Universidad de Valladolid

Facultad de Ciencias

Trabajo de Fin de Grado

Grado en MATEMÁTICAS

Construcción de ciertos diseños combinatorios denominados BIBD

Autor: Enrique González Manrique

Tutor: José Enrique Marcos

2021

Índice general

Introducción

La teoría de diseños combinatorios tiene como objetivo poner orden en situaciones de supuesto caos. Dado un conjunto, los diseños combinatorios tratan, utilizando distintos métodos, de organizar y ordenar dicho conjunto ajustándose a una serie de reglas.

En un primer lugar, los diseños combinatorios aparecen en las matemáticas recreativas como, por ejemplo, en el famoso problema de las colegialas de Kirkman. A pesar de que en los siglos XVIII y XIX ya se estaba trabajando en los diseños combinatorios, es en el siglo XX cuando este campo emerge como una disciplina por sí sola en las matemáticas. Esta labor se debe principalmente a Ronald Fischer, y posteriormente a Raj Chandra Bose, que asienta las bases de la teoría de diseños combinatorios (véase [4]). A partir de este momento, esta teoría avanza rápidamente debido a las profundas conexiones que tiene con la geometría, el álgebra y la teoría de números.

Aunque en este trabajo nos hemos centrado en la construcción de diseños combinatorios, cabe resaltar que en este campo se pueden encontrar numerosas aplicaciones en diseño de experimentos, criptografía, computación y estadística (véase [9], [20]). En muchos experimentos, el número de casos y tratamientos que se quieren comparar es muy alto y, por tanto, compararlos de uno en uno puede suponer un gasto de recursos y trabajo muy grande. Gracias a los diseños combinatorios, podemos organizar los distintos tratamientos de manera que el coste del experimento sea menor. Por ejemplo, imaginemos que se está estudiando el efecto de veinte medicinas aplicadas a unos pacientes con una enfermedad rara. Si hiciéramos el experimento administrando una medicina a cada paciente y comparando con los demás, nos haría falta un gran número de pacientes para obtener un resultado concluyente. Sin embargo, organizando el experimento acorde con un diseño combinatorio, se pueden distribuir varias medicinas a cada paciente. De esta manera, se requieren menos pacientes y, gracias a esta distribución, podríamos comparar el efecto de cada medicina utilizando menos recursos.

En este trabajo nos centramos en los BIBD (“ *Balanced Incomplete Block Design* ”). Estos diseños se ocupan de organizar un conjunto en subconjuntos de un mismo tamaño, denominados *bloques*, de manera que dos elementos cualesquiera distintos del conjunto estén simultáneamente en un mismo número de bloques.
Los BIBD más sencillos, que más han sido estudiados y de los que más información se posee son los *sistemas triples de Steiner*, que tienen bloques de tamaño 3. Por esa razón, en este trabajo hemos decidido centrarnos en los BIBD de tamaño 4, de los cuales se posee menos información pero, a su vez, se pueden encontrar interesantes ejemplos y métodos para construir BIBD.

Este trabajo ha sido dividido en 5 partes o capítulos:

Comenzamos explicando en primer lugar los BIBD más sencillos, los *sistemas triples de Steiner*.

A continuación, se introducen de una manera general los BIBD y se exponen varios ejemplos ilustrativos para empezar a entender y familiarizarnos con estos diseños. También se estudia cómo representar los BIBD, ya sea gráficamente o con su *matriz de incidencia*.

En el segundo capítulo estudiamos las *familias de diferencias*, unas familias de conjuntos que nos ayudan a lo largo de todo el trabajo en el desarrollo y la construcción de BIBD.

En el tercer y cuarto capítulo profundizamos en los $(v, 4, 1)$-BIBD, es decir, en los diseños con bloques de tamaño 4 y donde cada par de elementos distintos está contenido exactamente en un único bloque. Mientras que en un primer lugar trabajamos en conjuntos con un tamaño concreto, después nos centramos en construcciones inductivas, es decir, tratamos de construir nuevos BIBD a partir de otros. En este cuarto capítulo aparecen unos nuevos diseños, los *transversal design*, los cuales se aplican también en la construcción de nuevos BIBD.

