*

Demostración. Es claro que si $x, y \in Aut(D)$ entonces $xy : X \to X$ y además es biyectiva, pues la composición de funciones biyectivas es biyectiva. Para probar que $xy \in Aut(D)$ resta probar que $[\{xy(a) : a \in C\} : C \in A] = A$. Llamemos $T := [\{xy(a) : a \in C\} : C \in A]$, sea $C \in A$ entonces $\{xy(a) : a \in C\} \in T$, como $y \in Aut(D)$ entonces por definición $H := \{y(a) : a \in C\} \in A$, luego como $x \in Aut(D)$ entonces también por la definición de automorfismo tenemos que $\{x(b) : b \in H\} \in A$ pero si $b \in H$ entonces $b = y(a)$ para algún $a \in C$ entonces es claro que $\{xy(a) : a \in C\} = \{x(b) : b \in H\} \in A$ como C fue un elemento arbitrario de A entonces $\{xy(a) : a \in C\}$ fue elemento arbitrario de T por lo tanto $T \subseteq A$.
Sea ahora $P \in A$ como $y \in Aut(D)$ entonces por definición $[\{x(b) : b \in H\} : H \in A] = A$, es decir, $P \in [\{x(b) : b \in H\} : H \in A]$ por lo que existe un bloque $L \in A$ tal que $P = \{x(b) : b \in L\} \in A$. Como $y \in Aut(D)$ entonces por definición $[\{y(a) : a \in C\} : C \in A] = A$, es decir, $L \in [\{y(a) : a \in C\} : C \in A]$ por lo que existe un bloque $M \in A$ tal que $L = \{y(a) : a \in M\}$. Por lo tanto tenemos

$$P = \{x(b) : b \in L\} = \{x(b) : b \in \{y(a) : a \in M\}\} = \{xy(a) : a \in M\}$$

como $M \in A$ entonces por la definición de T se tiene que $P = \{xy(a) : a \in M\} \in T$ y como

P fue elemento arbitrario de A entonces $A \subseteq T$, con lo que tendríamos que $A = T$ y con ello $xy \in Aut(D)$.

Sean ahora $x, y, z \in Aut(D)$ entonces es claro que $x(yz) = (xy)z$ con lo que se cumple la asociatividad, además la función $e : X \to X$, $e(a) = a$ para todo $a \in X$ es el elemento identidad.

Resta probar que si $x \in Aut(D)$ entonces la función inversa $x^{-1} : X \to X$ está en $Aut(D)$. Es claro que es la función inversa es inyectiva, por lo que basta probar que $J := [\{x^{-1}(a) : a \in C\} : C \in A] = A$. Sea $C \in A$ entonces $\{x^{-1}(a) : a \in C\} \in J$ por definición como $x \in Aut(D)$ entonces $[\{x(a) : a \in H\} : H \in A] = A$, como $C \in A$ entonces $C \in [\{x(a) : a \in H\} : H \in A]$ por lo que existe un bloque $N \in A$ tal que $C = \{x(b) : b \in N\}$, así

$$\begin{aligned}\{x^{-1}(a) : a \in C\} &= \{x^{-1}(a) : a \in \{x(b) : b \in N\}\} \\ &= \{x^{-1}(x(b)) : b \in N\} = N \in A\end{aligned}$$

por lo tanto como C fue elemento arbitrario de A entonces $[\{x^{-1}(a) : a \in C\} : C \in A]$ fue elemento arbitrario de J y así tenemos que $J \subseteq A$.

Ahora sea $R \in A$ podemos escribir $R = \{x^{-1}x(a) : a \in R\}$ pero $x \in Aut(D)$ por lo que $[\{x(a) : a \in H\} : H \in A] = A$ entonces $\{x(a) : a \in R\} \in A$ es decir, existe un bloque $G \in A$ tal que $G = \{x(a) : a \in R\}$, y podemos escribir $R = \{x^{-1}(b) : b \in G\}$ por lo que $R \in J$ y como R es elemento arbitrario de A entonces $A \subseteq J$ y por lo tanto $J = A$ con lo que $x^{-1} \in Aut(D)$. □

Dado que lo que se busca es hacer una clasificación de los diseños de acuerdo a su grupo de automorfismos, es importante repasar algunas propiedades de los grupos. Por ello debemos introducir algunas definiciones y conceptos que serán de utilidad para entender el teorema de clasificación de O'Nan-Scott que provienen del álgebra abstracta. Comenzaremos con la definición de subgrupo normal:

Definición 12. Si G es un grupo y $N < G$ es un subgrupo de G diremos que N es un subgrupo normal de G si para toda $g \in G$ y toda $n \in N$ se cumple $gng^{-1} \in N$, y escribiremos $N \trianglelefteq G$.

Tenemos el siguiente criterio para distinguir cuando un subgrupo es normal:

Lema 7. *Si G es un grupo entonces $N \trianglelefteq G$ si y solo si $gNg^{-1} = N$ para todo $g \in G$ donde $gNg^{-1} := \{gng^{-1} \in G : n \in N\}$.*

Demostración. Supongamos que $N \trianglelefteq G$ entonces si $g \in G$ tenemos que de la definición 12 es claro que $gNg^{-1} \subseteq N$ y también es claro que $g^{-1}N(g^{-1})^{-1} = g^{-1}Ng \subseteq N$. Entonces $N = g(g^{-1}Ng)g^{-1} \subseteq gNg^{-1} \subseteq N$ por lo que $N = gNg^{-1}$. Supongamos ahora que $gNg^{-1} = N$ para toda $g \in G$ entonces en particular $gNg^{-1} \subseteq N$ con lo que $N \trianglelefteq G$. □

Dada la anterior definición podemos decir lo que es el grupo cociente, pero antes debemos dar la noción de clase lateral:

Definición 13. Sea G un grupo y $H < G$ un subgrupo, sea $g \in G$ entonces decimos que el conjunto $gH = \{gh \in G : h \in H\}$ es una clase lateral izquierda de H en G. Análogamente diremos que el conjunto $Hg = \{hg \in G : h \in H\}$ es la clase lateral derecha de H en G.

Así tenemos un lema que da un criterio para saber cuando un subgrupo es normal usando la noción de clases laterales, de hecho para un subgrupo normal sus clases laterales derechas son sus clases laterales izquierdas.

Lema 8. *Sea G un grupo y $N < G$ entonces N es un subgrupo normal de G si y sólo si $gN = Ng$ para toda $g \in G$.*

Demostración. Supongamos que $N \trianglelefteq G$ entonces para todo $g \in G$ tenemos que $gNg^{-1} = N$, entonces $(gNg^{-1})g = Ng$ lo que implica que $gN = Ng$. Ahora supongamos que $gN = Ng$ para toda $g \in G$ entonces $(gN)g^{-1} = (Ng)g^{-1}$ por lo que $gNg^{-1} = N$ y por lo tanto $N \trianglelefteq G$. □

Tenemos la siguiente definición que servirá para introducir la operación de un grupo cuyos elementos son las clases laterales de un subgrupo normal.

Definición 14. Sea G un grupo y $N \trianglelefteq G$, definimos la siguiente operación sobre el conjunto de las clases laterales de N, $NaNb = \{n_1an_2b \in G : n_1, n_2 \in N\}$ para cualesquiera $a, b \in G$.

Ahora tenemos el siguiente resultado que será de utilidad para demostrar que el conjunto de las clases laterales de un subgrupo normal forman un grupo y este es conocido como grupo cociente.

Lema 9. *Si G es un grupo y $N \trianglelefteq G$ entonces $NaNb = Nab$ para cualesquiera $a, b \in G$.*

Demostración. Supongamos que $N \trianglelefteq G$, sean $a, b \in G$, Na y Nb clases laterales derechas de N en G, entonces $NaNb = \{n_1an_2b \in G : n_1, n_2 \in N\}$, afirmamos que $NaNb = Nab$, sea $n_1, n_2 \in N$ entonces $n_1an_2b \in NaNb$, como N es subgrupo normal tenemos que existe un elemento $m \in N$ tal que $n_2 = a^{-1}ma$ por lo que $n_1an_2b = n_1aa^{-1}mab = n_1mab \in Nab$ pues $n_1m \in N$, por lo tanto $NaNb \subseteq Nab$. Sea $nab \in Nab$ entonces $na \in Na$ además $b = eb \in Nb$ por lo que $nab \in NaNb$ y así $Nab \subseteq NaNb$. Con esto podemos concluir que $NaNb = Nab$.

□

Ahora estamos en condiciones de definir el grupo cociente y lo haremos mediante el siguiente lema:

Lema 10. *Si G es un grupo y $N \trianglelefteq G$, denotamos por G/N el conjunto de todas las clases laterales derechas de N en G. Entonces G/N es un grupo mediante la operación definida en el Lema 9. A este se le denomina grupo cociente de G por N.*

Demostración. La cerradura quedó demostrada en el Lema 9. Probemos la asociatividad, sean $Na, Nb, Nc \in G/H$ clases laterales derechas con $a, b, c \in G$ entonces $Na(NbNc) = NaNbc = Na(bc) = N(ab)c = NabNc = (NaNb)(Nc)$ así queda demostrada tal propiedad.
Afirmamos que el elemento identidad es $N = Ne \in G/N$, pues sea $Na \in G/N$ una clase lateral derecha de N en G entonces $NaNe = Nae = Na$ de igual forma tenemos que $NeNa = Nea = Na$, por lo tanto es cierta nuestra afirmación y tenemos el elemento identidad el cual es único.
Afirmamos que dada una clase lateral derecha $Na \in G/N$ su elemento inverso es Na^{-1}, veamos, $NaNa^{-1} = Naa^{-1} = Ne = N$ análogamente $Na^{-1}Na = Na^{-1}a = Ne = N$, es decir, el producto de Na por la derecha y por la izquierda con Na^{-1} da el elemento neutro, por lo que efectivamente Na^{-1} es el elemento inverso de Na. □

Ahora daremos la definición también usada por O'Nan-Scott de grupo simple, en esta definición se habla del grupo trivial el cual es el grupo que tiene como único elemento a la identidad.

Definición 15. Un grupo simple es un grupo que sólo tiene como subgrupos normales al grupo trivial y a sí mismo.

Algunos ejemplos de grupos que se utilizan en este trabajo son los siguientes:

1. Sea $Z(G) = \{a \in G : ax = xa \quad \forall x \in G\}$ este se conoce como el centro de G y es un subgrupo de G.

2. El grupo simétrico S_n de un conjunto X de n elementos, es el grupo cuyos elementos son todas las permutaciones de los n elementos de X, y cuya operación es la composición de dichas permutaciones.

3. Una permutación par es aquella que se escribe como composición de un número par de trasposiciones. Así el subgrupo de S_n consistente de todas las permutaciones pares se le conoce como el grupo alternante y se le denota como A_n.

4. El conjunto de todos los automorfismos de un espacio vectorial V forman un grupo conocido como grupo lineal general de V y se le denota por $GL(V)$. En el caso particular en que $V = \mathbb{F}^n$ con $\mathbb{F}$ un campo se escribe su grupo lineal general como $GL(n, \mathbb{F})$, en este caso dicho grupo es isomorfo al grupo de matrices invertibles $n \times n$ con entradas en $\mathbb{F}$. Si el campo es finito y de orden q se escribe $GL(n, q)$ o $GL_n(q)$.

5. Sea $\mathbb{F}$ un campo, consideremos el subgrupo de $GL(n, \mathbb{F})$ de las matrices de determinante 1. Lo denotamos por $SL(n, \mathbb{F})$ y se le conoce como grupo lineal especial. Si el campo es finito y de orden q se escribe $SL(n, q)$ o $SL_n(q)$.

6. Sea $\mathbb{F}$ un campo y consideremos el espacio vectorial $V = \mathbb{F}^n$ y sea el espacio proyectivo $P^{n-1}(\mathbb{F})$ (el conjunto de los subespacios uno dimensionales de $\mathbb{F}^n$). Sea $I \in GL(n, \mathbb{F})$ la matriz identidad y sea $Z = \{cI : c \in Z(\mathbb{F}), c \neq 0\}$ a este se le conoce como el grupo de las transformaciones escalares. Se define el grupo

$$PGL(n, \mathbb{F}) = GL(n, \mathbb{F})/Z$$

   y se le conoce como grupo lineal general proyectivo. Si el campo es finito y de orden q se escribe $PGL(n, q)$ o $PGL_n(q)$.

7. Sea $\mathbb{F}$ un campo y consideremos el espacio vectorial $V = \mathbb{F}^n$, entonces definimos el grupo especial lineal proyectivo como

$$PSL(n, \mathbb{F}) = SL(n, \mathbb{F})/(SL(n, \mathbb{F}) \cap Z)$$

Nótese que dada la definición de Z entonces $SL(n,\mathbb{F})\cap Z$ es el subgrupo de transformaciones escalares cuyo determinante es uno. Si el campo es finito y de orden q se escribe $PSL(n,q)$ o $PSL_n(q)$.

En este trabajo nos interesa la interacción entre el grupo de automorfismos del diseño y el conjunto de lo que definimos como banderas de un diseño simétrico. Esta interacción entre un grupo y un conjunto también se define en el álgebra abstracta y se le conoce como acción del grupo en el conjunto. Empecemos recordando dicha definición y algunos tipos de acciones y sus propiedades tanto dentro del álgebra misma como ya en el área de los diseños simétricos.

Definición 16. Si G es un grupo y X es un conjunto, entonces una acción de grupo ϕ de G en X es una función

$$\phi : G \times X \to X :$$

tal que se satisface lo siguiente (con $\phi(g,x) = gx$ para toda $g \in G$ y toda $x \in X$)

i) Para todo $g,h \in G$ y toda $x \in X$ se tiene $(gh)x = g(hx)$,

ii) Para toda $x \in X$ se tiene $ex = x$, con e el elemento identidad de G.

En este caso decimos que X es un G-conjunto.

Cuando se estudia la acción de un grupo sobre un conjunto surgen ciertos elementos del grupo que se destacan por que dejan fijo a un elemento del conjunto, estos elementos forman lo que se denomina estabilizador de un elemento del conjunto.

Definición 17. Sea G un grupo y X un G-conjunto, sea $x \in X$, definimos el estabilizador de x como $G_x = \{g \in G | gx = x\}$ y definimos la órbita de un elemento $x \in X$ como $Gx = \{gx \in X | g \in G\}$.

En particular el estabilizador de un elemento de un G-conjunto es un subgrupo del grupo G lo cual se prueba en el siguiente Lema:

Lema 11. *Sea G un grupo y X un G-conjunto, sea $x \in X$, entonces el estabilizador de x, $G_x = \{g \in G | gx = x\}$ es un subgrupo de G, es decir, $G_x < G$.*

Demostración. Sean $a,b \in G_x$ entonces $bx = x$ luego, $abx = ax = x$ por lo que $ab \in G_x$.
Sea $a \in G_x$ entonces $ax = x$ entonces tenemos que $x = a^{-1}ax = a^{-1}x$, por lo tanto $a^{-1} \in G_x$.
Usando el Lema 5 probamos que $G_x < G$. □

En este trabajo nos centramos en acciones de grupo transitivas en banderas, entonces necesitamos introducir la definición de acción transitiva.

Definición 18. Sea X un G-conjunto decimos que la acción es transitiva si para toda $x, y \in X$ existe $g \in G$ tal que $gx = y$.

Y tenemos el siguiente resultado:

Lema 12. *Sea X un G-conjunto entonces la acción es transitiva si y sólo si existe una única órbita.*

Demostración. Supongamos que G actúa transitivamente en X entonces si $x \in X$ es claro que $Gx \subseteq X$, ahora sea un elemento $y \in X$ entonces dado que la acción es transitiva existe un elemento $g \in G$ tal que $gx = y$ dada la definición de una órbita tenemos que $y \in Gx$ por lo que $X \subseteq Gx$ y por lo tanto $Gx = X$ para todo $x \in X$, es decir, existe una única órbita.
Supongamos ahora que existe una única órbita, sea $x \in X$ de tal forma que Gx sea tal órbita entonces todo elemento de X debe estar ahí, es decir, dado $y \in X$ entonces $y \in Gx$ y de la definición de órbita debemos tener que $y = gx$ para algún $g \in G$. Por lo tanto para toda $y \in X$ existe una $g \in G$ tal que $y = gx$. Sean ahora dos elementos arbitrarios $a, b \in X$ entonces existen $m, n \in G$ tales que $a = mx$ y $b = nx$ de esta última tenemos que $x = n^{-1}b$ y por lo tanto $a = mn^{-1}b$ con $mn^{-1} = h \in G$, por lo tanto dados dos elementos $a, b \in X$ arbitrarios existe un elemento $h \in G$ tal que $a = hb$ por lo que la acción es transitiva. □

Definición 19. Sea X un conjunto y sea G un grupo cuyos elementos son permutaciones de X, es decir, biyecciones de X en X. A G se le conoce como grupo de permutaciones. Si este grupo es transitivo y además el subgrupo estabilizador de un punto $x \in X$ actúa transitivamente en $X - \{x\}$, decimos que G es un grupo 2-transitivo.
Equivalentemente, G es un grupo 2-transitivo si es un grupo de permutaciones de X y actúa transitivamente en el conjunto de las parejas ordenadas $\{(x, y) \in X \times X : x \neq y\}$.

Las siguientes dos definiciones nos dan dos tipos de acciones de grupo sobre un conjunto que son importantes dentro de la teoría de grupos de permutaciones.

Definición 20. Sea X un G-conjunto. Si para todo $x \in X$, $gx = x$ implica que g es la identidad de G (es decir, sólo el elemento identidad fija a cualquier $x \in X$), entonces decimos que la acción es libre.

Definición 21. Dado un G-conjunto X, si la acción es transitiva y libre, es decir, que para toda $x, y \in X$ existe una única $g \in G$ tal que $gx = y$, diremos que la acción es regular.

Como hemos mencionado estamos interesados en clasificar a los diseños simétricos cuyo grupo de automorfismos es transitivo en las banderas del diseño, para ello necesitamos primero ver si podemos definir una acción sobre este conjunto con base en la definición 16 y esto es cierto por el siguiente:

Lema 13. *Sea $D = (X, A)$ un diseño simétrico, cuyo grupo de automorfismos es G, sea F el conjunto de banderas de D, entonces F es un G-conjunto.*

Demostración. Definimos la acción de G en F dada por $g(p, B) = (gp, gB)$, es claro que $g(p, B) \in F$ pues por la definición 8, $gB \in A$ además de la definición 7 tenemos que $p \in B$ y como $gB = \{gb | b \in B\}$ entonces $gp \in gB$ y por la definición 7 tenemos que $g(p, B) = (gp, gB) \in F$.
Luego si $e \in G$ es el elemento identidad entonces es claro que $e(p, B) = (ep, eB) = (p, B)$ para toda $p \in X$ y toda $B \in A$. Además, sean $g, h \in G$ y $(p, B) \in F$ entonces ya que g y h están en G que es un grupo y por lo tanto la operación es asociativa se tiene $(gh)(p, B) = ((gh)p, (gh)B) = (g(hp), g(hB)) = g(hp, hB) = g(h(p, B))$. Así tenemos de la definición 16 que F es un G-conjunto. □

Nótese en el lema anterior que como G es el grupo de automorfismos del diseño D, entonces X también es un G-conjunto con la acción definida de manera natural como $gx = g(x)$, para todo $g \in G$ y toda $x \in X$, así mismo A es un G-grupo con la acción $gB = g(B)$, para todo $g \in G$ y toda $B \in A$.

Una vez que hemos demostrado que la acción del grupo de automorfismos sobre el conjunto de banderas está bien definida, podemos hablar de un grupo de automorfismos transitivo en banderas.

Definición 22. Sea D un diseño simétrico, cuyo grupo de automorfismos es G, decimos que G es transitivo en banderas si la acción, definida en el Lema 13, sobre el conjunto de banderas F, es transitiva.

Debemos notar que aunque un diseño y su complemento tienen el mismo grupo de automorfismos, la transitividad en banderas sobre el diseño no implica transitividad en banderas sobre el complemento.

Estudiemos algunas consecuencias de tener un diseño simétrico con un grupo de automorfismos transitivo en banderas. En particular tenemos el siguiente resultado que relaciona de cierta forma la transitividad en banderas del grupo con la transitividad en bloques del estabilizador de un punto del diseño.

Lema 14. *Sea $D = (X, A)$ un diseño cuyo grupo de automorfismos es G y cuyo conjunto de banderas es F, si G es transitivo en banderas entonces G_x es transitivo en el conjunto de bloques de D que contienen a x para todo $x \in X$.*

Demostración. Supongamos que G es transitivo en el conjunto de banderas F, sea $x \in X$ y sean $(x, M), (x, N) \in F$ dos banderas tales que los bloques contienen a x, entonces como la acción es transitiva en banderas existe $g \in G$ tal que $g(x, M) = (x, N)$. Dada la acción definida en el Lema 13 tenemos que $g(x, M) = (gx, gM) = (x, N)$, es decir, $gx = x$ y $gM = N$ por lo que $g \in G_x$, es decir, dados dos bloques $M, N \in A$ arbitrarios que contienen a un punto $x \in X$ existe un elemento $g \in G_x$ tal que $gM = N$. Entonces G_x actúa transitivamente en los bloques del diseño que contienen a x, por lo que hemos probado el Lema. □

Además tenemos el siguiente resultado bastante importante para lo que sigue y que nos habla de la importancia de pedir la transitividad en banderas para el grupo de automorfismos de un diseño.