Hasta este momento el trabajo se centra en los diseños donde cada par de elementos distintos está contenido en un único bloque. Por ello, y para poder hacernos una idea de otros BIBD, en el último capítulo se introducen los $(v, 4, 2)$-BIBD y los $(v, 4, 3)$-BIBD, es decir, los BIBD con bloques de tamaño 4 donde cada par de elementos distintos está contenido exactamente en dos y en tres bloques, respectivamente.

Por último, debido a que algunas comprobaciones sobre las familias de diferencias no se pueden hacer a simple vista, se ha añadido un Apéndice en el que se muestra un programa de Matlab que nos ayuda a resolver este problema.

Aparte de la gran contribución de Bose a esta disciplina y a mi trabajo, quiero resaltar, dentro de la bibliografía, *" The CRC Handbook of combinatorial designs "*, libro escrito por C. J. Colbourn y J. H. Dinitz (véase [7]). Se trata de un manual que estudia una amplia variedad de diseños combinatorios así como una gran cantidad de ejemplos, y el cual ha resultado de gran ayuda en este trabajo, tanto en la construcción de BIBD como en el desarrollo de familias de diferencias. Cabe resaltar la medalla Euler que fue entregada a Colbourn en 2004 por sus importantes aportaciones en el campo de la combinatoria. A Dinitz, por su parte, se le atribuye la conjetura de Dinitz, un resultado sobre cuadrados latinos también incluido en el campo de la combinatoria.

Capítulo 1

Introducción a los BIBD

En este primer capítulo empezaremos abordando un ejemplo básico e importante de BIBD, los *sistemas triples de Steiner*. Veremos varias construcciones y resultados para adentrarnos en estos diseños y así poder después estudiar otros BIBD más complejos. Para escribir este capítulo hemos utilizado las definiciones y los resultados más básicos obtenidos mayormente de [14] y [18].

1.1. Sistemas triples de Steiner

Los sistemas triples de Steiner son los diseños más sencillos dentro de los BIBD, también son los mejor estudiados y de los que más información podemos encontrar en el campo de los diseños combinatorios.

Definición 1.1.1. *Un* ***sistema triple de Steiner*** *es un conjunto V de v elementos y una familia $\mathcal{B}$ de ternas de V de manera que, dados dos elementos distintos $x, y \in V$, existe una única terna de la familia tal que x e y pertenecen a esa terna.*

Las ternas son conjuntos de tres elementos y, a veces, también las denominamos bloques.
Un sistema triple de Steiner se denota como STS(v), S(2, 3, v) sistema de Steiner o también como un $(v, 3, 1)$-BIBD.

Ejemplo 1.1.2. Dado el conjunto $V = \{1, 2, 3, 4, 5, 6, 7\}$ y la familia de ternas

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

obtenemos un $STS(7)$. Este es un ejemplo característico, ya que si tomamos cada elemento de V como un punto y las ternas como rectas o circunferencias, con su representación gráfica obtenemos el *plano proyectivo de Fano* (véase Figura 1.1).

En el ejemplo del plano proyectivo de Fano apreciamos que cada par de puntos distintos está unido por una única recta o circunferencia, y que cada recta o circunferencia solo abarca tres puntos, que representan las ternas. Veamos ahora otro ejemplo con un conjunto mayor.