Lema 15. *Sea $D = (X, A)$ un diseño cuyo grupo de automorfismos es G y cuyo conjunto de banderas es F, si G es transitivo en banderas entonces G es transitivo en puntos.*

Demostración. Sean $x, y \in X$ entonces $x \in M$, $y \in N$ para algunos $M, N \in A$ por lo que tenemos que $(x, M), (y, N) \in F$, como G es transitivo en banderas, existe $g \in G$ tal que $g(x, M) = (y, N)$. Pero dada la acción definida en el Lema 13 tendremos que $(y, N) = g(x, M) = (gx, gM)$ por lo que $gx = y$, es decir, existe un $g \in G$ tal que $gx = y$ para todo $x, y \in X$, por lo tanto la acción es transitiva en puntos. □

Es decir, pedir transitividad en banderas para un grupo de automorfismos de un diseño simétrico es una condición más fuerte que pedir solo la transitividad en puntos.

Veamos algunos ejemplos de diseños que admiten grupos de automorfismos transitivos en banderas, para ello debemos estudiar antes una manera de obtener diseños simétricos que es mediante los conocidos conjuntos diferencia:

Definición 23. Un (v, k, λ) conjunto diferencia es un subconjunto D de un grupo G tal que el orden de G es v, el tamaño de D es k y cada elemento $g \in G$ distinto de la identidad puede ser expresado como $g = d_1 d_2^{-1}$ con $d_1, d_2 \in D$ en exactamente λ formas con el producto de G.

Si D es un (v, k, λ)-conjunto diferencia y $g \in G$ entonces la clase lateral $gD = \{gd \in G : d \in D\}$ es también un conjunto diferencia y es llamado la traslación de D por g. El conjunto de todas las traslaciones de un conjunto diferencia D y los puntos de D forman un (v, k, λ)-diseño simétrico.

Estamos en condiciones de dar algunos ejemplos de diseños cuyo grupo de automorfismos es transitivo en banderas, de hecho los siguientes ejemplos son los seis biplanos conocidos tales que su grupo de automorfismos es transitivo en banderas.
Para $k = 3$ existe un único $(4, 3, 2)$ biplano, donde un biplano es un (v, k, λ) diseño simétrico con $\lambda = 2$. Este biplano en particular se construye de un conjunto diferencia en $\mathbb{Z}_4$, cuyo grupo de automorfismos es S_4 y cuyo estabilizador es S_3.

Para $k = 4$ tenemos también un único $(7, 4, 2)$ biplano que es complemento de $PG(2, 7)$, este se construye de un conjunto diferencia en $\mathbb{Z}_7$, cuyo grupo de automorfismos es $PSL_2(7)$ y cuyo estabilizador es S_4.

Para $k = 5$ tenemos también un único $(11, 5, 2)$ biplano construido de un conjunto diferencia de cuadrados en $\mathbb{Z}_{11}$, cuyo grupo de automorfismos es $PSL_2(11)$ y cuyo estabilizador es A_5.

Para $k = 6$ tenemos dos $(16, 6, 2)$ biplanos que admiten un grupo de automorfismos transitivo en banderas, el primero se construye de un conjunto diferencia en $\mathbb{Z}_2^4$ cuyo grupo de automorfismos es $\mathbb{Z}_2^4 S_6$ donde $\mathbb{Z}_2^4$ es el grupo de translaciones y S_6 es el estabilizador, transitivo en los 6 bloques que contienen a 0.
El segundo se construye de un conjunto diferencia en $\mathbb{Z}_2 \times \mathbb{Z}_8$ y el grupo de automorfismos es $(\mathbb{Z}_2 \times \mathbb{Z}_8)(S_4.2)$ con $\mathbb{Z}_2 \times \mathbb{Z}_8$ el grupo de traslaciones actuando regularmente y $S_4.2$ el estabilizador.

Para $k = 9$ tenemos un único $(37, 9, 2)$ biplano que admite un grupo de automorfismos transitivo en banderas, este se construye de un conjunto diferencia de los residuos cuadráticos en $\mathbb{Z}_{37}$, el grupo de automorfismos es $\mathbb{Z}_{37}.\mathbb{Z}_9$ donde $\mathbb{Z}_{37}$ es el grupo de translaciones y $\mathbb{Z}_9$ el estabilizador, transitivo en los nueve bloques que contienen a 0.

Así los seis biplanos que admiten un grupo de automorfismos transitivo en banderas con sus grupos de automorfismos y estabilizadores son:

1. $(4, 3, 2), S_4, S_3$
2. $(7, 4, 2), PSL_2(7), S_4$
3. $(11, 5, 2), PSL_2(11), A_5$
4. $(16, 6, 2), \mathbb{Z}_2^4 S_6, S_6$
5. $(16, 6, 2), (\mathbb{Z}_2 \times \mathbb{Z}_8)(S_4.2), S_4.2$
6. $(37, 9, 2), \mathbb{Z}_{37}.\mathbb{Z}_9, \mathbb{Z}_9$

Al definir una estructura algebraica normalmente se hace también la introducción de aplicaciones que preserven las propiedades algebraicas de dicha estructura, en este caso ésta es lo que se conoce como homomorfismo de grupos.

Definición 24. Sean M y N dos grupos. Una aplicación $\phi : M \to N$ es un homomorfismo si para todo $a, b \in M$ se tiene que $\phi(ab) = \phi(a)\phi(b)$. Si dicho homomorfismo es biyectivo entonces se dice que ϕ es un isomorfismo y M y N son grupos isomorfos, cuando esto sucede

escribiremos $M \cong N$. Si existe un isomorfismo de M en si mismo llamaremos a este un automorfismo de M.

Al igual que para los diseños el conjunto de automorfismos de un grupo forma a su vez un grupo, esto lo probamos en el siguiente:

Lema 16. *Si G es un grupo, el conjunto de todos los automorfismos de G denotado por $Aut(G)$ es un grupo.*

Demostración. Probemos la cerradura, sean $\alpha, \beta \in Aut(G)$ entonces es claro que $\alpha\beta$ es biyectiva, sean ahora $a, b \in G$ entonces $\alpha\beta(ab) = \alpha(\beta(a)\beta(b)) = (\alpha\beta(a))(\alpha\beta(b))$ y por lo tanto $\alpha\beta \in Aut(G)$.
Si $\alpha, \beta, \gamma \in Aut(G)$ es claro que se cumple $\alpha(\beta\gamma) = (\alpha\beta)\gamma$ con lo que tenemos la asociatividad.
El elemento identidad es como sigue, $e : G \to G$ tal que $e(g) = g$ para todo $g \in G$ y es claro que $e(ab) = ab = e(a)e(b)$ por lo que $e \in Aut(G)$.
Por último tomemos como elemento inverso de $\alpha \in Aut(G)$ como la aplicación inversa α^{-1} probemos que está en $Aut(G)$, sean $a, b \in G$ entonces $\alpha((\alpha^{-1}a)(\alpha^{-1}b)) = (\alpha(\alpha^{-1}a))(\alpha(\alpha^{-1}b)) = (e(a))(e(b)) = ab$, es decir, $\alpha((\alpha^{-1}a)(\alpha^{-1}b)) = ab$ y por lo tanto $(\alpha^{-1}a)(\alpha^{-1}b) = \alpha^{-1}(ab)$.
Con lo cual probamos que efectivamente $Aut(G)$ es un grupo. □

Acompañada de la definición de automorfismo viene la de automorfismo interno la cual es muy utilizada dentro del teorema de O'Nan-Scott.

Definición 25. Sea G un grupo y $g \in G$ un elemento. Definimos $T_g : G \to G$ como $T_g x = g^{-1}xg$ para toda $x \in G$

Es claro que $T_g \in Aut(G)$ para toda $g \in G$ pues es suprayectiva dado que si $y \in G$ y sea $x = gyg^{-1}$ entonces x cumple que $T_g x = T_g(gyg^{-1}) = g^{-1}gyg^{-1}g = y$. Además es inyectiva pues si $T_g x = T_g y$ entonces $g^{-1}xg = g^{-1}yg$ lo que implica claramente que $x = y$. Luego si $x, y \in G$ entonces $T_g xy = g^{-1}xyg = g^{-1}xgg^{-1}yg = T_g x T_g y$, por lo tanto se cumple que efectivamente $T_g \in Aut(G)$.

A T_g se le conoce como automorfismo interno correspondiente a g y al conjunto de todos

los automorfismos internos de G se le denota por $Inn(G)$. Este último es de hecho un subgrupo normal de $Aut(G)$.

Lema 17. *Sea G un grupo, entonces $Inn(G) \trianglelefteq Aut(G)$.*

Demostración. Sea $T_g, T_h \in Inn(G)$ entonces si $x \in G$ tendremos que $T_g T_h x = g^{-1}h^{-1}xhg = (hg)^{-1}xhg = T_{hg}x$ por lo que $T_g T_h \in Inn(G)$. Sea $T_g \in Inn(G)$ entonces afirmamos que $(T_g)^{-1} = T_{g^{-1}}$, en efecto $T_g T_{g^{-1}} x = g^{-1}(g^{-1})^{-1}xg^{-1}g = x$, análogamente $T_{g^{-1}}T_g x = (g^{-1})^{-1}g^{-1}xgg^{-1}$, y claramente $T_{g^{-1}} \in Inn(G)$ por lo que de acuerdo al Lema 11 tenemos $Inn(G) < Aut(G)$.
Probemos ahora que es un subgrupo normal, sea $\alpha \in Aut(G)$ y $T_g \in Inn(G)$ ambos arbitrarios, sea además $x \in G$, entonces $\alpha T_g \alpha^{-1} x = \alpha(g^{-1}(\alpha^{-1}x)g) = \alpha(g^{-1})(\alpha(\alpha^{-1}x)\alpha(g) = \alpha(g^{-1})x\alpha(g) = (\alpha(g))^{-1}x\alpha(g) = T_{\alpha(g)}x$ por lo tanto como $x \in G$ fue arbitrario tenemos que $\alpha T_g \alpha^{-1} = T_{\alpha(g)} \in Inn(G)$ con lo cual concluimos que $Inn(G) \trianglelefteq Aut(G)$ pues $\alpha \in Aut(G)$ y $T_g \in Inn(G)$ fueron elementos arbitrarios. □

Otro concepto importante del que se hace uso dentro de este teorema de clasificación es el concepto de producto semidirecto así como del producto directo. Veámos estas definiciones mediante los siguientes lemas.

Lema 18. *Sean $G_1, G_2, ..., G_n$ grupos, el producto cartesiano $G_1 \times G_2 \times ... \times G_n$ dotado con la operación $(g_1, ..., g_n)(h_1, ..., h_n) = (g_1h_1, ..., g_nh_n)$ con $g_i, h_i \in G_i$ y $i = 1, ..., n$, posee la estructura de grupo y se le conoce como producto directo de los grupos $G_1, G_2, ..., G_n$.*

Demostración. La cerradura es clara, mientras que la asociatividad es heredada de la estructura de los grupos que originan al producto cartesiano pues si $g_i, h_i, m_i \in G_i$ y $i = 1, ..., n$ entonces

$$\begin{aligned}(g_1, ..., g_n)((h_1, ..., h_n)(m_1, ..., m_n)) &= (g_1, ..., g_n)(h_1m_1, ..., h_nm_n) = \\ &= (g_1(h_1m_1), ..., g_n(h_nm_n)) = ((g_1h_1)m_1, ..., (g_nh_n)m_n) = \\ = (g_1h_1, ..., g_nh_n)(m_1, ..., m_n) &= ((g_1, ..., g_n)(h_1, ..., h_n))(m_1, ..., m_n).\end{aligned}$$

Luego el elemento identidad será $(e_1, ..., e_n)$ con e_i el elemento identidad del grupo G_i para $i = 1, ..., n$ pues si $(g_1, .., g_n) \in G_1 \times G_2 \times ... \times G_n$ entonces

$$(g_1, ..., g_n)(e_1, ..., e_n) = (g_1e_1, ..., g_ne_n) = (g_1, ..., g_n).$$

Análogamente se tiene que $(e_1, ..., e_n)(g_1, ..., g_n) = (g_1, ..., g_n)$.
Sea $g_i \in G_i$ y $i = 1, ..., n$ entonces el elemento inverso de $(g_1, ..., g_n)$ es $(g_1^{-1}, ..., g_n^{-1})$, pues

$$(g_1, ..., g_n)(g_1^{-1}, ..., g_n^{-1}) = (g_1 g_1^{-1}, ..., g_n g_n^{-1}) = (e_1, ..., e_n).$$

Análogamente tenemos que $(g_1^{-1}, ..., g_n^{-1})(g_1, ..., g_n) = (e_1, ..., e_n)$. Por lo tanto hemos probado que el producto directo de los grupos G_i con $i = 1, .., n$ es un grupo. □

Ahora veamos la definición de producto semidirecto mediante el siguiente lema donde probamos que éste forma al igual que el producto directo un grupo.

Lema 19. *Sean G, H grupos y $\phi : H \to Aut(G)$ un homomorfismo de grupos. Dotamos al producto cartesiano $G \times H$ con la operación*

$$(a, b) \rtimes_\phi (c, d) = (a\phi_b(c), bd),$$

para todo $a, c \in G$ y toda $b, d \in H$. Entonces $G \times H$ con este producto forma un grupo al que se le conoce como el producto semidirecto de G y H con respecto a ϕ y lo denotamos por $G \rtimes_\phi H$.

Demostración. La cerradura es clara, probemos la asociatividad. Sean $a, c, e \in G$ y $b, d, f \in H$ entonces

$$\begin{aligned}
(a, b) \rtimes_\phi ((c, d) \rtimes_\phi (e, f)) &= (a, b) \rtimes_\phi (c\phi_d(e), df) = \\
&= (a\phi_b(c\phi_d(e)), b(df)) = \\
&= (a\phi_b(c)\phi_b\phi_d(e), (bd)f) \\
&= (a\phi_b(c)\phi_{bd}(e), (bd)f) \\
&= (a\phi_b(c), bd) \rtimes_\phi (e, f) \\
&= ((a, b) \rtimes_\phi (c, d)) \rtimes_\phi (e, f)
\end{aligned}$$

Luego el elemento neutro es (e_g, e_h) con e_g el elemento neutro de G y e_h el elemento neutro de H, en efecto sea $a \in G$ y $b \in H$ entonces

$$(a, b) \rtimes_\phi (e_g, e_h) = (a\phi_b(e_g), be_h) = (ae_g, be_h) = (a, b)$$

Análogamente tendremos

$$(e_g, e_h) \rtimes_\phi (a, b) = (e_g \phi_{e_h}(a), e_h b) = (e_g a, e_h b) = (a, b)$$

Por último tendremos que el elemento inverso de (a, b) es $(\phi_{b^{-1}}(a^{-1}), b^{-1})$, en efecto

$$\begin{aligned}(a, b) \rtimes_\phi (\phi_{b^{-1}}(a^{-1}), b^{-1}) &= (a\phi_b \phi_{b^{-1}}(a^{-1}), bb^{-1}) \\ &= (a\phi_{bb^{-1}}(a^{-1}), e_h) \\ &= (a\phi_{e_h}(a^{-1}), e_h)) \\ &= (aa^{-1}, e_h) = (e_g, e_h)\end{aligned}$$

Así mismo tendremos

$$\begin{aligned}(\phi_{b^{-1}}(a^{-1}), b^{-1}) \rtimes_\phi (a, b) &= (\phi_{b^{-1}}(a^{-1})\phi_{b^{-1}}(a), b^{-1}b) \\ &= (\phi_{b^{-1}}(a^{-1}a), e_h) \\ &= (\phi_{b^{-1}}(e_g), e_h)) \\ &= (e_g, e_h)\end{aligned}$$

Con lo cual hemos probado que en efecto el producto semidirecto de dos grupos es también un grupo. □

Podemos con la definición de producto semidirecto introducir otro ejemplo de un grupo que se utiliza en este trabajo, dicho grupo es el grupo afín o grupo lineal afín.
Sea $\mathbb{F}$ un campo, consideremos el espacio vectorial $V = \mathbb{F}^n$ entonces definimos el grupo

$$AGL(n, \mathbb{F}) = \mathbb{F}^n \rtimes_\phi GL(n, \mathbb{F})$$

con $\phi_A(x) = Ax$ para toda $A \in GL(n, \mathbb{F})$ y todo $x \in \mathbb{F}^n$. A este grupo se le conoce como grupo afín general del espacio afín sobre el campo $\mathbb{F}$. Si el campo es finito de orden q escribimos también $AGL(n, q)$ o bien $AGL_n(q)$.

Al buscar clasificar los diseños por sus grupos de automorfismos nos encontramos que hay dos tipos de grupos transitivos, los primitivos e imprimitivos, en este trabajo además de pedir a los grupos de automorfismos que sean transitivos en banderas pediremos que sean primitivos en puntos. Nos centramos en este tipo de grupos pues al pedir esta condición, el Teorema de O'Nan-Scott nos da una primera clasificación. Así introducimos la siguiente:

Definición 26. Sea X un conjunto y sea G un grupo cuyos elementos son permutaciones de X, si G actúa transitivamente en X y además G no preserva ninguna partición no trivial de X, decimos que G es primitivo. Si G preserva alguna partición no trivial de X decimos que G es imprimitivo.

Una manera análoga de definir una acción primitiva es la siguiente, con las hipótesis dadas antes, sea Γ un subconjunto de X, si para todo $g \in G$ se cumple que $g\Gamma = \Gamma$ o $\Gamma \cap g\Gamma = \emptyset$ entonces decimos que Γ es un bloque. A X y a $\{\alpha\}$ con α un elemento de X se les llama bloques triviales. Decimos que G es primitivo en X si los únicos bloques de X son los triviales.

3.1. Teorema de O'Nan-Scott

Ahora estudiaremos los grupos primitivos y veremos la siguiente clasificación de ellos, esta es debida a O'Nan-Scott.

Definición 27. Sean A, B grupos entonces denotamos $A.B$ a la extensión de A por B. Es decir, $A.B$ es un grupo tal que la sucesión

$$0 \to A \to A.B \to B \to 0 \tag{3.1}$$

es exacta, esto es $\alpha : A \to A.B$ es inyectiva, $\beta : A.B \to B$ es sobreyectiva y además induce un isomorfismo $A.B/im(\alpha) \cong B$.

Definición 28. Si G, H son grupos de permutaciones en Ω y Δ respectivamente, decimos que G es una permutación equivalente a H si existe una biyección $\phi : \Omega \to \Delta$ y un isomorfismo $\psi : G \to H$ tales que $\phi(g\omega) = (\psi g)(\phi\omega)$.

Notamos que si Ω y Δ son identificados mediante la biyección ϕ entonces G y H consisten del mismo conjunto de permutaciones en Ω.
También haremos uso del concepto del soclo de un grupo para ello necesitamos aclarar que un subgrupo normal mínimo de un grupo G es un subgrupo normal no trivial N tal que el único subgrupo propio de N que es normal en G es el subgrupo trivial. A continuación daremos la definición del soclo de un gupo.

Definición 29. Sea G un grupo definimos como el soclo de G al producto de todos los subgrupos normales mínimos de G. Si G no tiene subgupos normales mínimos entonces decimos que su soclo es trivial.

A continuación introduciremos la definción de los cinco tipos de grupos de permutaciones primitivos de los cuales hace mención el Teorema de O'Nan-Scott. Para lo que sigue G será un grupo de permutación primitiva en un conjunto finito Ω de tamaño n y α será un punto en Ω. Denotaremos B como el soclo de G, tenemos que cuando un grupo es finito su soclo es un producto directo de grupos simples, por lo que entonces $B \cong T^k$ para algún $k \geq 1$ y T es un grupo simple.

1. Grupos afines

   En este caso $T = \mathbb{Z}_p$ para algún primo p y B es el único subgrupo normal mínimo de G y es regular en Ω de grado $n = p^k$. El conjunto Ω puede ser identificado con $B = \mathbb{Z}_p^k$ así que G es subgrupo del grupo afín $AGL(k,p)$, que es el grupo de todas las transformaciones invertibles afines del espacio afín (con el espacio vectorial $\mathbb{Z}_p^k$ como el grupo de traslaciones) en si mismo. Recordemos que entonces $AGL(k,p) = \mathbb{Z}_p^k \rtimes GL(k,p)$ con $GL(k,p)$ el grupo lineal general, es decir, el grupo de todas las matrices invertibles de orden k con entradas en $\mathbb{Z}_p$. Y $G_\alpha = G \cap GL(k,p)$ irreducible en B.

2. Grupos casi simples

   Aquí $k = 1$, T es un grupo no abeliano simple y $T \trianglelefteq G \leq Aut(T)$. Además $T_\alpha \neq 1$.

3. En este caso $B \cong T^k$ con $k \geq 2$ y T un grupo simple no abeliano. Tenemos tres tipos de grupos

   a) Acción diagonal simple

      Sea $W = \{\pi(a_1, ..., a_k) | a_i \in Aut(T), \pi \in S_k, a_i \equiv a_j \pmod{Inn(T)} \quad \forall i, j\}$, donde $\pi \in S_k$ sólo permuta las componentes a_i naturalmente. Con la multiplicación obvia, W es un grupo con soclo $B \cong T^k$ y $W = B.(Out(T \times S_k))$, Definimos una acción de W en Ω por

      $W_\alpha = \{\pi(a, ..., a) | a \in Aut(T), \pi \in S_k\}$ así $W_\alpha \cong Aut(T) \times s_k, B_\alpha \cong T$ y $n =$

$|T|^{n-1}$.

Para $1 \leq i \leq k$ sea T_i el subgrupo de B consistiendo de las k-tuplas con 1 en todas las entradas excepto la i-ésima componente, así $T_i \cong T$ y $B \cong T_1 \times ... \times T_k$. Sea $L = \{T_1, ..., T_k\}$ de modo que W actúa en L. Decimos que el subgrupo G de W es de tipo diagonal simple si $B \leq G$ y siendo P el grupo de permutaciones G^L, una de las siguientes condiciones se tiene

i) P es primitivo en L,

ii) $k = 2$ y $P = 1$.

Tenemos $G_\alpha \leq Aut(T) \times P$ y $G \leq B.(Out(T \times P))$. Más aún en el caso (i) B es el único subgrupo normal mínimo de G y en el caso (ii) G tiene dos subgrupos normales mínimos T_1 y T_2 ambos regulares en Ω.

b) Acción producto

Sea H un grupo de permutación primitivo en un conjunto Γ de tipo casi simple o de diagonal simple. Para $l > 1$ sea $W = HwrS_l$ y hacemos actuar W en $\Omega = \Gamma^l$ con la acción producto natural. Recordemos que $HwrS_l = H^l \rtimes S_l$ donde S_l actúa en H^l de la siguiente manera $w = b(h_1, ..., h_n) = (h_{b1}, ..., h_{bn}) \quad \forall b \in S_l, (h_1, ..., h_n) \in H^l$. Luego la acción producto natural de W en $\Omega = \Gamma^l$ estará dada por $w(x_1, .., x_n) = b(h_1, ..., h_n)[(x_1, .., x_n)] = (x_{b1}^{h_{b1}}, ..., x_{bn}^{h_{bn}})$ para todo $w \in W$ y $(x_1, .., x_n) \in \Omega$.
Entonces para toda $\gamma \in \Gamma$ y $\alpha = (\gamma, ..., \gamma) \in \Omega$ tenemos $W_\alpha = H_\gamma wrS_l$ y $n = |\Gamma|^l$, si K es el soclo de H entonces el soclo B de W es K^l y $B_\alpha = K_\gamma^l \neq 1$.
Ahora W actúa naturalmente en los l factores de K^l y decimos que el subgrupo G de W es de tipo acción producto si $B \leq G$ y G actúa transitivamente en estos l factores.

Luego si

i) H es de tipo casi simple, $K \cong T$, $k = l$ y B es el único subgrupo normal mínimo de G,

ii) H es de tipo diagonal simple, $K \cong T^{k/l}$ y G y H tienen m subgrupos normales mínimos , donde $m \leq 2$, si $m = 2$ estos dos subgrupos normales mínimos de G son regulares en Ω.

c) Acción de corona torcida (Twisted wreath action)

Aquí $G = Ttwr_\phi P$ definido como sigue. Si P es un grupo de permutación primitivo en $\{1, ..., k\}$ y sea Q el estabilizador P_1, supongamos que hay un homorfismo $\phi : Q \to Aut(P)$ tal que $Im(\phi)$ contiene $Inn(T)$. Definimos $B = \{f : P \to T | f(pq) = f(p)^{\phi(p)} \quad \forall p \in P, q \in Q\}$.

Entonces B es un grupo bajo la multiplicación y $B \cong T^k$. Definimos la siguiente acción de P en B

$$p(f(x)) = f(px) \quad \forall p, x \in P.$$

Definimos $G = Ttwr_\phi P$ como el producto semidirecto de B por P con está acción y definimos la acción de G en Ω tal que $G_\alpha = P$. Entonces $n = |T|^k$ y B es el único subgrupo normal mínimo de G y actúa regularmente en Ω.

Decimos que G es de tipo acción de corona torcida si es primitivo en Ω.

Tenemos el siguiente teorema importante de clasificación de los grupos primitivos, que como dijimos, al trabajar con ellos nos da una primera clasificación de los diseños con este tipo de grupos de automorfismos.

Teorema de O'Nan-Scott 1. *(Para grupos finitios de permutación primitivo). Cualquier grupo finito de permutación primitivo es equivalente a uno de los siguientes tipos:*

i) Grupo afín

ii) Grupo casi simple

iii) Acción diagonal simple

iv) Acción producto

v) Acción de corona torcida

Demostración. Ver [3] □

CAPÍTULO 4

Imprimitividad

A partir de aquí trabajaremos con los conceptos y resultados dados hasta ahora. Dado que nos centraremos en diseños con grupos de automorfismos transitivos en banderas y primitivos, empezaremos dando un resultado importante de la imprimitividad en los grupos de automorfismos de los diseños simétricos, para después entrar de lleno a lo que se trabaja en esta tesis, que como dijimos es la primitividad.

Teorema 4. *Si D es un (v, k, λ) diseño simétrico adimitiendo un grupo de automorfismos imprimitivo y transitivo en banderas, entonces se cumple alguna de las siguientes condiciones:*

i) $(v, k, \lambda) = (\lambda^2(\lambda + 2), \lambda(\lambda + 1), \lambda)$

ii) $k \leq \lambda(\lambda - 2)$.

Demostración. Supongamos que D es un (v, k, λ) diseño simétrico adimitiendo un grupo de automorfismos imprimitivo G y transitivo en banderas. Entonces el conjunto de puntos se particiona en n bloques no triviales de imprimitividad, llamémosles Δ_j con $j = 1, ..., n$ y cada uno de tamaño c con $c, n > 1$, entonces es claro que $v = cn$.

Como G es transitivo en banderas, cada bloque del diseño y cada bloque de imprimitividad que se intersectan de manera no trivial, lo hacen en un número constante de puntos,

digamos d, esto ya que G permuta esta intersección transitivamente. Tenemos que d divide a k, es decir $k = ds$ donde s es el número de bloques de imprimitividad que intersectan a cada bloque de D, con $s > 1$.

Fijemos un punto del diseño, digamos x contemos las banderas (p, B_i) tales que p y x están en el mismo bloque de imprimitividad Δ_j y además p y x esten en el bloque B_i. Dado que Δ_j tiene tamaño c debe haber $c-1$ puntos incidentes en ese bloque de imprimitividad junto con x, además x y $p \in \Delta_j$ son incidentes en λ bloques del diseño para todo $p \in \Delta_j$, por lo que hay $\lambda(c-1)$ de dichas banderas. Contémoslas de otra manera, sabemos que hay k bloques que contienen a x, cada uno de estos bloques intersecta a Δ_j en d puntos de los cuales $d-1$ no son x por lo que hay $k(d-1)$ de esas banderas, por lo tanto tenemos $\lambda(c-1) = k(d-1)$. Entonces tenemos las siguientes ecuaciones:

1. $v = cn$
2. $k = ds$
3. $\lambda(v-1) = k(k-1)$
4. $\lambda(c-1) = k(d-1)$

Con $c, n, d, s > 1$ enteros. De la última ecuación obtenemos que

$$cn = \frac{(k(d-1)+\lambda)n}{\lambda}$$

Como $v = cn$ y además $k(k-1) = \lambda(v-1)$ entonces tenemos

$$v = cn = \frac{k(k-1)+\lambda}{\lambda}$$

restando las dos ecuaciones anteriores tendremos $\lambda(n-1) = k(k-1-n(d-1))$, sea $x = k-1-n(d-1)$ que debe ser un entero positivo, además $\lambda(n-1) = kx$ de donde $n = \frac{kx+\lambda}{\lambda}$. Luego podemos obtener

$$cn = \frac{k(k-1)+\lambda}{\lambda} = \frac{(k(d-1)+\lambda)(kx+\lambda)}{\lambda^2}$$

Resolviendo para k obtenemos

$$k = \frac{\lambda(x+d)}{\lambda - x(d-1)} \tag{4.1}$$

Donde se debe cumplir que $\lambda > x(d-1)$ el cual es un entero positivo. De esta última desigualdad obtenemos las siguientes posibilidades:

1. $x(d-1) < x+d < \lambda$
2. $x(d-1) < \lambda \leq x+d$
3. $x+d \leq x(d-1) < \lambda$

Supongamos $x(d-1) < x+d$, entonces $x = 1$ o $x = 2$ y $d \leq 3$ o $d = 2$.
Consideremos $x+d < \lambda$ de manera que $\lambda \geq 4$. Además $k < \frac{\lambda^2}{2}$ y ya que $\lambda \geq 4$ entonces $k \leq \lambda(\lambda-2)$ con lo que se cumple la condición (ii) del teorema.
Consideremos ahora $x(d-1) < \lambda \leq x+d$, asumimos primero que $x = 1$, entonces $\lambda = d$ o $\lambda = d+1$. Si $\lambda = d+1$ entonces $k = \frac{(d+1)^2}{2}$, aquí d no divide a k lo que es una contradicción. Si $\lambda = d$ entonces $k = \lambda(\lambda+1)$ y como $k(k-1) = \lambda(v-1)$ entonces $v = \lambda^2(\lambda+2)$ por lo que se cumple la condición (i) del teorema.

Ahora, supongamos $x = 2$.
Entonces si $d = 2$ tendremos $2 < \lambda \leq 4$ y $k = \frac{4\lambda}{\lambda-2}$. Si $\lambda = 4$ entonces $k = 8$ y $v = 15$ que justamente satisface la condición (ii) del teorema y estos parámetros corresponden al complemento del diseño de Hadamard $(15, 7, 3)$. Si $\lambda = 3$ entonces $k = 12$ y $v = 45$, y se cumple de nuevo la condición (i) del teorema.
Si $d = 3$ entonces $\lambda = 5$ de manera que $k = 25$ entonces es claro que d no divide a k lo que es una contradicción.

Ahora supongamos que $x \geq 3$ y $d = 2$. Entonces $\lambda = x+1$ o $\lambda = x+2$. Si $\lambda = x+2$ entonces $k = \frac{\lambda^2}{2}$ y $v = \frac{\lambda^3}{4} - \lambda^2 + 1$ de manera que se satisface la condición (ii) del teorema. Si $\lambda = x+1$ entonces $k = \lambda(\lambda+1)$ y $v = \lambda^2(\lambda+2)$ y ahora se cumple la condición (i) del teorema.

Supongamos ahora que $x+d = x(d-1)$. Entonces $d \neq 2$ y $x \neq 1$ y como $x+d = xd-x$ se tiene $2x = d(x-1)$ y $d = x(d-2)$ y entonces $x = 2$ y $d = 4$, o $x = 3 = d$. En cualquier caso tenemos $k = \frac{\lambda(x+d)}{\lambda - x(d-1)}$ lo que obliga a que $k = \frac{6\lambda}{\lambda-6}$. Si $\lambda \geq 12$ entonces $v \leq k \leq \lambda$ lo que es una contradicción. Si $\lambda = 11$ entonces $k = \frac{66}{5}$ lo que es una contradicción pues k debe ser

entero positivo.Si $\lambda = 10$ obtenemos la terna $(22, 15, 10)$ pero $v = 22$ es par y $k - \lambda = 5$ no es un cuadrado contradiciendo el Teorema de Bruck- Ryser-Chowla.

Si $7 \leq \lambda \leq 9$ obtenemos los siguientes parámetros $(247, 42, 7), (70, 24, 8)$ y $(35, 18, 9)$. Los últimos dos cumplen la condición (ii) del teorema. Supongamos que existe un $(247, 42, 7)$-diseño simétrico con un grupo de automorfismos transitivo en banderas e imprimitivo. Entonces $v = cn = 13 \times 19$ además sabemos que $d = 3$ o $d = 4$, pero $k = 2 \times 3 \times 7$ así que $d = 3 = x$ y entonces cada bloque intersecta 14 bloques de imprimitividad en 3 puntos exactamente. Como $x = k - 1 - n(d - 1)$ entonces $n = 19$. Hay ocho grupos transitivos en 19 puntos [7]. Cinco de estos tienen orden menor a $247 = v$ y entonces se descartan. De los tres que restan uno tiene orden 342 el cual no es divisible por 247 y también se descarta. Los dos que restan son A_{19} y S_{19}, estos grupos producen al menos un bloque por 14 bloques y esto obliga a más de v bloques en conjunto.
Por último supongamos $x + d < x(d - 1) < \lambda$, entonces $k \leq \lambda(\lambda - 2)$ y esto concluye la prueba. □

Y tenemos el siguiente resultado que nos dice cuáles son los únicos posibles diseños simétricos con grupo de automorfismos transitivo en banderas e imprimitvo y siempre que $\lambda < 20$, con lo que el resto de los diseños con $\lambda < 20$ con grupo de automorfismo transitivo en banderas, si es que existen, deberán tener un grupo de automorfismo primitivo y entrarían en lo que estudiaremos más adelante.

Corolario 1. *Si G es un grupo de automorfismos transitivo en banderas de un (v, k, λ)- diseño simétrico D con $\lambda \leq 20$ entonces G es primitivo o D tiene los parámetros* $(16, 6, 2), (45, 12, 3)$,
$(15, 8, 4), (96, 20, 4), (175, 30, 5), (16, 10, 6), (36, 15, 6), (288, 42, 6)$,
$(27, 14, 7), (247, 42, 7), (441, 56, 7), (640, 72, 8), (70, 24, 8), (125, 32, 8), (891, 90, 9)$,
$(35, 18, 9), (435, 63, 9), (1200, 110, 10), (39, 20, 10), (120, 35, 10), (1573, 132, 11)$,
$(2016, 156, 12), (64, 28, 12), (36, 21, 12), (189, 48, 12), (21, 16, 12), (427, 72, 12)$,
$(2535, 182, 13), (825, 104, 13), (1045, 117, 13), (51, 26, 13), (205, 52, 13), (3136, 210, 14)$,
$(280, 63, 14), (221, 56, 14), (3825, 240, 15), (105, 40, 15), (133, 45, 15), (1491, 150, 15)$,
$(85, 36, 15), (323, 70, 15), (4608, 272, 16), (396, 80, 16), (63, 32, 16), (1017, 128, 16)$,
$(5491, 306, 17), (6480, 342, 18), (540, 99, 18), (160, 54, 18), (40, 27, 18), (111, 45, 18)$,

$(540, 99, 18), (285, 72, 18), (1450, 162, 18), (7581, 380, 19), (2725, 228, 19), (75, 38, 19),$
$(679, 114, 19), (8800, 420, 20), (715, 120, 20), (64, 36, 20), (100, 45, 20), (1991, 200, 20)$.

Demostración. Por el Teorema 4 si $\lambda = 2$ o 3 entonces tendríamos la conclusión (i) del teorema, lo que fuerza a $v = 16$ y $k = 6$ en el primer caso y $v = 45$ y $k = 12$ en el segundo.

Si $\lambda = 4$ entonces se tiene la conclusión (i), haciendo que $v = 96$ y $k = 20$ o se tiene la conclusión (ii) haciendo que $k \leq 8$ pero para que el diseño sea no trivial se debe tener $k > 5$. Como $k(k-1) = \lambda(v-1)$ por lo que $k(k-1)$ debe ser divisible por 4 y entonces k no puede ser ni 6 ni 7. Entonces $k = 8$ y con ello $v = 15$.

De la ecuación (4.1) que surge en la demostración del teorema anterior tenemos que se debe cumplir que $\lambda > x(d-1) > 0$ y las ecuaciones

1. $v = cn$
2. $k = ds$
3. $\lambda(v-1) = k(k-1)$
4. $\lambda(c-1) = k(d-1)$

Analicemos cada uno de los casos para $\lambda = 5, 6, 7$

1. $\lambda = 5$: Para este valor de λ tenemos que $5 > x(d-1) > 0$ lo que nos arroja las siguientes posibilidades:

   a) $x = 1$ y $d = 2, 3, 4, 5$

   b) $x = 2$ y $d = 2, 3$

   c) $x = 3$ y $d = 2$

   d) $x = 4$ y $d = 2$

   Cuando $x = 2$ el único valor admisible para k es $k = 25$, esto cuando $d = 3$ pero aquí d no divide a k por lo que este caso queda totalmente descartado.
   En el caso en que $x = 1$ se obtiene un único valor para k que es $k = 30$ cuando $d = 5$. Igualemente para el tercer caso obtenemos que $k = 30$. Por lo que si $k = 30$ sustituyendo

en la ecuación $k(k-1) = \lambda(v-1)$ obtenemos $870 = 5(v-1)$ y esto nos da que $v = 175$ y la única terna posible es, para este caso, $(175, 30, 5)$

2. $\lambda = 6$: En este caso tenemos que $6 > x(d-1) > 0$ lo que nos arroja las siguientes posibilidades:

   a) $x = 1$ y $d = 2, 3, 4, 5, 6$

   b) $x = 2$ y $d = 2, 3$

   c) $x = 3$ y $d = 2$

   d) $x = 4$ y $d = 2$

   e) $x = 5$ y $d = 2$

   En el primer caso el único entero k más grande que λ tal que d divide a k es 42 con $d = 6$ y le terna posible es $(288, 42, 6)$.
   En el segundo caso obtenemos que $k = 15$ lo cual nos da los parámetros $(36, 15, 6)$.
   Cuando $x = 3$ obtenemos que k debe ser 10 y esto nos da la terna $(16, 10, 6)$.
   Mientras que si $x = 4$ tendremos el único valor posible $k = 18$ lo que implica que $v = 52$ pero como v es par , entonces $k - \lambda$ debería ser un cuadrado lo cual no sucede pues $k - \lambda = 12$, por lo que este caso queda descartado.
   Por último en el caso en que $x = 5$ obtenemos al igual que en el primer caso que $k = 42$, y en este caso la terna posible sería $(288, 42, 6)$.

3. $\lambda = 7$: En este caso tenemos que $7 > x(d-1) > 0$ con lo que tenemos que las posibles combinaciones para x y d son:

   a) $x = 1$ y $d = 2, 3, 4, 5, 6, 7$

   b) $x = 2$ y $d = 2, 3, 4$

   c) $x = 3$ y $d = 2, 3$

   d) $x = 4$ y $d = 2$

   e) $x = 5$ y $d = 2$

   f) $x = 6$ y $d = 2$

En el primer caso el único entero k más grande que λ tal que es divisible por d es $k = 56$ con $d = 7$ y obtenemos la terna $(441, 56, 7)$.

En el segundo caso obtenemos que no existe ningún valor para k divisible por d.

Cuando $x = 3$ obtenemos que k es el único valor posible para k tal que es divisible por d es $k = 42$ con $d = 3$ y esto nos da la terna $(247, 42, 7)$.

En el caso en que $x = 4$ y $d = 2$ tendremos elúnico valor posible $k = 14$ lo que implica que $v = 27$ y obtenemos los parámetros $(27, 14, 7)$.

Si $x = 5$ no hay valores enteros posibles para k por lo que este caso está descartado, mientras que para el último caso obtenemos la única terna posible $(441, 56, 7)$.

4. $\lambda = 8$: En este caso tenemos que $8 > x(d-1) > 0$ con lo que tenemos que las posibles combinaciones para x y d son:

   a) $x = 1$ y $d = 2, 3, 4, 5, 6, 7, 8$

   b) $x = 2$ y $d = 2, 3, 4$

   c) $x = 3$ y $d = 2, 3$

   d) $x = 4, 5, 6, 7$ y $d = 2$

   En el primer caso el único entero k más grande que λ tal que es divisible por d es $k = 72$ con $d = 8$ y obtenemos la terna $(640, 72, 8)$.

   En el segundo caso obtenemos que el único valor para k divisible por d es $k = 24$ con $d = 4$ y en este caso obtenemos la terna $(70, 24, 8)$.

   Cuando $x = 3$ obtenemos que el único valor posible para k tal que es divisible por d es $k = 24$ con $d = 3$ y esto nos da la misma terna que en el caso anterior.

   En el caso en que $x = 4$ y $d = 2$ tendremos el único valor posible $k = 12$ pero entonces $k(k-1)$ no es divisible por $\lambda = 8$.

   Si $x = 5$ no hay valores enteros posibles para k por lo que este caso está descartado.

   Mientras que para el caso $x = 6$ con el único posible caso $d = 2$ obtenemos la única terna posible $(125, 32, 8)$.

   Y en el último caso $x = 7$ $d = 2$ obtenemos la terna $(640, 72, 8)$.

5. $\lambda = 9$: En este caso tenemos que $9 > x(d-1) > 0$ con lo que tenemos que las posibles combinaciones para x y d son:

a) $x = 1$ y $d = 2, 3, 4, 5, 6, 7, 8, 9$

b) $x = 2$ y $d = 2, 3, 4, 5$

c) $x = 3$ y $d = 2, 3$

d) $x = 4$ y $d = 2, 3$

e) $x = 5, 6, 7, 8$ y $d = 2$

En el primer caso el único entero k más grande que λ tal que es divisible por d es $k = 90$ con $d = 9$ y obtenemos la terna $(891, 90, 9)$.

En el segundo caso $x = 2$ no obtenemos ningún valor entero posible para k tal que d divida a k.

Cuando $x = 3$ obtenemos que el único valor posible para k tal que es divisible por d es $k = 18$ con $d = 3$ y esto nos da la terna $(35, 18, 9)$.

En el caso en que $x = 4$ y $d = 3$ tendremos el único valor posible $k = 63$ y los parámetros posibles son $(435, 63, 9)$.

Si $x = 5$ no hay valores enteros posibles para k por lo que este caso está descartado.

En el caso $x = 6$ con el único posible caso $d = 2$ obtenemos $k = 24$ pero entonces $k(k-1)$ no es divisible por 9, por lo que se descarta tal caso.

En el caso $x = 7$ $d = 2$ no obtenemos valor entero de k.

Y en el último caso $x = 8$ $d = 2$ obtenemos que $k = 90$ y obtenemos la misma terna que para $x = 1$.