Ejemplo 1.1.3. Sea ahora el conjunto $V = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13\}$. Para elegir las ternas utilizamos un método alfabético como en un diccionario, empezando por la terna con los

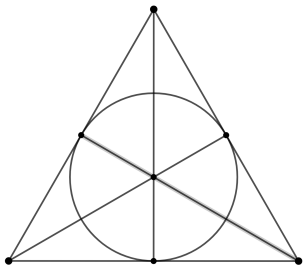


Figura 1.1: Plano proyectivo de Fano

números más pequeños posibles y aumentando progresivamente, siempre comprobando que dos elementos distintos no estén a la vez en dos ternas distintas, sino en una única.

$$\mathcal{B} = \{\ \{1,2,3\}, \{1,4,5\}, \{1,6,7\}, \{1,8,9\}, \{1,10,11\}, \{1,12,13\}, \{2,4,6\}, \{2,5,7\},$$
$$\{2,8,10\}, \{2,9,12\}, \{2,11,13\}, \{3,4,8\}, \{3,5,12\}, \{3,6,10\}, \{3,7,11\}, \{3,9,13\},$$
$$\{4,7,9\}, \{4,10,13\}, \{4,11,12\}, \{5,6,13\}, \{5,8,11\}, \{5,9,10\}, \{6,8,12\},$$
$$\{6,9,11\}, \{7,8,13\}, \{7,10,12\}\ \}$$

En las dos siguientes proposiciones veremos cómo calcular dos importantes propiedades de los sistemas triples de Steiner: el número de ternas o bloques en los que está contenido cada elemento y el número total de bloques.

Proposición 1.1.4. *Sea (V, $\mathcal{B}$) un STS(v). Entonces cada elemento $x \in V$ está contenido exactamente en $r = \frac{v-1}{2}$ ternas. Este es el* ***número de replicación****.*

Demostración. Fijamos un elemento $x \in V$. Las ternas en las que se encuentra x son de la forma $\{x, a, b\}$, con $a, b \in V$. Cada par de elementos distintos está simultáneamente en una única terna, luego cada par de elementos determina una terna. Tenemos $v - 1$ posibilidades de escoger el elemento a. Nos encontramos con que escoger a y la terna en la que aparece a y está b es lo mismo que escoger b y la terna en la que aparece b y está a, luego tenemos que dividir entre 2 a $v - 1$ y se obtiene finalmente $r = \frac{v-1}{2}$.

□

Proposición 1.1.5. *Sea (V, $\mathcal{B}$) un STS(v). Hay exactamente $b = \frac{v(v-1)}{6}$ ternas. Este es el* ***número de bloques****.*

Demostración. Cada par de elementos a, b de V están simultáneamente en una única terna, es decir, cada par de elementos distintos determina una terna. Luego para calcular el número de ternas se tiene $\binom{v}{2}$, que son las formas de coger 2 elementos de V (que contiene v elementos). Por otra parte, dada la terna $\{a, b, c\}$ hay que dividir entre $\binom{3}{2}$, ya que éstas son las combinaciones de

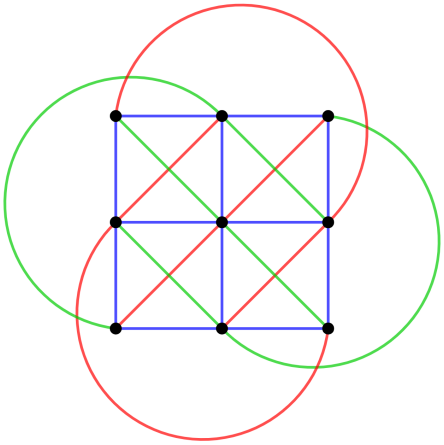


Figura 1.2: Plano afin $\mathbb{F}_3^2$

coger 2 elementos de la terna, es decir, (a, b), (a, c) ó (b, c). Por tanto, obtenemos el resultado que buscábamos:

$$b = \frac{\binom{v}{2}}{\binom{3}{2}} = \frac{\frac{v(v-1)}{2}}{3} = \frac{v(v-1)}{6}$$

□

Nótese, que operando con los dos resultados anteriores, obtenemos que $3b = rv$.
Observemos ahora otro ejemplo de STS relacionado con una representación gráfica.