6. $\lambda = 10$: Aquí se cumple $10 > x(d-1) > 0$ con lo que tenemos los siguientes casos:

   a) $x = 1$ y $d = 2, 3, 4, 5, 6, 7, 8, 9, 10$

   b) $x = 2$ y $d = 2, 3, 4, 5$

   c) $x = 3$ y $d = 2, 3$

   d) $x = 4$ y $d = 2, 3$

   e) $x = 5, 6, 7, 8, 9$ y $d = 2$

   En el primer caso el único entero k más grande que λ tal que es divisible por d es $k = 110$ con $d = 10$ y obtenemos la terna $(1200, 110, 10)$.

   En el segundo caso $x = 2$ obtenemos que el único valor posible para k que cumple las

hipotesis es $k = 35$ con $d = 5$ y con ello obtenemos la posible terna $(120, 35, 10)$.

Cuando $x = 3$ obtenemos que el único valor posible para k tal que es divisible por d es $k = 15$ con $d = 3$ sin embargo al hacer el cálculo de v obtenemos $v = 22$ que es par, con lo que $k - \lambda$ debería ser un cuadrado sin embargo $k - \lambda = 5$ por lo que este caso queda descartado.

En el caso en que $x = 4$ y $d = 3$ tendremos el único valor posible $k = 35$ y con ello la misma terna que en el caso $x = 2$.

Si $x = 5$ obtenemos que el único valor posible para k divisible por d es $k = 14$ son embargo en este caso $k(k-1) = 14(13) = 182$ que no es divisble por $\lambda = 10$ por lo que descartamos este caso.

En el caso $x = 6$ con el único posible caso $d = 2$ obtenemos $k = 20$ y obtenemos la terna $(39, 20, 10)$.

En el caso $x = 7$ $d = 2$ obtenemos que $k = 30$ y con ello $v = 88$ que es par, pero $k - \lambda = 20$ no es un cuadrado.

En el caso $x = 8$ $d = 2$ obtenemos que $k = 50$ y obtenemos $v = 246$ que es par, pero $k - \lambda = 40$ que no es cuadrado, por lo que al igual que en el caso anterior se descarta.

Por último cuando $x = 9$ obtenemos la terna $(1200, 110, 10)$.

7. $\lambda = 11$: En este caso tenemos que $11 > x(d-1) > 0$ con lo que tenemos que las posibles combinaciones para x y d son:

   a) $x = 1$ y $d = 2, 3, 4, 5, 6, 7, 8, 9, 10, 11$

   b) $x = 2$ y $d = 2, 3, 4, 5, 6$

   c) $x = 3$ y $d = 2, 3, 4$

   d) $x = 4$ y $d = 2, 3$

   e) $x = 5$ y $d = 2, 3$

   f) $x = 6, 7, 8, 9, 10$ y $d = 2$

   En el primer caso el único entero k más grande que λ tal que es divisible por d es $k = 132$ con $d = 11$ y obtenemos la terna $(1573, 132, 11)$.

   En el segundo caso $x = 2$ obtenemos que $k = 88$ con $d = 6$ por lo que se descarta pues k debe ser divisible por d.

Cuando $x = 3$, $x = 4$, $x = 6$, $x = 7$, $x = 8$, $x = 9$ no obtenemos ningún valor entero para k.

Si $x = 5$ obtenemos que $k = 88$ cuando $d = 3$ por lo que queda descartado.

En el caso $x = 6$ con el único posible caso $d = 2$ obtenemos $k = 24$ pero entonces $k(k-1)$ no es divisible por 9, por lo que se descarta tal caso.

Y en el último caso $x = 10$ $d = 2$ obtenemos que $k = 132$ y obtenemos la misma terna que para $x = 1$.

8. $\lambda = 12$: Aquí se cumple $12 > x(d-1) > 0$ con lo que tenemos los siguientes casos:

   a) $x = 1$ y $d = 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12$

   b) $x = 2$ y $d = 2, 3, 4, 5$

   c) $x = 3$ y $d = 2, 3, 4$

   d) $x = 4$ y $d = 2, 3$

   e) $x = 5$ y $d = 2, 3$

   f) $x = 6, 7, 8, 9, 10, 11$ y $d = 2$

   En el primer caso el único entero k más grande que λ tal que es divisible por d es $k = 156$ con $d = 12$ y obtenemos la terna $(2016, 156, 12)$.

   En el segundo caso $x = 2$ obtenemos un valor para k divisible por d, $k = 48$ con $d = 6$ lo que nos da la terna $(189, 48, 12)$.

   Cuando $x = 3$ obtenemos que el único valor posible para $k > \lambda$ tal que es divisible por d es $k = 28$ con $d = 4$ con lo que obtenemos la terna $(64, 28, 12)$.

   En el caso en que $x = 4$ y $d = 3$ tendremos el único valor posible $k = 21$ en este caso obtenemos la terna $(36, 21, 12)$.

   Si $x = 5$ obtenemos que el único valor posible para k divisible por d es $k = 48$ con $d = 3$ y obtenemos la terna $(189, 48, 12)$.

   En el caso $x = 6$ con el único posible caso $d = 2$ obtenemos $k = 16$ y obtenemos la terna $(21, 16, 12)$.

   En el caso $x = 7$ $d = 2$ no obtenemos ningún valor entero de k.

   En el caso $x = 8$ $d = 2$ obtenemos que $k = 30$ pero $k(k-1) = 870$ no es divisible por 12, por lo que se descarta.

Cuando $x = 9$ obtenemos que $k = 44$ pero $k(k-1) = 1892$ no es divisible por 12, por lo que se descarta.

Si $x = 10$ y $d = 2$ tenemos que $k = 72$ y obtenemos la terna $(427, 72, 12)$.

Por último cuando $x = 11$ otenemos la misma terna que en el caso $x = 1$.

9. $\lambda = 13$: Aquí se cumple $13 > x(d-1) > 0$ con lo que tenemos los siguientes casos:

   a) $x = 1$ y $2 \leq d \leq 13$

   b) $x = 2$ y $d = 2, 3, 4, 5, 6, 7$

   c) $x = 3$ y $d = 2, 3, 4, 5$

   d) $x = 4$ y $d = 2, 3, 4$

   e) $x = 5$ y $d = 2, 3$

   f) $x = 6$ y $d = 2, 3$

   g) $x = 7, 8, 9, 10, 11, 12$ y $d = 2$

   En el primer caso el único entero k más grande que λ tal que es divisible por d es $k = 182$ con $d = 13$ y obtenemos la terna $(2535, 182, 13)$.

   En el segundo caso $x = 2$ y $x = 3$ no obtenemos ningún valor para k divisible por d.

   En el caso en que $x = 4$ y $d = 4$ tendremos el único valor posible $k = 104$ en este caso obtenemos la terna $(825, 104, 13)$.

   Si $x = 5$ no obtenemos ningún valor entero de k.

   En el caso $x = 6$ $d = 3$ obtenemos $k = 117$ y obtenemos la terna $(1045, 117, 13)$.

   En el caso $x = 7$ $d = 2$ no obtenemos ningún valor entero de k.

   En el caso $x = 8$ $d = 2$ obtenemos que $k = 26$ con lo que obtenemos la terna $(51, 26, 13)$.

   Cuando $x = 9$ no obtenemos ningún valor entero de k.

   Si $x = 10$ y $d = 2$ tenemos que $k = 52$ y obtenemos la terna $(205, 52, 13)$.

   Cuando $x = 11$ tampoco se obtienen valores enteros de k.

   Por último cuando $x = 12$ se obtiene la misma terna que para $x = 1$.

10. $\lambda = 14$: Aquí se cumple $14 > x(d-1) > 0$ con lo que tenemos los siguientes casos:

    a) $x = 1$ y $2 \leq d \leq 14$

    b) $x = 2$ y $d = 2, 3, 4, 5, 6, 7$

c) $x = 3$ y $d = 2, 3, 4, 5$

d) $x = 4$ y $d = 2, 3, 4$

e) $x = 5$ y $d = 2, 3$

f) $x = 6$ y $d = 2, 3$

g) $x = 7, 8, 9, 10, 11, 12$ y $d = 2$

En el primer caso el único entero k más grande que λ tal que es divisible por d es $k = 210$ con $d = 14$ y obtenemos la terna $(3136, 210, 14)$.

En el segundo caso $x = 2$ $d = 7$ obtenemos que $k = 63$ con lo que se obtiene la terna $(280, 63, 14)$.

Mientras que si $x = 3$ no obtenemos ningún valor para k divisible por d.

En el caso en que $x = 4$ y $d = 4$ tendremos el único valor posible $k = 56$ en este caso obtenemos la terna $(221, 56, 14)$.

Si $x = 5$ no obtenemos ningún valor entero de k divisible por d.

En el caso $x = 6$ $d = 3$ obtenemos $k = 63$ y obtenemos la misma terna que en el caso $x = 2$.

En el caso $x = 7$ $d = 2$ obtenemos que el único valor de k es $k = 18$ pero $k(k-1) = 306$ que no es divisible por 14 por lo que se descarta dicho caso.

En los casos $x = 8$ $x = 9$ no se obtiene valor entero de k.

Si $x = 10$ y $d = 2$ tenemos que $k = 42$ y obtenemos $v = 124$ que es par pero $k - \lambda = 28$ que no es cuadrado por lo que se descarta el caso.

Cuando $x = 11$ y $x = 12$ no se obtienen valores enteros de k.

Por último cuando $x = 13$ se obtiene la misma terna que para $x = 1$.

11. $\lambda = 15$: Aquí se cumple $15 > x(d-1) > 0$ con lo que tenemos los siguientes casos:

a) $x = 1$ y $2 \leq d \leq 15$

b) $x = 2$ y $d = 2, 3, 4, 5, 6, 7, 8$

c) $x = 3$ y $d = 2, 3, 4, 5$

d) $x = 4$ y $d = 2, 3, 4$

e) $x = 5$ y $d = 2, 3$

f) $x = 6$ y $d = 2, 3$

g) $x = 7$ y $d = 2, 3$

h) $x = 8, 9, 10, 11, 12, 13, 14$ y $d = 2$

En el primer caso el único entero k más grande que λ tal que es divisible por d es $k = 240$ con $d = 15$ y obtenemos la terna $(3825, 240, 15)$.

En el segundo caso $x = 2$ $d = 6$ obtenemos que $k = 24$ con lo que se $k(k-1) = 552$ que no es divisible por 15 por lo que se descarta y es el único valor de k divisible por d.

Mientras que si $x = 3$ se obtiene que $k = 40$ con $d = 5$ y entonces se tiene la terna $(105, 40, 15)$.

En el caso en que $x = 4$ y $d = 4$ tendremos el único valor posible $k = 40$ y se tiene la misma terna que en el caso anterior.

Si $x = 5$ $d = 3$ se obtiene $k = 24$ y con ello la misma terna que en el caso $x = 1$.

En el caso $x = 6$ $d = 3$ obtenemos $k = 45$ y obtenemos la terna $(133, 45, 15)$.

En el caso $x = 7$ $d = 3$ obtenemos que el único valor de k es $k = 150$ y obtenemos la terna $(1491, 150, 15)$.

En los casos $x = 8$ $x = 9$ no se obtiene valor entero de k.

Si $x = 10$ y $d = 2$ tenemos que $k = 36$ y obtenemos la terna $(85, 36, 15)$.

Cuando $x = 11$ no se obtienen valores enteros de k.

En el caso en que $x = 12$ el único valor de k es $k = 70$ y con esto se obtiene la terna $(323, 70, 15)$.

Cuando $x = 13$ no hay valor entero para k.

Por último cuando $x = 14$ se obtiene la misma terna que para $x = 1$.

12. $\lambda = 16$: Aquí se cumple $16 > x(d-1) > 0$ con lo que tenemos los siguientes casos:

a) $x = 1$ y $2 \leq d \leq 16$

b) $x = 2$ y $d = 2, 3, 4, 5, 6, 7, 8$

c) $x = 3$ y $d = 2, 3, 4, 5, 6$

d) $x = 4, 5$ y $d = 2, 3, 4$

e) $x = 6, 7$ y $d = 2, 3$

f) $x = 8, 9, 10, 11, 12, 13, 14, 15$ y $d = 2$

En el primer caso el único entero k más grande que λ tal que es divisible por d es $k = 272$ con $d = 16$ y obtenemos la terna $(4608, 272, 16)$.

En el segundo caso $x = 2$ $d = 8$ obtenemos que $k = 80$ con lo que se tiene la terna $(396, 80, 16)$.

Mientras que si $x = 3$ se obtiene que $k = 144$ con $d = 6$ y entonces se tiene que $v = 1288$ que es par, pero $k - \lambda = 128$ que no es cuadrado por lo que se descarta.

En el caso en que $x = 4$ y $d = 4$ tendremos el único valor posible $k = 32$ y se tiene la terna $(63, 32, 16)$.

Si $x = 5$ $d = 4$ se obtiene $k = 144$ que se descarta por lo dicho en el caso $x = 3$.

En el caso $x = 6$ $d = 3$ obtenemos $k = 36$ pero $k(k - 1) = 1260$ que no es divisile por 16.

En el caso $x = 7$ no se obtienen valores mayores que λ divisibles por d.

En el caso $x = 8$ se tiene que $k = 20$ pero $k(k - 1) = 380$ que no es divisible por 16 .

Cuando $x = 9$ no se obtiene ningún valor entero para k.

Si $x = 10$ y $d = 2$ tenemos que $k = 32$ y obtenemos la misma terna que en el caso $x = 4$.

Cuando $x = 11$ no se obtienen valores enteros de k.

En el caso en que $x = 12$ el único valor de k es $k = 56$ pero $k(k - 1) = 3080$ que no es divisile por 16.

Cuando $x = 13$ se obtiene el único valor para k es $k = 80$ y con ello la misma terna que en el caso $x = 2$.

Mientras que en el caso $x = 14$ se obtiene que $k = 128$ y con ello la terna $(1017, 128, 16)$.

Y en el último caso se obtiene la misma terna que en el primer caso.

13. $\lambda = 17$: Aquí se cumple $17 > x(d - 1) > 0$ con lo que tenemos los siguientes casos:

    a) $x = 1$ y $2 \leq d \leq 17$

    b) $x = 2$ y $d = 2, 3, 4, 5, 6, 7, 8$

    c) $x = 3$ y $d = 2, 3, 4, 5, 6$

    d) $x = 4$ y $d = 2, 3, 4, 5$

e) $x = 5$ y $d = 2, 3, 4$

f) $x = 6, 7, 8$ y $d = 2, 3$

g) $x = 9, 10, 11, 12, 13, 14, 15, 16$ y $d = 2$

En el primer caso el único entero k más grande que λ tal que es divisible por d es $k = 306$ con $d = 17$ y obtenemos la terna $(5491, 306, 17)$.

En los casos $x = 2, 4, 8$ no se tienen valores para k divisibles por d.

Mientras que si $x = 3, 5, 6, 7, 9, 10, 11, 12, 13, 14, 15$ no se obtiene ningún entero k.

Y en el último caso se obtiene la misma terna que en el primer caso.

14. $\lambda = 18$: Aquí se cumple $18 > x(d-1) > 0$ con lo que tenemos los siguientes casos:

a) $x = 1$ y $2 \leq d \leq 18$

b) $x = 2$ y $d = 2, 3, 4, 5, 6, 7, 8, 9$

c) $x = 3$ y $d = 2, 3, 4, 5, 6$

d) $x = 4$ y $d = 2, 3, 4, 5$

e) $x = 5$ y $d = 2, 3, 4$

f) $x = 6, 7, 8$ y $d = 2, 3$

g) $x = 9, 10, 11, 12, 13, 14, 15, 16, 17$ y $d = 2$

En el primer caso el único entero k más grande que λ tal que es divisible por d es $k = 342$ con $d = 18$ y obtenemos la terna $(6480, 342, 18)$.

En el segundo caso $x = 2$ $d = 9$ obtenemos que $k = 99$ con lo que se tiene la terna $(540, 99, 18)$.

Mientras que si $x = 3$ se obtiene que $k = 54$ con $d = 6$ y entonces obtenemos la terna $(160, 54, 18)$.

En el caso en que $x = 4$ y $d = 4$ tendremos el único valor posible $k = 24$ pero $k(k-1) = 552$ que no es divisible por 18 por lo que se descarta el caso.

Si $x = 5$ no se obtiene ningún valor entero mayor que λ para k divisible por d.

En el caso $x = 6$ $d = 3$ obtenemos $k = 27$ con ello tenemos la terna $(40, 27, 18)$.

En el caso $x = 7$ $d = 3$ tenemos la terna $(111, 45, 18)$.

En el caso $x = 8$ $d = 3$ obtenemos la terna $(540, 99, 18)$.

Cuando $x = 9$ tenemos que $k = 22$ pero $k(k-1) = 462$ que no es divisible por 18 con lo que se descarta el caso.

Si $x = 10$ y $d = 2$ tenemos que $k = 27$ y obtenemos la misma terna que en el caso $x = 6$.

Cuando $x = 11$ no se obtienen valores enteros de k.

En el caso en que $x = 12$ el único valor de k es $k = 42$ pero $k(k-1) = 1722$ que no es divisile por 18.

Cuando $x = 13$ se obtiene el único valor para k es $k = 54$ y con ello la misma terna que en el caso $x = 3$.

Mientras que en el caso $x = 14$ se obtiene que $k = 72$ y con ello la terna $(285, 72, 18)$.

Cuando se tiene que $x = 15$ obtenemos que $k = 102$ pero $k(k-1) = 10302$ que no es divisible por 18.

Mientras que si $x = 16$ obtenemos que $k = 162$ y con ello la terna $(1450, 162, 18)$.

Y en el último caso se obtiene la misma terna que en el primer caso.

15. $\lambda = 19$: Aquí se cumple $19 > x(d-1) > 0$ con lo que tenemos los siguientes casos:

    a) $x = 1$ y $2 \leq d \leq 19$

    b) $x = 2$ y $d = 2, 3, 4, 5, 6, 7, 8, 9, 10$

    c) $x = 3$ y $d = 2, 3, 4, 5, 6, 7$

    d) $x = 4$ y $d = 2, 3, 4, 5$

    e) $x = 5, 6$ y $d = 2, 3, 4$

    f) $x = 7, 8, 9$ y $d = 2, 3$

    g) $x = 10, 11, 12, 13, 14, 15, 16, 17, 18$ y $d = 2$

    En el primer caso el único entero k más grande que λ tal que es divisible por d es $k = 380$ con $d = 19$ y obtenemos la terna $(7581, 380, 19)$.

    En el segundo caso $x = 2, 5, 8, 10, 11, 13, 14, 15, 17$ no se obtienen valores enteros para k.

    Mientras que si $x = 3, 4, 6, 7$ no se obtienen valores para k divisibles por d.

    Cuando $x = 9$ $d = 3$ tenemos que $k = 228$ obtenemos la terna $(2725, 228, 19)$.

    En el caso en que $x = 12$ el único valor de k es $k = 38$ y obtenemos la terna $(75, 38, 19)$.

Mientras que si $x = 16$ obtenemos que $k = 114$ y con ello la terna $(679, 114, 19)$.

Y en el último caso se obtiene la misma terna que en el primer caso.

16. $\lambda = 20$: Aquí se cumple $20 > x(d-1) > 0$ con lo que tenemos los siguientes casos:

    a) $x = 1$ y $2 \leq d \leq 20$

    b) $x = 2$ y $d = 2, 3, 4, 5, 6, 7, 8, 9, 10$

    c) $x = 3$ y $d = 2, 3, 4, 5, 6, 7$

    d) $x = 4$ y $d = 2, 3, 4, 5$

    e) $x = 5, 6$ y $d = 2, 3, 4$

    f) $x = 7, 8, 9$ y $d = 2, 3$

    g) $x = 10, 11, 12, 13, 14, 15, 16, 17, 18, 19$ y $d = 2$

    En el primer caso el único entero k más grande que λ tal que es divisible por d es $k = 420$ con $d = 20$ y obtenemos la terna $(8800, 420, 20)$.

    En el segundo caso $x = 2$ $d = 10$ obtenemos que $k = 120$ con lo que se tiene la terna $(715, 120, 20)$.

    Mientras que si $x = 3$ $d = 6$ se obtiene que $k = 36$ entonces obtenemos la terna $(64, 36, 20)$.

    En el caso en que $x = 4$ y $d = 5$ tendremos el único valor posible $k = 45$ obtenemos la terna $(100, 45, 20)$.

    Si $x = 5$ $d = 4$ tenemos que $k = 36$ y se tiene la misma terna que cuando $x = 3$.

    En el caso $x = 6$ $d = 4$ obtenemos $k = 100$ con ello tenemos $v = 496$ que es par, pero $k - \lambda = 80$ que no es cuadrado.

    En los casos $x = 7, 11, 13, 14, 17$ no se tienen valores enteros de k.

    En el caso $x = 8$ no se tienen valores de k divisibles por d.

    Cuando $x = 9$ tenemos que $k = 120$ y se tendrá la misma terna que en $x = 2$.

    Si $x = 10$ y $d = 2$ tenemos que $k = 24$ pero $k(k-1) = 552$ que no es divisible por 20.

    En el caso en que $x = 12$ el único valor de k es $k = 35$ pero $k(k-1) = 1190$ que no es divisile por 20.

    Cuando se tiene que $x = 15$ obtenemos que $k = 68$ pero $k(k-1) = 4556$ que no es divisible por 20.

Mientras que si $x = 16$ obtenemos que $k = 90$ pero $k(k-1) = 8010$ que no es divisible por 20.

En el caso $x = 18$ obtenemos que $k = 200$ con lo que obtenemos la terna $(1991, 200, 20)$.

Y en el último caso se obtiene la misma terna que en el primer caso.

□

Observación: El hecho de que se haga mención en el anterior corolario de las ternas no implica la existencia de diseños con esos parámetros.

Demos algunos ejemplos de diseños simétricos que admiten grupo de automorfismos imprimitivo y transitivo en banderas. Como mencionamos al hablar de los biplanos que admiten grupos de automorfismos transitivos en banderas para $k = 6$ existen dos $(16, 6, 2)$ biplanos que admiten un grupo así. De hecho estos son $\mathbb{Z}_2^4 S_6$ y $(\mathbb{Z}_2 \times \mathbb{Z}_8)(S_2.2)$, ambos son grupos afines contenidos en $AGL_4(2)$ donde S_6 y $S_4.2$ son los estabilizadores en $GL_4(2)$. El grupo S_4 está contenido en ambos estabilizadores y es transitivo en las seis clases laterales de V_4 así que es transitivo en los seis bloques que contienen al punto fijo. Por lo tanto los subgrupos $\mathbb{Z}_2^4 S_4$ y $(\mathbb{Z}_2 \times \mathbb{Z}_8)(S_2.2)$ son aún transitivos en banderas en sus respectivos biplanos. Sin embargo S_4 fija un espacio de dimensión 2 en $\mathbb{Z}_2^4$ así que no es irreducible y por lo tanto estos subgrupos son imprimitivos.

Existe un ejemplo de un $(15, 8, 4)$ diseño simétrico con un grupo de automorfismos transitivo en banderas. Sea $P = \{1, ..., 15\}$ el conjunto de puntos y $B_1 = \{1, 2, 3, 4, 8, 11, 12, 14\}$ un bloque. Construyamos el conjunto de bloques como $B = \{B_1 + i : i \in \mathbb{Z}_1 5\}$, esta construcción nos da un $(15, 8, 4)$ diseño simétrico.
Las permutaciones $\alpha = (2, 5)(4, 14)(6, 11)(7, 15)(8, 13)(10, 20)$,
$\beta = (2, 8)(3, 7)(5, 10)(6, 11)(9, 14)(12, 13)$ y
$\gamma = (2, 5)(3, 9)(4, 13)(7, 10)(8, 14)(12, 15)$ fijan al punto 1.
El grupo H generado por α, β y γ es transitivo en los ocho bloques incidentes con 1 y preservan la partición de P en los conjuntos $\{1, 6, 11\}, \{2, 7, 12\}$,
$\{3, 8, 13\}, \{4, 9, 14\}$ y $\{5, 10, 15\}$. Este grupo tiene orden 24 y es isomorfo a S_4. [2].
El grupo $\mathbb{Z}_{15}$ de traslaciones actúa regularmente en los puntos y en los bloques y tengamos

en cuenta que preserva la misma partición de los puntos, aquí el grupo $G = \mathbb{Z}_{15}H$ es cual es isomorfo a $3S_5$ [2], actúa de manera imprimitiva y es transitivo en banderas en el diseño.

También hay un ejemplo de un $(96, 20, 4)$-diseño imprimitivo y transitivo en banderas, este es una estructura de incidencia (P, L, I) con parámetros (s, t) $s, t \geq 1$ conocido como cuadrángulo finito generalizado, cuyo conjunto de puntos es P y conjunto de líneas es L y una relación de incidencia I, tal que cada punto es incidente en $t + 1$ líneas y dos distintos puntos son incidentes con a lo más una línea, cada línea es incidente con $1 + s$ puntos y dos distintas líneas son incidentes en a lo más un punto, y si x es un punto y j una línea no incidente con x entonces hay un único par $(y, m) \in P \times L$ tal que $xImIyIj$, es decir, para cada punto x y una línea j que no son incidentes existe una única línea m y un único punto y tal que x está en m y y está en m y j.
Tomamos el cuadrángulo generalizado con parámetros $(5, 3)$ y contruyamos el diseño como sigue, los puntos son los puntos del cuadrángulo y los bloques son los puntos diferentes a x que son colineales con x para todo punto x. Existen 96 puntos y 96 bloques y este es un $(96, 20, 4)$-diseño simétrico. El grupo de automorfismos es $\mathbb{Z}_2^4 3S_6$ el cual es imprimitivo y el estabilizador es A_6 el cual actúa de manera transitiva en los 20 puntos y es transitivo en los 20 bloques que contienen al punto fijo. Por lo tanto el grupo de automorfismos es transitivo en banderas.

CAPÍTULO 5

Primitividad

Como mencionamos, trabajaremos con diseños cuyo grupo de automorfismos es transitivo en banderas y primitivo, entonces de acuerdo a la clasificación de O'Nan-Scott existen cinco de este tipo de grupos primitivos. Eugenia O'Reilly Regueiro en [2] reduce esta clasificación para $\lambda \leq 4$, demuestra que cuando se piden estas condiciones a los diseños, sus grupos de automorfismos sólo pueden ser afines o casi simples. Este trabajo busca dar un acercamiento a la generalización de dicho teorema, por lo que nos centraremos sólo en la acción producto y veremos qué consecuencias trae el suponer la existencia de un diseño cuyo grupo de automorfismos además de ser transitivo en banderas y primitivo sea de este tipo.

5.1. Acción producto

Empecemos recordando un resultado dado en [2] y que será de gran utilidad.

Corolario 2. *Si G es un grupo de automorfismos transitivo en banderas de un $(v, k, \lambda)-$diseño simétrico D, entonces k divide a $\lambda gcd(v-1, |G_x|)$ para cada estabilizador G_x.*

El siguiente es un lema importante pues nos da una condición aritmética que utilizaremos con regularidad tanto para la obtención de las primeras posibles ternas con la acción producto, como para los resultados centrales de esta tesis.

Supongamos que G tiene una acción producto en el conjunto de puntos P. Entonces hay un grupo H actuando primitivamente en Γ, con $|\Gamma| \geq 5$, de tipo casi simple o diagonal simple, donde

$$P = \Gamma^l \qquad y \qquad G \leq H^l \rtimes S_l = HwrS_l, \qquad l \geq 2.$$

Lema 20. *Si G es un grupo primitivo en puntos actuando transitivamente en banderas en un $(v, k, \lambda)-$ diseño simétrico D, con una acción producto en P, entonces k divide a $\lambda l(|\Gamma| - 1)$ y además $v = |\Gamma|^l \leq \lambda l^2(|\Gamma| - 1)^2$*

Demostración. Tomamos $x \in P$, si $x = (\gamma_1, ..., \gamma_l)$, definimos para $1 \leq j \leq l$ la línea cartesiana de la j-ésima clase paralela que pasa por x como el conjunto

$$G_{x,j} = \{(\gamma_1, ..., \gamma_{j-1}, \gamma, \gamma_{j+1}, ..., \gamma_l) | \gamma \in \Gamma\},$$

es decir

$$G_{x,j} = \{\gamma_1\} \times ... \times \{\gamma_{j-1}\} \times \Gamma \times \{\gamma_{j+1}\} \times ... \times \{\gamma_l\}$$

Denotamos $|\Gamma| = m$, luego, como G es primitivo afirmamos que G_x es transitivo en las l líneas cartesianas que pasan por x . Sea Δ la unión de estas líneas excluyendo a x, entonces Δ es una unión de órbitas de G_x, y cada bloque que contiene a x lo intersecta en el mismo número de puntos. Entonces, contemos las banderas (y, B) tales que $y \in \Delta$ y B es un bloque que contiene a x.

Por un lado x y y están en λ bloques y hay $l(m-1)$ puntos $y \in \Delta$, por lo que hay $\lambda l(m-1)$ banderas de esta forma. Por otro lado si r es la cantidad de puntos en los que un bloque que contiene a x intersecta a Δ, entonces dado que hay k bloques que contienen a x, habrá kr banderas de esta forma. Por lo tanto obtenemos que $kr = \lambda l(m-1)$, es decir, k divide a $\lambda l(m-1)$. Luego como $k^2 > \lambda(m^l - 1)$ entonces $(m^l - 1) < \lambda l^2(m-1)^2$ y por lo tanto

$$m^l \leq \lambda l^2(m-1)^2 \tag{5.1}$$

que era lo que se quería probar. □

El siguiente lema nos da posibles ternas con la acción producto usando un método similar al utilizado por Eugenia O'Reilly Regueiro en [2] pero ampliando la cota para λ. Este lema nos dará valiosa información de lo que estaría pasando para λ arbitraria.

Lema 21. *Si D es un $(v,k,\lambda)-$diseño simétrico con $\lambda \leq 20$ admitiendo un grupo de automorfismos primitivo en puntos y transitivo en banderas G, entonces G no tiene una acción producto no trivial o D tiene parámetros* $(121,25,5)$, $(36,15,6)$, $(441,56,7)$, $(125,32,8)$, $(25,16,10)$, $(64,28,12)$,$(289,64,14)$, $(1369,153,17)$, $(361,81,18)$, $(169,57,19)$, $(100,45,20)$.

Demostración. Para $\lambda = 2,3,4$ ya está hecha la prueba. Probemos el lema para $20 \geq \lambda \geq 4$. Del lema 20, tenemos $\lambda > \frac{5^{l-2}}{l^2}$.
De (5.1) tenemos que

$$m^{l-2} < \lambda l^2. \tag{5.2}$$

$\lambda = 5$.
Si $\lambda = 5$ entonces $l \in \{2,3,4\}$.

$l = 4$. Entonces $m^2 < 80$ entonces $m \in \{5,6,7,8\}$. Al sustituir $v = m^4$ y $\lambda = 5$ en (2.2) obtenemos $20m^4 - 19$ que no es cuadrado para ningún valor de m, contradiciendo el lema 1.

$l = 3$. De (5.2) tenemos que $m < 45$ entonces $m \in \{5, ..., 44\}$. Pero del Corolario 2 tenemos que k divide a $5gcd(3(m-1), m^3-1) = 5(m-1)gcd(3, m^2+m+1)$ de donde $gcd(3, m^2+m+1) \equiv 0 \pmod 3$ ó $gcd(3, m^2+m+1) = 1$.
Pero si $gcd(3, m^2+m+1) = 1$ entonces k divide a $5(m-1)$ de donde $k^2 \leq 25(m-1)^2$ pero $k^2 > 5(m^3-1)$ entonces $m^3 - 1 < 5(m-1)^2 < 5m^2$ entonces $m^3 \leq 5m^2$ y por lo tanto $m < 5$ lo que no es posible.
Luego si $gcd(3, m^2+m+1) \equiv 0 \pmod 3$ entonces $m \equiv 1 \pmod 3$ y entonces $m \in \{7+3i | 0 \leq i \leq 12\}$. Al sustituir $v = m^3$ y $\lambda = 5$ en (2.2) obtenemos $20m^3 - 19$ que no es cuadrado para ningún valor de m excepto $m \in \{25, 43\}$. Entonces como $k = \frac{1+\sqrt{20m^3-19}}{2}$, $k(25) = 280$ y $k(43) = 631$. Pero k debe dividir a $\lambda l(m-1) = 15(m-1)$. Lo cual no se cumple para $m \in \{25, 43\}$.

$l = 2$. Notemos que en general para cualquier λ, como k divide a $2\lambda(m-1)$ entonces existe un entero r tal que $1 \leq r \leq 2\lambda$ y $k = \frac{2\lambda(m-1)}{r}$, luego al sustituir en $k(k-1) = \lambda(m^2-1)$ y despejar m tenemos

$$m = \frac{r^2 + 2r + 4\lambda}{4\lambda - r^2} \tag{5.3}$$

Para este caso en particular tendremos que $m = \frac{r^2+2r+20}{20-r^2}$, entonces si

$r = 1$, $m = \frac{23}{19}$

$r = 2$, $m = \frac{28}{16}$

$r = 3$, $m = \frac{35}{11}$

entonces estos tres casos no pueden ser, si $r = 4$, $m = \frac{44}{4} = 11$

y en este caso obtenemos que $k = \frac{1+\sqrt{20m^2-19}}{2} = 25$ y $v = m^2 = 121$, entonces tenemos los parámetros $(121, 25, 5)$.

Luego para $r \geq 5$, $m < 0$, lo que es una contradicción.

$\lambda = 6$.

Del Lema 20, tenemos $\lambda > \frac{5^{l-2}}{l^2}$, de donde si $\lambda = 6$ entonces $l \in \{2, 3, 4, 5\}$.

$l = 5$. De (5.2) tenemos que $m^3 < 150$, entonces $m = 5$. Al sustituir $v = m^5$ y $\lambda = 6$ en (2.2) obtenemos $24m^5 - 23$ que no es cuadrado para $m = 5$, contradiciendo el Lema 1.

$l = 4$. De (5.2) tenemos que $m^2 < 96$ entonces $m \in \{5, 6, 7, 8, 9\}$. Al sustituir $v = m^4$ y $\lambda = 6$ en (2.2) obtenemos $24m^4 - 23$ que no es cuadrado para ningún valor de m, contradiciendo el Lema 1.

$l = 3$. De (5.2) tenemos que $m < 54$ entonces $m \in \{5, ..., 53\}$. Pero del Corolario 2 tenemos que k divide a $6gcd(3(m-1), m^3-1) = 6(m-1)gcd(3, m^2+m+1)$ de donde $gcd(3, m^2+m+1) \equiv 0 \pmod 3$ ó $gcd(3, m^2+m+1) = 1$.

Pero si $gcd(3, m^2+m+1) = 1$ entonces k divide a $6(m-1)$ de donde $k^2 \leq 36(m-1)^2$ pero $k^2 > 6(m^3-1)$ entonces $m^3 - 1 < 6(m-1)^2 < 6m^2$ entonces $m^3 \leq 6m^2$ y por lo tanto $m < 6$ entonces $m = 5$. Al sustituir $v = m^3$ y $\lambda = 6$ en (2.2) obtenemos $24m^3 - 23$ que no es cuadrado si $m = 5$ y por lo tanto este caso no puede ser.

Luego si $gcd(3, m^2+m+1) \equiv 0 \pmod 3$ entonces $m \equiv 1 \pmod 3$ y entonces $m \in \{7 + 3i | 0 \leq i \leq 15\}$. Al sustituir $v = m^3$ y $\lambda = 6$ en (2.2) obtenemos $24m^3 - 23$ que no es cuadrado para ningún valor de m excepto $m = 52$. Entonces como $k = \frac{1+\sqrt{24m^3-23}}{2}$, $k = 919$. Pero k debe dividir a $\lambda l(m-1) = 18(m-1) = 918$, lo cual no se cumple.

1. $l = 2$. De (5.3) tendremos que $m = \frac{r^2+2r+24}{24-r^2}$, entonces si

   $r = 1$, $m = \frac{27}{23}$

$r = 2$, $m = \frac{32}{20}$

$r = 3$, $m = \frac{39}{15}$

entonces estos tres casos no pueden ser, si $r = 4$, $m = \frac{48}{8} = 6$

y en este caso obtenemos que $k = \frac{1+\sqrt{24m^2-23}}{2} = 15$ y $v = m^2 = 36$, entonces tenemos los parámetros $(36, 15, 6)$.

Luego para $r \geq 5$, $m < 0$, lo que es una contradicción.

$\lambda = 7$.

Primero notemos que al sustituir $v = m^l$ y $\lambda = 7$ en (2.2) obtenemos

$$28m^l - 27. \tag{5.4}$$

Del lema 20, tenemos $\lambda > \frac{5^{l-2}}{l^2}$, de donde si $\lambda = 7$ entonces $l \in \{2, 3, 4, 5\}$

$l = 5$. De (5.2) tenemos que $m^3 < 175$, entonces $m = 5$. Al sustituir en (5.4) no se obtiene un cuadrado, contradiciendo el Lema 1.

$l = 4$. De (5.2) tenemos que $m^2 < 112$ entonces $5 \leq m \leq 10$. Al sustituir en (5.4) no se obtiene un cuadrado, para ningún valor de m, contradiciendo el Lema 1.

$l = 3$. De (5.2) tenemos que $m < 63$ entonces $m \in \{5, ..., 63\}$. Pero del Corolario 2 tenemos que k divide a $7gcd(3(m-1), m^3-1) = 7(m-1)gcd(3, m^2+m+1)$ de donde $gcd(3, m^2+m+1) \equiv 0 \pmod 3$ ó $gcd(3, m^2+m+1) = 1$.

Pero si $gcd(3, m^2+m+1) = 1$ entonces k divide a $7(m-1)$ de donde $k^2 \leq 49(m-1)^2$ pero $k^2 > 7(m^3-1)$ entonces $m^3 - 1 < 7(m-1)^2 < 7m^2$ entonces $m^3 \leq 7m^2$ y por lo tanto $m < 7$ entonces $m \in \{5, 6\}$. Al sustituir $v = m^3$ y $\lambda = 7$ en (2.2) obtenemos $28m^3 - 27$ que no es cuadrado para ningún valor de m y por lo tanto este caso no puede ser.

Luego si $gcd(3, m^2+m+1) \equiv 0 \pmod 3$ entonces $m \equiv 1 \pmod 3$ y entonces $m \in \{7 + 3i | 0 \leq i \leq 18\}$. Al sustituir $v = m^3$ y $\lambda = 7$ en (2.2) obtenemos $28m^3 - 27$ que no es cuadrado para ningún valor de m excepto $m = 61$. Entonces como $k = \frac{1+\sqrt{28m^3-27}}{2}$, $k = 1261$. Pero k debe dividir a $\lambda l(m-1) = 18(m-1) = 1260$, lo cual no se cumple.

Podemos enunciar los siguientes lemas que servirán para las siguientes λ.

Lema 22. *Si D es un $(v,k,\lambda)-$diseño simétrico con $\lambda \leq 20$ admitiendo un grupo de automorfismos primitivo en puntos y transitivo en banderas G con $v = m^3$, entonces $m \in \{7+3i | 0 \leq i \leq 3\lambda - 3\} \cup \{m < \lambda | m \equiv 0 \pmod 3, m \equiv 2 \pmod 3\}$*

Demostración. De (5.2) tenemos que $m < 9\lambda$ entonces $5 \leq m \leq 9\lambda - 1$. Pero del Corolario 2 tenemos que k divide a $\lambda gcd(3(m-1), m^3 - 1) = \lambda(m-1)gcd(3, m^2+m+1)$ de donde $gcd(3, m^2+m+1) \equiv 0 \pmod 3$ ó $gcd(3, m^2+m+1) = 1$.
Luego si $gcd(3, m^2+m+1) \equiv 0 \pmod 3$ entonces $m \equiv 1 \pmod 3$ y como $5 \leq m \leq 9\lambda - 1$ la cota inferior de m será 7 y la cota superior será $7 + 3i = 9\lambda - 2$ de donde es claro que la cota superior será $i = 3\lambda - 3$ y entonces $m \in \{7+3i | 0 \leq i \leq 3\lambda - 3\}$.
Pero si $gcd(3, m^2+m+1) = 1$ entonces k divide a $\lambda(m-1)$ de donde $k^2 \leq \lambda^2(m-1)^2$ pero $k^2 > \lambda^2(m^3 - 1)$ entonces $m^3 - 1 < \lambda(m-1)^2 < 7m^2$ entonces $m^3 \leq \lambda^2$ y por lo tanto $m < \lambda$. De donde es claro el resultado. □

Lema 23. *Si D es un $(v,k,\lambda)-$diseño simétrico con $\lambda \leq 20$ admitiendo un grupo de automorfismos primitivo en puntos y transitivo en banderas G con $v = m^3$ y $m = 9\lambda - 2$ entonces*

i) Al sustituir en (2.2) se obtiene un cuadrado,

ii) k no divide a $\lambda l(m-1)$.

Demostración. Al sustituir $l = 3$ y $m = 9\lambda - 2$ en (2.2) obtenemos $4\lambda(v-1) + 1 = 2916\lambda^4 - 1944\lambda^3 + 432\lambda^2 - 36\lambda + 1$ que podemos factorizar como $4\lambda(v-1) + 1 = (54\lambda^2 - 18\lambda + 1)^2$ con lo que probamos (i).
Recordemos que $k = \frac{1+\sqrt{4\lambda(v-1)+1}}{2}$ al sustituir tenemos que $k = 27\lambda^2 - 9\lambda + 1$, mientras que $\lambda l(m-1) = 27\lambda^2 - 9\lambda$, es decir $k = \lambda l(m-1) + 1$ por lo que se tiene (ii). □

Corolario 3. *Si D es un $(v,k,\lambda)-$diseño simétrico con $\lambda \leq 20$ admitiendo un grupo de automorfismos primitivo y transitivo en banderas G con $v = m^3$, entonces $m \in \{7+3i | 0 \leq i \leq 3\lambda - 4\} \cup \{m < \lambda | m \equiv 0 \pmod 3, m \equiv 2 \pmod 3\}$*

Demostración. Como se cumple el Lema 23 entonces el valor $m = 9\lambda - 2$ no puede ocurrir pues se contradice el hecho de que k divide a $\lambda l(m-1)$ por lo tanto la cota maxima se alcanza en $i = 3\lambda - 3 - 1 = 3\lambda - 4$ de donde se obtiene lo que se quería probar. □

Continuando con la prueba de $\lambda = 7$.

$l = 2$. De (5.3) tendremos que $m = \frac{r^2+2r+28}{28-r^2}$, entonces si

$r = 1$, $m = \frac{31}{27}$

$r = 2$, $m = \frac{36}{24}$

$r = 3$, $m = \frac{43}{19}$

$r = 4$, $m = \frac{52}{12}$

estos casos no pueden ser, si $r = 5$, $m = \frac{63}{12} = 21$

y en este caso obtenemos que $k = \frac{1+\sqrt{28m^2-27}}{2} = 56$ y $v = m^2 = 441$, entonces tenemos los parámetros $(441, 56, 7)$.