Ejemplo 1.1.6. Vamos a relacionar el plano afín $\mathbb{F}_3^2 = \{(a, b) \ : \ a, b \in \mathbb{Z}/(3)\}$ con un $STS(9)$. De nuevo, los puntos se identifican con los elementos y las rectas con las ternas. Hay dos tipos de rectas:

- $y = ax + b, \quad a, b \in \mathbb{Z}/(3)$.
- $x = c, \quad c \in \mathbb{Z}/(3)$.

Del primer tipo de rectas tenemos $3 \cdot 3 = 9$ rectas y del segundo tipo tenemos 3 rectas posibles, luego 12 en total. Comprobamos que se cumple la fórmula de $b = \frac{9(9-1)}{6} = 12$. Gráficamente, en la Figura 1.2, observamos que también se cumple que cada punto está incluido en $r = \frac{9-1}{2} = 4$ rectas o ternas.

- Las rectas verticales $x = c$, e horizontales $y = b$ están en azul.
- Las rectas $y = x + b$ están en rojo.
- Las rectas $y = 2x + b$ están en verde.

No se pueden construir sistemas triples de Steiner para cualquier v, comprobémoslo en el siguiente teorema.

Teorema 1.1.7. *Si un STS(v) existe, entonces* $v \equiv 1$ *ó* $3 \mod (6)$.

Demostración. Por las proposiciones anteriores tenemos, en primer lugar, $r = \frac{v-1}{2}$, luego $v = 2r+1$, es decir, v impar. Por otra parte, $b = \frac{v(v-1)}{6}$, y como b es un entero entonces $v(v-1) \equiv 0 \mod (6)$. Esto se satisface si y solo si $v \equiv 0,\ 1,\ 3$ ó $4 \mod (6)$. Finalmente, como teníamos v impar, concluimos que $v \equiv 1$ ó $3 \mod (6)$.

□

Luego tenemos que v no sólo es siempre impar en los sistemas triples de Steiner, sino que v es igual a $6t+1$ ó a $6t+3$ para cada $t \in \mathbb{N}$.

A partir del ejemplo anterior construyamos ahora un $STS(3^n)$.

Ejemplo 1.1.8. Dado el espacio afín $(\mathbb{F}_3)^n$, tomemos de nuevo como ternas las rectas, que en este caso se denotan como $\{p + \lambda\vec{u} \ :\ p \in (\mathbb{F}_3)^n,\ u \in (\mathbb{F}_3)^n,\ \lambda \in \mathbb{F}_3\}$, siendo p un punto y $\vec{u}$ el vector dirección. Como $\lambda \in \mathbb{F}_3$, tenemos solo tres valores posibles para λ y, además, cada recta contiene 3 puntos que forman la terna.
Veámoslo de otra manera, las ternas del STS son los subconjuntos $\{x, y, z\} \subseteq (\mathbb{F}_3)^n$ tales que $x + y + z = \bar{0}$.
Comprobemos ahora que es un STS. Dados $x, y \in (\mathbb{F}_3)^n$ distintos, defino z como el elemento tal que $x + y + z = \bar{0}$. Ahora solo nos falta comprobar que $z \neq x$ e $z \neq y$. Razonemos por reducción al absurdo, supongamos que $z = x$ (los dos casos son análogos). Tenemos que

$$\bar{0} = x + y + z = 2x + y = -x + y$$

Luego obtenemos $x = y$, lo cual es absurdo al haber supuesto en un principio x e y distintos. Por lo tanto, $z \neq x$ e $z \neq y$. Es decir, hemos construido un $STS(3^n)$ a partir de espacio afín $(\mathbb{F}_3)^n$.