Luego para $r \geq 6$, $m < 0$, lo que es una contradicción.

$\lambda = 8$. Primero notemos que al sustituir $v = m^l$ y $\lambda = 8$ en (2.2) obtenemos

$$32m^l - 31. \tag{5.5}$$

Del lema 20, tenemos $\lambda > \frac{5^{l-2}}{l^2}$, de donde si $\lambda = 8$ entonces $l \in \{2, 3, 4, 5\}$.

$l = 5$. De (5.2) tenemos que $m^3 < 200$, entonces $m = 5$. Al sustituir en (5.5) no se obtiene un cuadrado, contradiciendo el Lema 1.

$l = 4$. De (5.2) tenemos que $m^2 < 128$ entonces $5 \leq m \leq 11$. Al sustituir en (5.5) no se obtiene un cuadrado, para ningún valor de m, contradiciendo el lema 1.

$l = 3$. Del Corolario 3 tenemos que $m \in \{7 + 3i | 0 \leq i \leq 20\}$ o $m \in \{5, 6\}$, en el primer caso al sustituir en (5.5) no se obtiene ningún cuadrado, en el segundo caso se obtiene un cuadrado cuando $m = 5$ con lo que $k = 32$ y $v = m^l = 125$ entonces obtenemos los parámetros $(125, 32, 8)$.

$l = 2$. De (5.3) tendremos que $m = \frac{r^2+2r+32}{32-r^2}$, entonces si

$r = 1$, $m = \frac{35}{31}$

$r = 2$, $m = \frac{40}{28}$

$r = 3$, $m = \frac{47}{23}$

$r = 4$, $m = \frac{56}{16}$

$r = 5$, $m = \frac{67}{7}$

estos casos no pueden ser. Luego para $r \geq 6$, $m < 0$, lo que es una contradicción.

$\lambda = 9$.

Primero notemos que al sustituir $v = m^l$ y $\lambda = 9$ en (2.2) obtenemos

$$36m^l - 37. \tag{5.6}$$

Del lema 20, tenemos $\lambda > \frac{5^{l-2}}{l^2}$, de donde si $\lambda = 9$ entonces $l \in \{2, 3, 4, 5\}$

$l = 5$. De (5.2) tenemos que $m^3 < 225$, entonces $m = 5$. Al sustituir en (5.6) no se obtiene un cuadrado, contradiciendo el Lema 1.

$l = 4$. De (5.2) tenemos que $m^2 < 144$ entonces $5 \leq m \leq 11$. Al sustituir en (5.6) no se obtiene un cuadrado, para ningún valor de m, contradiciendo el Lema 1.

$l = 3$. Del Corolario 3 tenemos que $m \in \{7 + 3i | 0 \leq i \leq 23\}$ o $m \in \{5, 6, 8\}$, en ambos casos al sustituir en (5.6) no se obtiene ningún cuadrado.

$l = 2$. De (5.3) tendremos que $m = \frac{r^2+2r+36}{36-r^2}$, entonces si

$r = 1$, $m = \frac{39}{35}$

$r = 2$, $m = \frac{44}{32}$

$r = 3$, $m = \frac{51}{27}$

$r = 4$, $m = \frac{60}{20} =< 5$

$r = 5$, $m = \frac{71}{11}$

estos casos no pueden ser. Luego para $r \geq 6$, $m < 0$, lo que es una contradicción.

En el caso de $\lambda = 9$ no obtuvimos ninguna terna de parámetros.

$\lambda = 10$.

Primero notemos que al sustituir $v = m^l$ y $\lambda = 10$ en (2.2) obtenemos

$$40m^l - 39. \tag{5.7}$$

Del lema 20, tenemos $\lambda > \frac{5^{l-2}}{l^2}$, de donde si $\lambda = 10$ entonces $l \in \{2, 3, 4, 5\}$

$l = 5$. De (5.2) tenemos que $m^3 < 250$, entonces $m = 5$. Al sustituir en (5.7) no se obtiene un cuadrado, contradiciendo el Lema 1.

$l = 4$. De (5.2) tenemos que $m^2 < 160$ entonces $5 \leq m \leq 12$. Al sustituir en (5.7) no se obtiene un cuadrado, para ningún valor de m, contradiciendo el Lema 1.

$l = 3$. Del Corolario 3 tenemos que $m \in \{7 + 3i | 0 \leq i \leq 26\}$ o $m \in \{5, 6, 8, 9\}$, en ambos casos al sustituir en (5.7) no se obtiene ningún cuadrado.

$l = 2$. De (5.3) tendremos que $m = \frac{r^2+2r+40}{40-r^2}$, entonces si

$r = 1$, $m = \frac{43}{39}$

$r = 2$, $m = \frac{48}{36}$

$r = 3$, $m = \frac{55}{31}$

$r = 4$, $m = \frac{64}{24}$

estos casos no pueden ser, si $r = 5$, $m = \frac{75}{15} = 5$

y en este caso obtenemos que $k = \frac{1+\sqrt{40m^2-39}}{2} = 16$ y $v = m^2 = 25$, entonces tenemos los parámetros $(25, 16, 10)$.

Si $r = 6$, $m = \frac{88}{4} = 22$

y en este caso obtenemos que $k = 70$ y $v = m^2 = 484$, entonces tenemos parámetros $(484, 70, 10)$, notemos que $k - \lambda = 70 - 10 = 60$ que no es un cuadrado lo que no puede ser por el teorema de Bruck-Chowla-Ryser con v par, por lo que esta terna no es válida.

Luego para $r \geq 7$, $m < 0$, lo que es una contradicción.

$\lambda = 11$.

Primero notemos que al sustituir $v = m^l$ y $\lambda = 11$ en (2.2) obtenemos

$$44m^l - 43. \tag{5.8}$$

Del Lema 20, tenemos $\lambda > \frac{5^{l-2}}{l^2}$, de donde si $\lambda = 11$ entonces $l \in \{2, 3, 4, 5\}$.

$l = 5$. De (5.2) tenemos que $m^3 < 275$, entonces $m \in \{5, 6\}$. Al sustituir en (5.8) no se obtiene un cuadrado, contradiciendo el Lema 1.

$l = 4$. De (5.2) tenemos que $m^2 < 176$ entonces $5 \leq m \leq 13$. Al sustituir en (5.8) se obtiene

un cuadrado cuando $m = 13$, entonces $k = 561$ pero $\lambda l(m-1) = 528$ por lo tanto este caso no puede ser pues se contradice el hecho de que k divide a $\lambda l(m-1)$.

$l = 3$. Del Corolario 3 tenemos que $m \in \{7 + 3i | 0 \leq i \leq 29\}$ o $m \in \{5, 6, 8, 9\}$, en ambos casos al sustituir en (5.8) no se obtiene ningún cuadrado.

$l = 2$. De (5.3) tendremos que $m = \frac{r^2+2r+44}{44-r^2}$, para $1 \leq r \leq 6$ no se obtiene m entera y para $r \geq 7$, $m < 0$, lo que es una contradicción.

Por lo que para $\lambda = 11$ no obtuvimos ninguna terna de parámetros.

$\lambda = 12$.

Primero notemos que al sustituir $v = m^l$ y $\lambda = 12$ en (2.2) obtenemos

$$48m^l - 47. \tag{5.9}$$

Del Lema 20, tenemos $\lambda > \frac{5^{l-2}}{l^2}$, de donde si $\lambda = 12$ entonces $l \in \{2, 3, 4, 5\}$

$l = 5$. De (5.2) tenemos que $m^3 < 300$, entonces $m \in \{5, 6\}$. Al sustituir en (5.9) no se obtiene un cuadrado, contradiciendo el Lema 1.

$l = 4$. De (5.2) tenemos que $m^2 < 192$ entonces $5 \leq m \leq 13$. Al sustituir en (5.9) no se obtiene un cuadrado, para ningún valor de m, contradiciendo el Lema 1.

$l = 3$. Del Corolario 3 tenemos que $m \in \{7 + 3i | 0 \leq i \leq 32\}$ o $m \in \{5, 6, 8, 9, 11\}$, en ambos casos al sustituir en (5.9) no se obtiene ningún cuadrado.

$l = 2$. De (5.3) tendremos que $m = \frac{r^2+2r+48}{48-r^2}$, para $1 \leq r \leq 5$ no se obtiene m entera. Para $r = 6$ $m = 8$ y obtenemos que $k = \frac{1+\sqrt{48m^2-47}}{2} = 28$ y $v = m^2 = 64$, entonces tenemos los parámetros $(64, 28, 12)$.

Para $r \geq 7$, $m < 0$, lo que es una contradicción.

$\lambda = 13$

Primero notemos que al sustituir $v = m^l$ y $\lambda = 13$ en (2.2) obtenemos

$$52m^l - 51. \tag{5.10}$$

Del Lema 20, tenemos $\lambda > \frac{5^{l-2}}{l^2}$, de donde si $\lambda = 13$ entonces $l \in \{2, 3, 4, 5\}$.

$l = 5$. De (5.2) tenemos que $m^3 < 325$, entonces $m \in \{5, 6\}$. Al sustituir en (5.10) no se obtiene un cuadrado, contradiciendo el Lema 1.

$l = 4$. De (5.2) tenemos que $m^2 < 208$ entonces $5 \leq m \leq 14$. Al sustituir en (5.10) no se obtiene un cuadrado, para ningún valor de m, contradiciendo el Lema 1.

$l = 3$. Del Corolario 3 tenemos que $m \in \{7 + 3i | 0 \leq i \leq 35\}$ o
$m \in \{5, 6, 8, 9, 11, 12\}$, en ambos casos al sustituir en (5.10) no se obtiene ningún cuadrado.

$l = 2$. De (5.3) tendremos que $m = \frac{r^2+2r+52}{52-r^2}$, para $1 \leq r \leq 7$ no se obtiene m entera. Para $r = 8$ se obtiene $m = -11$ lo que no puede ser.
Para $r \geq 8$, $m < 0$, lo que es una contradicción.
Por lo que para $\lambda = 13$ no obtuvimos ninguna terna de parámetros.

$\lambda = 14$.

Primero notemos que al sustituir $v = m^l$ y $\lambda = 14$ en (2.2) obtenemos

$$56m^l - 55. \tag{5.11}$$

Del Lema 20, tenemos $\lambda > \frac{5^{l-2}}{l^2}$, de donde si $\lambda = 14$ entonces $l \in \{2, 3, 4, 5\}$

$l = 5$. De (5.2) tenemos que $m^3 < 350$, entonces $m \in \{5, 6, 7\}$. Al sustituir en (5.11) no se obtiene un cuadrado, contradiciendo el Lema 1.

$l = 4$. De (5.2) tenemos que $m^2 < 224$ entonces $5 \leq m \leq 14$. Al sustituir en (5.11) no se obtiene un cuadrado, para ningún valor de m, contradiciendo el Lema 1.

$l = 3$. Del corolario 3 tenemos que $m \in \{7 + 3i | 0 \leq i \leq 38\}$ o $m \in \{5, 6, 8, 9, 11, 12\}$, en ambos casos al sustituir en (5.11) no se obtiene ningún cuadrado.

$l = 2$. De (5.3) tendremos que $m = \frac{r^2+2r+56}{56-r^2}$, para $1 \leq r \leq 3$ no se obtiene m entera. Para $r = 4$ $m = 2$ lo que no puede ser, para $5 \leq r \leq 6$ no se obtiene m entera, para $r = 7$ $m = 17$ y obtenemos que $k = \frac{1+\sqrt{56m^2-55}}{2} = 64$ y $v = m^2 = 289$, entonces tenemos los parámetros $(289, 64, 14)$.
Para $r \geq 8$, $m < 0$, lo que es una contradicción.

$\lambda = 15$.

Primero notemos que al sustituir $v = m^l$ y $\lambda = 14$ en (2.2) obtenemos

$$60m^l - 59. \tag{5.12}$$

Del Lema 20, tenemos $\lambda > \frac{5^{l-2}}{l^2}$, de donde si $\lambda = 15$ entonces $l \in \{2, 3, 4, 5\}$

$l = 5$. De (5.2) tenemos que $m^3 < 375$, entonces $m \in \{5, 6, 7\}$. Al sustituir en (5.12) no se obtiene un cuadrado, contradiciendo el Lema 1.

$l = 4$. De (5.2) tenemos que $m^2 < 240$ entonces $5 \leq m \leq 15$. Al sustituir en (5.12) no se obtiene un cuadrado, para ningún valor de m, contradiciendo el Lema 1.

$l = 3$. Del Corolario 3 tenemos que $m \in \{7+3i | 0 \leq i \leq 41\}$ o $m \in \{5, 6, 8, 9, 11, 12, 14\}$, en el primer caso al sustituir en (5.12) no se obtiene ningún cuadrado, en el segundo caso se obtiene al sustituir en (5.12) que este es cuadrado cuando $m = 9$ lo que nos da $k = 105$ pero $\lambda l(m-1) = 360$ y entonces este caso no puede ser pues se contradice el hecho de que k divide a $\lambda l(m-1)$.

$l = 2$. De (5.3) tendremos que $m = \frac{r^2+2r+60}{60-r^2}$, para $1 \leq r \leq 7$ no se obtiene m entera.
Para $r \geq 8$, $m < 0$, lo que es una contradicción.
Por lo que para $\lambda = 15$ no obtuvimos ninguna terna de parámetros.

$\lambda = 16$.

Como antes, al sustituir $v = m^l$ y $\lambda = 16$ en (2.2) obtenemos

$$64m^l - 63. \tag{5.13}$$

Del Lema 20, tenemos $\lambda > \frac{5^{l-2}}{l^2}$, de donde si $\lambda = 16$ entonces $l \in \{2, 3, 4, 5\}$.

$l = 5$. De (5.2) tenemos que $m^3 < 400$, entonces $m \in \{5, 6, 7\}$. Al sustituir en (5.13) no se obtiene un cuadrado, contradiciendo el Lema 1.

$l = 4$. De (5.2) tenemos que $m^2 < 256$ entonces $5 \leq m \leq 15$. Al sustituir en (5.13) no se obtiene un cuadrado, para ningún valor de m, contradiciendo el Lema 1.

$l = 3$. Del corolario 3 tenemos que $m \in \{7 + 3i | 0 \leq i \leq 44\}$ o $m \in \{5, 6, 8, 9, 11, 12, 14, 15\}$, en ambos casos al sustituir en (5.13) no se obtiene ningún cuadrado.

$l = 2$. De (5.3) tendremos que $m = \frac{r^2+2r+64}{64-r^2}$, para $r \in \{1, 2, 3, 5, 6, 7\}$ no se obtiene m entera.
Para $r = 6$ $m = 4$ lo que no puede ser. Luego si $r = 8$ m se indetermina.
Para $r \geq 9$, $m < 0$, lo que es una contradicción.
Por lo que para $\lambda = 16$ no obtuvimos ninguna terna de parámetros.

$\lambda = 17$.
Al sustituir $v = m^l$ y $\lambda = 17$ en (2.2) obtenemos

$$68m^l - 67. \tag{5.14}$$

Del Lema 20, tenemos $\lambda > \frac{5^{l-2}}{l^2}$, de donde si $\lambda = 17$ entonces $l \in \{2, 3, 4, 5\}$.

$l = 5$. De (5.2) tenemos que $m^3 < 425$, entonces $m \in \{5, 6, 7\}$. Al sustituir en (5.14) no se obtiene un cuadrado, contradiciendo el Lema 1.

$l = 4$. De (5.2) tenemos que $m^2 < 272$ entonces $5 \leq m \leq 16$. Al sustituir en (5.14) no se obtiene un cuadrado, para ningún valor de m, contradiciendo el Lema 1.

$l = 3$. Del Corolario 3 tenemos que $m \in \{7 + 3i | 0 \leq i \leq 47\}$ o $m \in \{5, 6, 8, 9, 11, 12, 14, 15\}$, en ambos casos al sustituir en (5.14) no se obtiene ningún cuadrado.

$l = 2$. De (5.3) tendremos que $m = \frac{r^2+2r+68}{68-r^2}$, para $1 \leq r \leq 7$ no se obtiene m entera. Para $r = 8$ $m = 37$ de donde obtenemos que $k = \frac{1+\sqrt{68m^2-67}}{2} = 153$ y $v = m^2 = 1369$, entonces tenemos los parámetros $(1369, 153, 17)$.
Para $r \geq 9$, $m < 0$, lo que es una contradicción.

$\lambda = 18$.
Al sustituir $v = m^l$ y $\lambda = 18$ en (2.2) obtenemos

$$72m^l - 71. \tag{5.15}$$

Del Lema 20, tenemos $\lambda > \frac{5^{l-2}}{l^2}$, de donde si $\lambda = 18$ entonces $l \in \{2, 3, 4, 5, 6\}$.

$l = 6$. De (5.2) tenemos que $m^4 < 648$, entonces $m = 5$. Al sustituir en (5.15) no se obtiene un cuadrado, contradiciendo el Lema 1.

$l = 5$. De (5.2) tenemos que $m^3 < 450$, entonces $m \in \{5, 6, 7\}$. Al sustituir en (5.15) no se obtiene un cuadrado, contradiciendo el Lema 1.

$l = 4$. De (5.2) tenemos que $m^2 < 288$ entonces $5 \leq m \leq 16$. Al sustituir en (5.15) no se obtiene un cuadrado, para ningún valor de m, contradiciendo el Lema 1.

$l = 3$. Del Corolario 3 tenemos que $m \in \{7+3i | 0 \leq i \leq 50\}$ o $m \in \{5, 6, 8, 9, 11, 12, 14, 15, 17\}$, en ambos casos al sustituir en (5.15) no se obtiene ningún cuadrado.

$l = 2$. De (5.3) tendremos que $m = \frac{r^2+2r+72}{72-r^2}$, para $1 \leq r \leq 7$ no se obtiene m entera. Para $r = 8$ $m = 19$ de donde obtenemos que $k = \frac{1+\sqrt{72m^2-71}}{2} = 81$ y $v = m^2 = 361$, entonces tenemos los parámetros $(361, 81, 18)$.
Para $r \geq 9$, $m < 0$, lo que es una contradicción.

$\lambda = 19$.
Al sustituir $v = m^l$ y $\lambda = 19$ en (2.2) obtenemos

$$76m^l - 75. \tag{5.16}$$

Del Lema 20, tenemos $\lambda > \frac{5^{l-2}}{l^2}$, de donde si $\lambda = 19$ entonces $l \in \{2, 3, 4, 5, 6\}$.

$l = 6$. De (5.2) tenemos que $m^4 < 684$, entonces $m = 5$. Al sustituir en (5.16) no se obtiene un cuadrado, contradiciendo el Lema 1.

$l = 5$. De (5.2) tenemos que $m^3 < 475$, entonces $m \in \{5, 6, 7\}$. Al sustituir en (5.16) no se obtiene un cuadrado, contradiciendo el Lema 1.

$l = 4$. De (5.2) tenemos que $m^2 < 304$ entonces $5 \leq m \leq 17$. Al sustituir en (5.16) no se obtiene un cuadrado, para ningún valor de m, contradiciendo el lema 1.

$l = 3$. Del Corolario 3 tenemos que $m \in \{7+3i | 0 \leq i \leq 53\}$ o $m \in \{5, 6, 8, 9, 11, 12, 14, 15, 17, 18\}$, en ambos casos al sustituir en (5.16) no se obtiene ningún cuadrado.

$l = 2$. De (5.3) tendremos que $m = \frac{r^2+2r+76}{76-r^2}$, para $1 \leq r \leq 7$ no se obtiene m entera. Para $r = 8$ $m = 13$ de donde obtenemos que $k = \frac{1+\sqrt{76m^2-75}}{2} = 57$ y $v = m^2 = 169$, entonces tenemos los parámetros $(169, 57, 19)$.

Para $r \geq 9$, $m < 0$, lo que es una contradicción.

$\lambda = 20$.

Al sustituir $v = m^l$ y $\lambda = 20$ en (2.2) obtenemos

$$80m^l - 79. \tag{5.17}$$

Del Lema 20, tenemos $\lambda > \frac{5^{l-2}}{l^2}$, de donde si $\lambda = 20$ entonces $l \in \{2, 3, 4, 5, 6\}$.

$l = 6$. De (5.2) tenemos que $m^4 < 720$, entonces $m = 5$. Al sustituir en (5.17) no se obtiene un cuadrado, contradiciendo el Lema 1.

$l = 5$. De (5.2) tenemos que $m^3 < 500$, entonces $m \in \{5, 6, 7\}$. Al sustituir en (5.17) no se obtiene un cuadrado, contradiciendo el Lema 1.

$l = 4$. De (5.2) tenemos que $m^2 < 320$ entonces $5 \leq m \leq 17$. Al sustituir en (5.17) no se obtiene un cuadrado, para ningún valor de m, contradiciendo el Lema 1.

$l = 3$. Del Corolario 3 tenemos que $m \in \{7 + 3i | 0 \leq i \leq 56\}$ o
$m \in \{5, 6, 8, 9, 11, 12, 14, 15, 17, 18\}$, en ambos casos al sustituir en (5.17) no se obtiene ningún cuadrado.

$l = 2$. De (5.3) tendremos que $m = \frac{r^2+2r+80}{80-r^2}$, para $1 \leq r \leq 7$ no se obtiene m entera. Para $r = 8$ $m = 10$ de donde obtenemos que $k = \frac{1+\sqrt{80m^2-79}}{2} = 45$ y $v = m^2 = 100$, entonces tenemos los parámetros $(100, 45, 20)$.
Para $r \geq 9$, $m < 0$, lo que es una contradicción.

Lo cual concluye la prueba. □

Observación: De igual manera que en el caso de imprimitividad, el hecho de que se haga mención de las ternas no implica la existencia de diseños con esos parámetros.

5.1.1. Caso $l = 2$

Como pudimos notar en el anterior lema, la mayoría de las posibles ternas surgen cuando $l = 2$, pues es el caso con la cota más grande, por lo que nos centraremos en este.

Además también podemos notar que en el caso en que m es par las ternas que surgen son muy particulares, de hecho cumplen las condiciones de lo que se conoce como diseños de Manon, este hecho coincide con lo que Delu Tian y Shenglin Zhou obtienen en el artículo Flag-transitive point-primitive symmetric (v, k, λ) designs with λ at most 100. Así surge el problema central de esta tesis, demostrar que cuando se supone un diseño con λ arbitrario y con grupo de automorfismos transitivo en banderas y primitivo con la acción producto, las únicas posibles ternas que surgen son las que cumplen con las condiciones de los diseños de Menon.

En el caso en que $l = 2$, se debe cumplir la ecuación $m = \frac{r^2+2r+4\lambda}{4\lambda-r^2}$ de donde tendremos

$$(m+1)r^2 + 2r - 4\lambda(m-1) = 0 \tag{5.18}$$

y resolviendo para r tendremos

$$r = \frac{-2 \pm \sqrt{4 + 16\lambda(m-1)(m+1)}}{2(m+1)} = \frac{-1 \pm \sqrt{1 + 4\lambda(m^2-1)}}{m+1}$$

por lo tanto

$$r = \frac{2(k-1)}{m+1} \tag{5.19}$$

Supongamos $(k, \lambda) = t > 1$ (el caso en que $(k, \lambda) = 1$ fue estudiado por Paul-Hermann Zieschang), entonces existen enteros positivos a y b tales que

$$k = at, \quad \lambda = bt. \tag{5.20}$$

Entonces del Lema 20 tenemos que

$$k = \frac{2\lambda(m-1)}{r}, \tag{5.21}$$

al sustituir (5.20) en esta y en $k(k-1) = \lambda(v-1)$ tendremos

$$a = \frac{2b(m-1)}{r}, \tag{5.22}$$

$$a(at-1) = b(m^2-1). \tag{5.23}$$

De (5.22) tenemos que a divide a $b(m-1)$. Pero $(k,\lambda) = t$ entonces $t = (at, bt)$ implica $(a,b) = 1$ por lo que a divide entonces a $m-1$, es decir, existe un entero positivo s tal que $m-1 = as$ y sustituyendo en (5.22) tenemos que $r = 2bs$, más aún, dado que $(a,b) = 1$ entonces $s = (m-1, \frac{r}{2})$.

Luego tenemos los siguientes resultados para los nuevos parámetros que surgen a y s.

Lema 24. *Sea D un (v,k,λ)-diseño simétrico con $v = m^2$ admitiendo un grupo de automorfismos primitivo en puntos, transitivo en banderas y con la acción producto. Si $k = at$, $\lambda = bt$ con $t = (k,\lambda)$ entonces $a \neq 1$.*

Demostración. Si $a = 1$ entonces $k = t$ y entonces $\lambda = kb$ con $b \geq 1$ lo que no puede ser pues $k > \lambda$, por lo tanto $a \neq 1$. □

Recordemos que se obtuvo que $m-1 = as$ y $r = 2bs$ cuando $t = (k,\lambda)$ y $kr = 2\lambda(m-1)$, entonces tenemos el siguiente lema sobre a y s.

Lema 25. *Sea D un (v,k,λ)-diseño simétrico con $v = m^2$ admitiendo un grupo de automorfismos primitivo en puntos, transitivo en banderas y con la acción producto. Si $k = at$, $\lambda = bt$ con $t = (k,\lambda)$ entonces $(a,s) = 1$, con s el entero positivo tal que $m-1 = as$ y $r = 2bs$.*

Demostración. Notemos que (5.19) pude reescribirse como

$$r + 1 = k - (m-1)\frac{r}{2}$$

es decir $2bs + 1 = at - asbs$ entonces $1 = a(t - bs^2) - 2bs$ de donde se tiene lo que se quería probar que $(a,s) = 1$ □

Luego notamos que una condición suficiente y necesaria para obtener los diseños de Manon es que el parámetro s sea igual a 1.

Lema 26. *Sea D un (v,k,λ)-diseño simétrico con $v = m^2$ admitiendo un grupo de automorfismos primitivo en puntos, transitivo en banderas y con la acción producto, si $t = (k,\lambda)$ y s el entero positivo tal que $m-1 = as$ y $r = 2bs$. Entonces tendremos que $s = 1$ si y sólo si $v = 4t^2$, $k = 2t^2 - t$ y $\lambda = t^2 - t$.*

Demostración. Supongamos $s = 1$ entonces $m - 1 = a$ por lo que $k = (m-1)t$, además $\frac{r}{2} = b$ lo que implica que $\lambda = \frac{r}{2}t$. Ahora de $m = \frac{r^2+2r+4\lambda}{4\lambda - r^2}$ tenemos

$$m = \frac{b + t + 1}{t - b} \tag{5.24}$$

y entonces

$$a = m - 1 = \frac{2b + 1}{t - b} \tag{5.25}$$

Notemos que $t \neq b$ pues si $t = b$ entonces $\lambda = tb = b^2 = \frac{r^2}{4}$ y sustituyendo en (5.18) tendremos

$$r^2(m + 1) + 2r - r^2(m - 1) = 0 \Rightarrow r(r + 1) = 0$$

Es decir $r = 0$ o $r = -1$ lo que no puede ser y por lo tanto $t \neq b$.

Así $t - b \geq 1$.

Probemos que $t - b = 1$. Supongamos que $t - b > 1$

Sea $x > 1$ un entero tal que $t = b + x$, notemos que x no puede ser par, pues si $x = 2y$ entonces $t = b + 2y$ sustituyendo en (5.25) tendremos

$$a = \frac{2b + 1}{2y}$$

lo que no puede ser, por lo tanto x debe ser impar, es decir debe existir un entero $y > 0$ tal que $x = 2y + 1 > 1$ y entonces $t = b + 2y + 1$, sustituyendo en (5.25) tendremos

$$a = \frac{2b + 1}{2y + 1}$$

y como $a > b$ entonces $2b + 1 > b(2y + 1)$ por lo que

$$1 > b(2y - 1) \tag{5.26}$$

Como supusimos que $t - b > 1$ entonces $x = 2y + 1 > 1$ por lo que $2y - 1 > -1$. Luego, para que se cumpla (5.26) se debe cumplir que $2y - 1 = 0$ lo que implicaria que $y = \frac{1}{2}$ lo que no puede ser pues pedimos que y fuera entero.

Entonces $b = t - 1$ con lo que $\lambda = t(t - 1)$ luego sustituyendo en (5.25) tenemos

$$a = 2(t - 1) + 1 = 2t - 1$$

por lo que $k = t(2t - 1)$ y $m = a + 1 = 2t$ por lo que $v = m^2 = 4t^2$.

Supongamos ahora que tenemos un diseño con $v = 4t^2$, $k = 2t^2 - t$ y $\lambda = t^2 - t$ entonces $a = 2t - 1$ y $b = t - 1$, además $m = 2t$ por lo que $m - 1 = 2t - 1 = a$ pero $m - 1 = as$ entonces $s = 1$, con lo que se demuestra el lema. □

En el Lema 21 en el caso $l = 2$ lo que hacíamos era fijar λ, variar $\frac{r}{2}$ y obtener los posibles m que cumplían con la condición $m = \frac{r^2+2r+4\lambda}{4\lambda-r^2}$. Si ahora fijamos $m-1$ variamos $\frac{r}{2}$ y obtenemos los posibles λ que cumplen con la misma ecuación, nos damos cuenta de que cuando $m-1$ es una potencia de primo impar se obtienen justamente las ternas que cumplen las condiciones de los diseños de Menon. Entonces obtenemos el siguiente resultado:

Lema 27. *Sea D un (v, k, λ)-diseño simétrico con $v = m^2$ admitiendo un grupo de automorfismos primitivo en puntos, transitivo en banderas y con la acción producto, si $t = (k, \lambda)$ y s el entero positivo tal que $m - 1 = as$ y $r = 2bs$. Si $m - 1 = p^d$ con p un primo impar y d un natural se tiene que $v = 4t^2$, $k = 2t^2 - t$ y $\lambda = t^2 - t$.*

Demostración. Como $m - 1 = as = p^d$ tenemos los siguientes casos

1. $s = p^i$ & $a = p^{d-i}$ para algún $i < d$ natural
   Este caso no puede ser pues implicaría que $(a, s) = p^j$ para algun natural j contradiciendo el Lema 25.

2. $a = p^i$ & $s = p^{d-i}$ para algún $i < d$ natural
   Este caso no puede ser pues implicaría que $(a, s) = p^j$ para algun natural j contradiciendo el Lema 25.

3. $s = p^d$ & $a = 1$
   Este caso tampoco se puede cumplir por el Lema 24.

4. $a = p^d$ & $s = 1$
   Como $s = 1$, por el Lema 26 tenemos que $v = 4t^2$, $k = 2t^2 - t$ y $\lambda = t^2 - t$, con lo que queda demostrado el lema.

□

Notemos que el resultado anterior no se puede generalizar para cualquier $m - 1$ pues las ternas $(4900, 3267, 2178)$, $(16900, 2752, 448)$ y $(44100, 8019, 1458)$ son contraejemplos de esa

posible generalización. Estas son las únicas ternas que surgen para $v \leq (210)^2$ además de las ternas de Menon.

Recordemos la definición de las líneas cartesianas del Lema 20, en el caso que estamos estudiando, cuando $l = 2$, sólo existen dos líneas cartesianas para todo punto en el diseño.
Entonces tenemos dos posibles casos; el primero, para todo punto x en el diseño cada bloque que lo contiene intersecta a las dos líneas cartesianas que pasan por x, el segundo caso es que exista un punto para el cual exista un bloque que lo contenga tal que este intersecte sólo a una de las dos líneas cartesianas que pasan por x. Estudiemos este último:

Teorema: Caso 1. *Sea D un $(v, k, \lambda)-$ diseño simétrico admitiendo un grupo de automorfismos G primitivo en puntos y transitivo en banderas con una acción producto en P. Si existe una bandera (x, A) en el diseño de tal forma que A intersecte sólo a una de las dos líneas cartesianas que pasan por x entonces $r + 1$ divide a k.*

Demostración. Por las hipótesis existe una bandera (x, A) tal que A intersecta solo una línea cartesiana que pasa por $x := (a_0, b_0)$, supongamos sin pérdida de generalidad que A intersecta a la segunda línea cartesiana que pasa por x. Probaremos primero que para cualquier elemento del bloque A, este intersecta solo a la segunda línea cartesiana que pasa por dicho punto.

Por el Lema 20 tenemos que el tamaño de la intersección de A con la segunda línea cartesiana que pasa por x es $r + 1$, es decir, el número de elementos de la segunda línea cartesiana que pasa por x que además están en A es $r + 1$.

Notemos que si tomamos un punto $y \in A$ que además pertenece a la segunda línea cartesiana que pasa por x, entonces $y = (a_0, \nu)$ para algún $\nu \in \Gamma$ por lo que el conjunto de elementos de la segunda línea cartesiana que pasa por y que están en A coincide con la intersección de A con la segunda línea cartesiana que pasa por x y se cumple lo que buscamos probar.

Sea ahora un punto $y \in A$ que no pertenece a la segunda línea cartesiana que pasa por

x, por lo que $y \neq x$, entonces si $y := (a_1, b_1)$ se tiene en particular que $a_1 \neq a_0$. Consideremos la bandera (y, A), dado que el grupo G es transitivo en banderas, existe un $g \in G$ tal que $g(x, A) = (y, A)$, es decir, $g(x) = y$ entonces

$$g(a_0, b_0) = (a_1, b_1), \tag{5.27}$$

esto implica que $g|_\Gamma(a_0) = a_1$. Por lo que para $\mu \in \Gamma$ tal que $(a_0, \mu) \in A$ se tiene que $g(a_0, \mu) = (a_1, \nu)$ para algún $\nu \in \Gamma$. Por lo tanto g a cada elemento de la segunda línea que pasa por x que está en A lo manda a un elemento de la segunda línea que pasa por y que además está en A. De esta forma A intersecta únicamente a elementos de la segunda línea que pasan por y. Por como se tomó y podemos concluir lo mismo para todo elemento del bloque A que no está en la segunda línea cartesiana que pasa por x, más aún la cantidad de elementos de la segunda línea que pasa por y que están a su vez en A es $r+1$, esto por el Lema 20.

Sea A_0 el conjunto de puntos de la segunda línea cartesiana que pasa por x que están en A incluido el propio x, la cardinalidad de dicho conjunto es $r+1$. Sea un elemento $x_1 \in A - A_0$, entonces por lo dicho anteriormente A intersecta sólo a la segunda línea cartesiana que pasa por x_1, por lo tanto si A_1 es el conjunto de puntos de la segunda línea cartesiana que pasa por x_1 que están en A incluido x_1 entonces la cardinalidad de A_1 también es $r+1$. De igual forma sea ahora $x_2 \in A - (A_0 \cup A_1)$ igual que antes podemos construir A_2 como el conjunto de puntos de la segunda línea cartesiana que pasa por x_2 que están en A incluido x_2 y por lo dicho anteriormente la cardinalidad de dicho conjunto es de igual manera $r+1$.
De esta manera continuamos este proceso hasta que no haya más puntos que tomar en A, así obtenemos una colección de puntos $x_0, x_1, ..., x_i \in A$ y una colección de conjuntos $A_0, A_1, ..., A_i$ para algún natural i, tal que A_j es la intersección de la segunda línea cartesiana que pasa por x_j con A por lo que A_j tiene cardinalidad $r+1$ para todo j. Además se cumple que $A = \cup_{j=0}^{j=i} A_j$ y por la construcción se tiene que si $x_g \neq x_h$ entonces $A_g \neq A_h$ con $1 \leq g, h \leq i$.

Para demostrar el teorema basta probar que cada par de conjuntos de esta colección son disjuntos, es decir, si $A_e \neq A_f$ son dos conjuntos de la colección antes construida, debemos probar que $A_e \cap A_f = \emptyset$ con $1 \leq e, f \leq i$ $e \neq f$. Supongamos que existe un elemento

$p \in A_e \cap A_f$, con $x_e := (a_e, b_e)$ y $x_f := (a_f, b_f)$ entonces $p = (a_e, \mu) = (a_f, \nu)$ para algunos $\mu, \nu \in \Gamma$. Pero de la igualdad podemos observar que $a_e = a_f$ lo que implica que x_e está en la segunda línea cartesiana de x_f lo que es una contradicción pues $A_e \neq A_f$.

Por lo tanto obtuvimos una partición del bloque A, por un lado el tamaño de A es k y por otro lado $A = \cup_{j=0}^{j=i} A_j$ y la cardinalidad de $\cup_{j=0}^{j=i} A_j$ es $i(r+1)$ pues son todos conjuntos disjuntos, por lo tanto $k = i(r+1)$ que era lo que se quería demostrar. □

En este caso tenemos lo siguiente, sea (x, A) la bandera del Teorema anterior, contemos la cantidad de banderas (y, C) tales que $x \in C$ y con y en la segunda línea cartesiana que pasa por x excluyendo a x.
Por un lado esta cantidad de banderas es el número de bloques que contienen a su vez a x y a elementos de la segunda línea cartesiana que pasa por x, digamos z, multiplicado por el número de elementos de la segunda línea cartesiana que pasa por x (excluyendo a x) que están en estos bloques, es decir, r, por lo tanto el número de banderas de está forma son zr. Por otro lado x y y están en λ bloques y hay $m-1$ puntos de la segunda línea cartesiana que pasa por x por lo que al contar la banderas (y, C) de esta forma obtenemos que son $\lambda(m-1)$. Así debemos tener que $zr = \lambda(m-1)$, pero se cumple que $kr = 2\lambda(m-1)$ por lo que $z = \frac{k}{2}$ y como z es entero, entonces k debe ser un número par. Es decir, la mitad de los bloques que contienen a x intersectan a la segunda línea cartesiana y la otra mitad de dichos bloques intersectan a la primer línea cartesiana, esto es dado que podemos repetir el procedimiento tomando ahora la primera línea cartesiana que pasa por x.

Tenemos el siguiente resultado al estudiar el caso restante.

Teorema: Caso 2. *Sea D un $(v, k, \lambda)-$ diseño simétrico admitiendo un grupo de automorfismos G primitivo y transitivo en banderas con una acción producto en P. Si para todo punto en el diseño, cada bloque que lo contiene intersecta a las dos líneas cartesianas que pasan por dicho punto entonces $\frac{r}{2} + 1$ divide a k.*

Demostración. Sea un punto $x = (a_0, b_0)$ arbitrario del diseño entonces por las hipótesis del teorema, cada bloque que contiene a x intersecta a las dos líneas cartesianas que pasan por x. Sea A un bloque que contiene a x, entonces hay r_1 elementos de la primera línea cartesiana

que pasa por x (excluyendo a x) en A y hay r_2 elementos de la segunda línea cartesiana que pasa por x (excluyendo a x) en A, r_1 y r_2 cumplen la relación $r = r_1 + r_2$, esto por el Lema 20.
Sea C algún otro bloque que contiene a x, por lo dicho antes, este intersecta a las dos líneas cartesianas que pasan por x. Como G actúa transitivamente en las banderas del diseño, entonces existe un elemento $g \in G$ tal que $g(x, A) = (x, C)$, de aquí observamos que $g(x) = x$, es decir, $g|_\Gamma$ fija a a_0 y a b_0.

Demostremos que el elemento g manda a los elementos de la primera línea cartesiana que pasa por x y que están en A a elementos de la primera línea cartesiana que pasa por x y que están en C, en efecto, sea un (μ, b_0) un elemento de la primera línea cartesiana que pasa por x y que además está en A, entonces $g(\mu, b_0) = (\nu, b_0) \in C$ para algún $\nu \in \Gamma$, esto último es consecuencia de que $g|_\Gamma$ fija a b_0. Análogamente tenemos que g manda a los elementos de la segunda línea cartesiana que pasa por x y que están en A a elementos de la segunda línea cartesiana que pasa por x y que están en C, en efecto, sea un (a_0, μ) un elemento de la segunda línea cartesiana que pasa por x y que además está en A, entonces $g(a_0, \mu) = (a_0, \nu) \in C$ para algún $\nu \in \Gamma$, esto último es consecuencia de que $g|_\Gamma$ fija a a_0. Por lo tanto tendremos que el bloque C tiene la misma cantidad de elementos de la primera línea cartesiana que pasa por x que A, así mismo C tiene la misma cantidad de elementos de la segunda línea cartesiana que pasa por x que A. Como C fue un bloque arbitrario que contiene a x, entonces tendremos la conclusión anterior para cada bloque que contiene a x.

Ahora contemos la cantidad de banderas (y, C) del diseño tales que y es un elemento de la primera línea cartesiana que pasa por x (excluyendo a x) y C un bloque que contiene a x. Por un lado, por lo que mencionamos antes, cada bloque contiene la misma cantidad de elementos de la primera línea cartesiana que pasa por x, r_1 si excluimos a x y hay k bloques que contienen a x y todos ellos intersectan a la primera línea cartesiana que pasan por x, por lo tanto hay kr_1 banderas de este tipo. Por otro lado y y x están en λ bloques y existen $m - 1$ elementos de la primera línea cartesiana que pasa por x (excluyendo a x), por lo que al contar las banderas de esta forma obtenemos $\lambda(m - 1)$.
Así obtenemos $kr_1 = \lambda(m - 1)$, pero se cumple por el Lema 20 que $kr = 2\lambda(m - 1)$ de donde

concluimos que $r_1 = \frac{r}{2}$. Además se debe cumplir que $r_1 + r_2 = r$ por lo que todos los bloques que contienen a x intersectan a la segunda línea cartesiana que pasa por x (excluyendo a x) en exactamente $r_2 = \frac{r}{2}$ puntos.

El elemento x fue un elemento arbitrario del diseño, entonces obtenemos la misma conclusión para cualquier punto del diseño, es decir, para cada elemento del diseño todos los bloques que lo contienen intersectan a la primera línea cartesiana que pasa por dicho punto (excluyendo a dicho punto) en $\frac{r}{2}$ elementos y en la misma cantidad para la segunda línea cartesiana que pasa por dicho punto (excluyendo a dicho punto).

Sea A_0 el conjunto de puntos de la segunda línea cartesiana que pasa por x que están en A incluido el propio x, la cardinalidad de dicho conjunto es $\frac{r}{2}+1$, sea un elemento $x_1 \in A - A_0$, entonces por lo dicho anteriormente A intersecta a la segunda línea cartesiana que pasa por x_1 en $\frac{r}{2}$ puntos, por lo tanto si A_1 es el conjunto de puntos de la segunda línea cartesiana que pasa por x_1 que están en A incluido x_1, entonces la cardinalidad de A_1 es $\frac{r}{2}+1$, ahora sea $x_2 \in A - (A_0 \cup A_1)$ igual que antes podemos construir A_2 como el conjunto de puntos de la segunda línea cartesiana que pasa por x_2 que están en A incluido x_2 y por lo dicho anteriormente la cardinalidad de dicho conjunto es de igual manera $\frac{r}{2}+1$.
De esta manera continuamos este proceso hasta que no haya mas puntos que tomar en A, así obtenemos una colección de puntos $x_0, x_1, ..., x_i \in A$ y una colección de conjuntos $A_0, A_1, ..., A_i$ para algún natural i, tal que A_j es la intersección de la segunda línea cartesiana que pasa por x_j con A por lo que A_j tiene cardinalidad $\frac{r}{2}+1$ para todo j. Además se cumple que $A = \cup_{j=0}^{j=i} A_j$ y por la construcción se tiene que si $x_g \neq x_h$ entonces $A_g \neq A_h$ con $1 \leq g, h \leq i$.

Para demostrar el teorema resta probar que cada par de conjuntos de esta colección son disjuntos, es decir, si $A_e \neq A_f$ son dos conjuntos de la colección antes construida, debemos probar que $A_e \cap A_f = \emptyset$ con $1 \leq e, f \leq i$ $e \neq f$. Supongamos que existe un elemento $p \in A_e \cap A_f$, con $x_e := (a_e, b_e)$ y $x_f := (a_f, b_f)$ entonces $p = (a_e, \mu) = (a_f, \nu)$ para algunos $\mu, \nu \in \Gamma$. Pero de la igualdad podemos observar que $a_e = a_f$ lo que implica que x_e está en la segunda línea cartesiana de x_f lo que es una contradicción pues $A_e \neq A_f$.

Por lo tanto obtuvimos una partición del bloque A, por un lado el tamaño de A es k y por otro lado $A = \cup_{j=0}^{j=i} A_j$ y la cardinalidad de $\cup_{j=0}^{j=i} A_j$ es $i(\frac{r}{2}+1)$ por lo tanto $k = i(\frac{r}{2}+1)$ que era lo que se quería demostrar. □

Luego obtenemos como consecuencia los siguientes resultados.

Corolario caso 2. 1. *Con las hipótesis del Teorema caso 2 tenemos que* $\frac{r}{2}+1$ *divide a* m.

Demostración. De (5.19) tenemos que podemos reescribirla como

$$k = \frac{r}{2}m + \frac{r}{2} + 1,$$

del caso 2 del teorema anterior, tenemos que existe un entero p tal que $k = p(\frac{r}{2}+1)$ sustituyendo en la ecuación anterior tendremos $(p-1)\left(\frac{r}{2}+1\right) = \frac{r}{2}m$ como $\left(\frac{r}{2}+1, \frac{r}{2}\right) = 1$ entonces $\frac{r}{2}+1$ divide a m. □

Corolario caso 2. 2. *Con las hipótesis del Teorema caso 2 tenemos que* $\frac{r}{2}+1$ *divide a* λ.

Demostración. Del Teorema caso 2 tenemos que existe un entero p tal que $k = p(\frac{r}{2}+1)$ sustituyendo esta y (5.19) en $k(k-1) = \lambda(m-1)(m+1)$ tenemos

$$p\frac{r}{2}\left(\frac{r}{2}+1\right) = \lambda(m-1)$$

pero del corolario anterior $\frac{r}{2}+1$ divide a m por lo que $\left(\frac{r}{2}+1, m-1\right) = 1$ y entonces $\frac{r}{2}+1$ debe dividir a λ. □

Y como t es el máximo común divisor de k y λ surge de manera natural el siguiente

Corolario caso 2. 3. *Con las hipótesis del Teorema caso 2 tenemos que* $\frac{r}{2}+1$ *divide a* t.

Demostración. Como $\frac{r}{2}+1$ divide a k y divide a λ y además $(k, \lambda) = t$ entonces se debe tener que $\frac{r}{2}+1$ divide a t. □

Ahora tenemos un caso muy particular en el que se obtienen los parámetros de un diseño de Menon, este surge como consecuencia del corolario anterior pues como $\frac{r}{2}+1$ divide a t, es natural investigar lo que sucede en el caso particular en que t es primo. Este es un primer acercamiento al problema central de este trabajo, este resultado es el siguiente:

Lema 28. *Si D es un $(v,k,\lambda)-$diseño simétrico con $(k,\lambda)=t>1$ con t un primo y $v=m^2$ con m par, admitiendo un grupo de automorfismos primitivo en puntos y transitivo en banderas G y se cumple que para todo punto del diseño cada bloque que contiene a dicho punto intersecta a sus dos líneas cartesianas , entonces G no tiene una acción producto no trivial o D es un diseño de Menon, es decir, tiene parámetros $(4t^2, 2t^2-t, t^2-t)$.*

Demostración. Del Corolario 3 del Teorema del caso 2 tenemos que $\frac{r}{2}+1$ divide a t pero como t es un número primo entonces $\frac{r}{2}=0$ o $\frac{r}{2}+1=t$.
Si $\frac{r}{2}=0$ entonces de (5.19) tenemos que $k-1=0$ lo que no puede ser.
Si $\frac{r}{2}+1=t$, entonces de $m=\frac{r^2+2r+4\lambda}{4\lambda-r^2}$ tenemos

$$m=\frac{bs^2+s+t}{t-bs^2} \tag{5.28}$$

de donde $t>bs^2$ pues si $t=bs^2$ entonces $\lambda=b^2s^2=\frac{r^2}{4}$ y sustituyendo en (5.18) tendremos

$$r^2(m+1)+2r-r^2(m-1)=0\Rightarrow r(r+1)=0$$

Es decir $r=0$ o $r=-1$ lo que no puede ser y por lo tanto $t>bs^2$.
Entonces $t=\frac{r}{2}+1=bs+1>bs^2$ entonces $1>bs(s-1)$ de donde tendremos $s=1$ y del Lema 26 tendremos que $v=4t^2$, $k=2t^2-t$ y $\lambda=t^2-t$ que era lo que se quería probar. □

Con estos resultados podemos estudiar lo que sucede con las ternas
$(4900,3267,2178)$, $(16900,2752,448)$ y $(44100,8019,1458)$ quienes nos impiden demostrar la conjetura para $v\leq(210)^2$ pues no cumplen las condiciones para ser diseños de Manon.

Lema 29. *Si D es un $(v,k,\lambda)-$diseño simétrico con $(k,\lambda)=t>1$ y $v=m^2\leq(210)^2$ con m par, admitiendo un grupo de automorfismos primitivo en puntos y transitivo en banderas G, entonces G no tiene una acción producto no trivial o se cumple alguna de las siguientes conclusiones:*

1. *D es un diseño de Menon, es decir, tiene parámetros $(4t^2, 2t^2-t, t^2-t)$*
2. *D tiene parámetros $(16900, 2752, 448)$.*

Demostración. Las ternas que se obtienen para $m\leq 210$ que no cumplen las condiciones de los diseños de Manon y la condición $k-\lambda$ es un cuadrado son $(4900,3267,2178)$, $(16900,2752,448)$

y $(44100, 8019, 1458)$ para los cuales $\frac{r}{2}+1$ vale respectivamente 47, 22 y 39 y ninguno de los tres cumplen el Teorema caso 2. Por otro lado $r+1$ es $93, 43, 78$ respectivamente. La primera y la tercera terna no cumplen el Teorema caso 1, pero la terna $(16900, 2752, 448)$ si lo cumple por lo cual es la única terna posible para $m^2 \leq (210)^2$. Notémos que para esta terna k es par lo que es congruente con lo dijimos al caer en este caso, además al hacer cálculos obtenemos que $s = 3$ y del Lema 26 sabemos que esta terna no puede ser un diseño de Menon. □

Esta terna, $(16900, 2752, 448)$, como dijimos no es un diseño de Menon pues $s = 3$, pero cumple todas las condiciones aritméticas. Por lo que esta terna nos da la pauta para pensar que cuando estamos en el caso en el que en el diseño, los bloques que contienen a un punto intersecten a una sola línea cartesiana que pasa por dicho punto, no se obtendrá necesariamente un diseño de Menon y con ello ser un posible contraejemplo a la generalización de lo que Tian y Zhou obtienen en su artículo, acerca de que cuando estudiaron el caso $l = 2$ los diseños que resultan son los de Manon .

Estamos en condiciones de dar nuestro resultado central, el cual considera los dos casos ya mencionados. En un caso obtenemos como conclusión directa los diseños de Menon, esta demostración es similar a la demostración que se hace del caso en que $m-1$ es una potencia de primo impar. Es decir, en ese sentido es una generalización de esa demostración sin embargo, por la existencia ahora del parámetro s en las condiciones aritméticas, esa generalización no se daba de manera natural. Para ello necesitamos de una condición aritmética extra para poder dar una demostración análoga a la del Lema 27, y esa condición la encontramos en el Corolario 3 del Teorema caso 2.

Por otro lado, en el caso restante obtenemos una condición aritmética sobre el parámetro a y por lo tanto sobre k. Dado que existe una terna que no es un diseño de Menon entonces este caso no concluye en la obtención de diseños de Manon y con ello podemos pensar que no se pueden obtener los diseños de Menon para un λ arbitrario cuando estudiamos la acción producto en los diseños simétricos que admiten un grupo de automorfismos primitivo y transitivo en banderas en el caso $l = 2$. Además este caso nos da una parametrización de v, k, λ en términos de t y s que se reduce a los diseños de Menon cuando $s = 1$.

Es decir el siguiente teorema nos da una parametrización en términos de t y s que generaliza la parametrización de los diseños de Menon, estos nuevos posibles diseños son los que surgen con las hipótesis de considerar un diseño simétrico admitiendo un grupo de automorfismos primitivo y transitivo en banderas que tiene la acción producto, restringiéndonos al caso en el que $v = m^2$ con m un número par.

Teorema 5. *Si D es un $(v, k, \lambda)-$diseño simétrico con $(k, \lambda) = t > 1$ y $v = m^2$ con m par, admitiendo un grupo de automorfismos primitivo en puntos y transitivo en banderas G, entonces G no tiene una acción producto no trivial o D es un diseño con parámetros $\left((2t+s-1)^2, \frac{2t^2-(2-s)t}{s}, \frac{t^2-t}{s^2}\right)$ con $s \geq 1$ impar .*
Cuando $s = 1$ se obtienen los diseños de Menon y si $s > 1$ entonces t es par.

Demostración. Con las hipótesis del teorema y tomando en cuenta el Lema 20 tenemos dos posibles casos, cuando para cualquier punto todos los bloques que lo contienen intersectan a las dos líneas cartesianas que pasan por dicho punto y el caso contrario, cuando existe un punto para el cual los bloques intersectan a una sola línea cartesiana que pasa por ese punto. Tomemos en cuenta que esto último implica que para todos los puntos todos los bloques que lo contienen intersectan a una sola línea cartesiana.
En este último caso, se cumple el Teorema caso 1, es decir se debe cumplir que $r + 1$ divide a k con r un número entero mayor que uno tal que $kr = 2\lambda(m-1)$. Además se debe cumplir que $k - 1 = \frac{r}{2}(m+1)$ de donde obtenemos $k = \frac{r}{2}m + \frac{r}{2} + 1$. Por lo dicho antes, existe un entero p tal que $k = p(r+1)$ haciendo la sustitución obtenemos:

$$m - 1 = (r+1)(m+1-2p)$$

Entonces $r+1$ divide a $m-1$, pero $m-1 = as = x(r+1)$ con $x := m+1-2p$, como $r = 2bs$ entonces $(r+1, s) = 1$ de donde tenemos que $r+1$ debe dividir al parámetro a. Por otro lado sabemos que $m - 1 = \frac{2bs+1}{t-bs^2}s = \frac{r+1}{t-bs^2}s$ y como $m - 1 = as$ entonces $a = \frac{r+1}{t-bs^2}$, es decir, $r + 1 = a(t - bs^2)$, a divide a $r + 1$. Por lo tanto, dado que $r + 1$ divide a a y a divide a $r + 1$ se debe tener que $r + 1 = a$, de donde $k = (r + 1)t$.

Al obtener esto tenemos que $t - bs^2 = 1$ de donde $b = \frac{t-1}{s^2}$ y con esto obtenemos los parámetros $\lambda = \frac{t-1}{s^2}t$, $k = \frac{2t+s-2}{s}t$, $v = (2t + s - 1)^2$. Por lo dicho en el Teorema caso 1, k debe

ser par y como $r+1$ es impar, entonces t debe ser par. Luego, como $m = 2t + s - 1$ y m es par entonces s debe ser impar. La terna $(16900, 2752, 448)$ cumple con las condiciones sobre v, k, λ obtenidas, con $t = 64$ y $s = 3$, es decir, no es un diseño de Manon.

Notémos que cuando $s = 1$ se obtienen las ternas de los diseños de Manon con t par.

Analicemos el caso restante, es decir, cuando para cada punto del diseño todos los bloques que lo contienen intersectan a las dos líneas cartesianas que pasan por dicho punto, entonces se cumple el Teorema caso 2 y del Corolario 3 de dicho Teorema tenemos que existe un $x > 1$ tal que:

$$t = \left(\frac{r}{2} + 1\right) x = (bs + 1)x \tag{5.29}$$

Luego de (5.28) tenemos que $m = \frac{s(bs+1)+t}{t-bs^2} = \frac{s(bs+1)+(bs+1)x}{t-bs^2}$ es decir tendremos

$$m = \left(\frac{s+x}{t-bs^2}\right)\left(\frac{r}{2}+1\right) \tag{5.30}$$

Usando (5.29) podemos escribir

$$t - bs^2 = x + bs(x - s) \tag{5.31}$$

Así tenemos los siguientes casos

1. $x < s$

   En el Lema 28 vimos que $t - bs^2 > 0$ y de (5.31) tenemos $x > bs(s - x) > bx(s - x)$ entonces $1 > b(s - x) > 0$ pues $x < s$, lo que no puede ser pues $b(s - x)$ es un entero.

2. $s < x$

   De (5.30) tenemos que $s + x \geq t - bs^2$ pero si $s + x = t - bs^2$ entonces de (5.30) $m = \frac{r}{2} + 1$ de donde $as = m - 1 = \frac{r}{2} = bs$ entonces $a = b$ pero $(a, b) = 1$ entonces $a = 1$ lo que no puede ser por el Lema 24, con lo que entonces $s + x > t - bs^2$ y de (5.31) $s + x > x + bs(x - s)$ de donde $1 > b(x - s) > 0$ lo que no puede ser pues $b(x - s)$ es entero.

3. $s = x$

   Si $s = x$ de (5.29) tenemos que s divide a t, pero de (5.19) tenemos que $at - bs(as+2) = 1$,

es decir, $(t, s) = 1$ por lo tanto $s = 1$ y del Lema 26 tenemos que $v = 4t^2$, $k = 2t^2 - t$ y $\lambda = t^2 - t$

Con ello obtenemos la conclusión del teorema cuando $s = 1$, es decir, cuando caemos en este caso se deben obtener los diseños de Manon, esto para toda $t > 1$ y así terminamos la demostración. □

Del Teorema anterior observamos que si bien hay un caso en el que se obtienen los diseños de Menon, estas no son las únicas ternas que se pueden obtener al suponer que el diseño y su grupo de automorfismos tienen la acción producto. Hay más ternas que surgen de considerar el caso en que los bloques que contienen a un punto intersecten a una sola línea cartesiana.

Como vimos la terna $(16900, 2752, 448)$ es un ejemplo de ello pues es una terna que cumple con todas las condiciones aritméticas y que no es un diseño de Menon. Por lo tanto podemos pensar que la idea de obtener solo diseños de Manon al considerar la acción producto puede no cumplirse pues esta terna es un posible contraejemplo. Sin embargo obtuvimos una generalización de lo hecho por Tian y Zhou, pues con este Teorema damos expresiones explicitas de los parámetros v, k, λ que en el caso $s = 1$ se reducen a los diseños de Menon.

5.1.2. Caso general $l \geq 2$

Además del resultado anterior, en el proceso de buscar una solución al problema obtuvimos el siguiente lema, el cual se puede generalizar de manera natural para cualquier l.

Lema 30. *Si D es un $(v, k, \lambda)-$diseño simétrico con $v = m^2$, admitiendo un grupo de automorfismos primitivo en puntos y transitivo en banderas G con una acción producto no trivial entonces el diseño complemento no es transitivo en banderas.*

Demostración. Supongamos que el diseño complemento es transitivo en banderas, entonces sus parámetros son $(v', k', \lambda') = (v, v-k, v-2k+\lambda)$ por lo tanto se debe cumplir (2.1) para estos parámetros, es decir, se debe cumplir

$$(v-k)(v-k-1) = (v-2k+\lambda)(m-1)(m+1). \tag{5.32}$$

Luego como D tiene un grupo de automorfismos G primitivo, entonces el diseño complemento D' tiene el mismo grupo de automorfismos primitivo G y podemos hacer la misma construcción de las líneas cartesianas que pasan por un punto x que se hizo para D en el Lema 20, pues G es transitivo en los puntos de D', así que se debe cumplir también que k' divida a $\lambda' l(m-1)$, es decir debe existir un entero p tal que

$$(v-k)p = 2(v-2k+\lambda)(m-1) \tag{5.33}$$

Sustituyendo en (5.32) tenemos

$$2(v-k)(v-1-k) = (v-k)p(m+1) \Rightarrow 2((m-1)(m+1)-k) = p(m+1)$$

de donde obtenemos

$$2k = q(m+1) \tag{5.34}$$

con $q = 2(m-1) - p > 0$.
Sustituyendo (5.34) en (5.19) tenemos

$$q(m+1) - 2 = r(m+1) \Rightarrow (q-r)(m+1) = 2$$

esto implica que $m+1 = 1$ o $m+1 = 2$ lo cual no puede ser pues $m \geq 5$. □

Generalizando el lema anterior para una l arbitraria tenemos el siguiente

Teorema 6. *Si D es un $(v,k,\lambda)-$diseño simétrico con $v=m^l$, admitiendo un grupo de automorfismos primitivo y transitivo en banderas G con una acción producto no trivial entonces el diseño complemento no es transitivo en banderas.*

Demostración. Supongamos que el diseño complemento es transitivo en banderas, entonces sus parámetros son $(v',k',\lambda')=(v,v-k,v-2k+\lambda)$ por lo tanto se debe cumplir (2.1) para estos parámetros, es decir, se debe cumplir

$$(v-k)(v-k-1)=(v-2k+\lambda)(m-1)(m^{l-1}+m^{l-2}+...+1). \tag{5.35}$$

Luego como D tiene un grupo de automorfismos G primitivo, entonces el diseño complemento D' tiene el mismo grupo de automorfismos primitivo G y podemos hacer la misma construcción de las líneas cartesianas que pasan por un punto x que se hizo para D en el Lema 20, pues G es transitivo en los puntos de D', así que se debe cumplir también que k' divida a $\lambda' l(m-1)$, es decir debe existir un entero p tal que

$$(v-k)p=l(v-2k+\lambda)(m-1) \tag{5.36}$$

Sustituyendo en (5.35) tenemos

$$\begin{aligned} l(v-k)(v-1-k)&=(v-k)p(m^{l-1}+m^{l-2}+...+1)\\ \Rightarrow l((m-1)(m^{l-1}+m^{l-2}+...+1)-k)&=p(m^{l-1}+m^{l-2}+...+1)\end{aligned}$$

de donde obtenemos

$$lk=q(m^{l-1}+m^{l-2}+...+1) \tag{5.37}$$

con $q=l(m-1)-p>0$.

Ahora como para D se cumple $k=\frac{l\lambda(m-1)}{r}$ y $k(k-1)=\lambda(v-1)$ entonces tenemos

$$k(k-1)=\frac{kr}{l(m-1)}(m^l-1)$$

de donde tenemos la generalización de (5.19)

$$l(k-1)=r(m^{l-1}+m^{l-2}+...+1) \tag{5.38}$$

por lo tanto sustituyendo (5.37) en (5.38) tendremos

$$\begin{aligned} q(m^{l-1}+m^{l-2}+...+1)-l&=r(m^{l-1}+m^{l-2}+...+1)\\ \Rightarrow (q-r)(m^{l-1}+m^{l-2}+...+1)&=l\end{aligned}$$

con lo que $m^{l-1} + m^{l-2} + ... + 1 \leq l$ lo que implica que $m \leq 1$ pues si $m > 1$ entonces $l \geq m^{l-1} + m^{l-2} + ... + 1 > l$, lo que no puede ser.

Por lo tanto $m \leq 1$ pero esto es una contradicción pues $m \geq 5$ y entonces se tiene que no existe tal diseño y con ello lo que se deseaba probar $\square$

Bibliografía

[1] Z.X. Wan, Design Theory, Higher Education Press and World Scientific, 2009, 221 pp.

[2] E. O'Reilly Regueiro, On primitivity and reduction for flag-transitive symmetric designs, Journal of Combinatorial Theory, Series A 109 (1), 135-148.

[3] Martin W. Liebeck, Cheryl E. Praeger y Jan Saxl, On the O'Nan-Scott theorem for finite primitive permutation groups. J. Austral. Math. Soc. (series A) 44 (1988), 389-396.

[4] Delu Tian and Shenglin Zhou, Flag-transitive point-primitive symmetric (v, k, λ) designs with at most 100, Journal of combinatorial designs, 21: 127-141.

[5] Y.J Ionin and T. van Trung, Symmetric designs, in handbook of combinatorial designs, C.J. Colbourn and J.H. Dinitz (editors), Chapman Hall/CRC, Boca Raton, 2007, pp. 110-124.

[6] I.N. Herstein, Algebra moderna,Editorial Trillas,1990, 392 pp.

[7] The GAP Group, GAP-Groups, Algorithms, and Programming, Version 4.3; 2002, http://www.gap-system.org.

[8] M.P. Shutzenberg, A nonexistence theorem for an infinite family of symmetrical block designs, Ann. Eugen. 14 (1949)286-287.