Ejemplo 1.1.9. En este ejemplo vamos a definir un $STS(2^n - 1)$ a partir del conjunto $V = (\mathbb{F}_2)^n \setminus \{\bar{0}\}$.
En primer lugar, tenemos que tanto en $(\mathbb{F}_2)^n$ como en $\mathbb{F}_2$ todo elemento x cumple que $2x = x+x = 0$. Luego en el grupo conmutativo $((\mathbb{F}_2)^n, +)$ de 2^n elementos todos los elementos salvo el neutro son de orden 2.
Definimos las ternas del STS, que son de la forma $\{x, y, z\} \subseteq V$ tales que $x + y + z = \bar{0}$. Comprobemos que tenemos realmente un STS:
Dados $x, y \in V$ distintos, definimos $z = x + y$. Tenemos que $z \neq \bar{0}$, ya que $x \neq y$ y hemos visto antes que $x + y = \bar{0}$ si y solo si $x = y$, por ser elemento de orden 2. Luego tenemos $z \in V$, y en este conjunto tenemos que $z = -z$. Como teníamos $z = x + y$, entonces ahora obtenemos que $x + y + z = \bar{0}$. Para comprobar que es una terna válida solo nos queda ver que $z \neq x$ e $z \neq y$. Si fuera $z = x$ (ambos casos son análogos), tendríamos

$$\bar{0} = x + y + z = x + y + x = y$$

Hemos llegado a un absurdo, ya que $y \in V = (\mathbb{F}_2)^n \setminus \{\bar{0}\}$. Por lo tanto, hemos encontrado tres

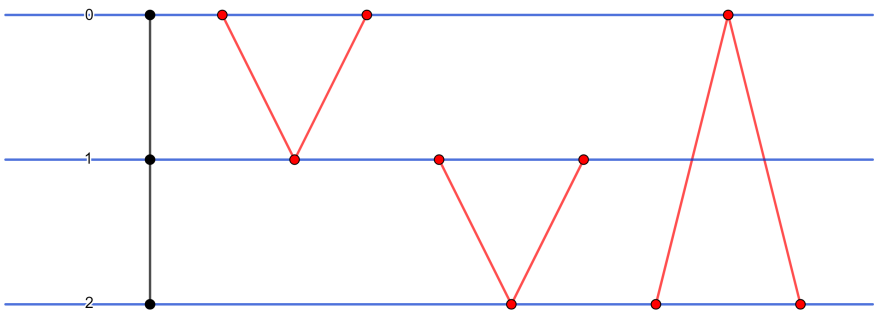


Figura 1.3: Tipos de ternas en $G \times \mathbb{Z}/(3)$.

elementos $\{x, y, z\}$ distintos de 0 y distintos entre sí, es decir, hemos comprobado que las ternas del conjunto V de $2^n - 1$ elementos son válidas y construyen nuestro $STS(2^n - 1)$.

Observemos ahora tres resultados en los que, a partir del producto de grupos, construiremos distintos STS. Este tipo de diseños nos serán útiles en capítulos posteriores, en los que desarrollaremos distintas construcciones inductivas para BIBD más complejos.

Teorema 1.1.10. *Sea $n = 2t + 1$ un número impar, $(G, +)$ un grupo conmutativo de orden n y $(\mathbb{Z}/(3), +)$ el grupo de tres elementos. Consideramos el grupo $(G \times \mathbb{Z}/(3), +)$.*
Entonces existe un $STS(6t + 3)$.

Demostración. Tenemos que el orden del grupo G es $2t + 1$ impar, luego el orden del grupo $V = G \times \mathbb{Z}/(3)$ es $3(2t + 1) = 6t + 3$.
Las ternas, que se pueden observar en la Figura 1.3, son de la siguiente forma:

- $\{(x, \bar{0}), (x, \bar{1}), (x, \bar{2})\}$ para cada $x \in G$.
- $\{(x, i), (y, i), (\frac{x+y}{2}, i + 1)\}$ para cada $x, y \in G$, $x \neq y$, $i \in \mathbb{Z}/(3)$.

Sea $x \in G$. Como G tiene orden impar, la expresión $\frac{x}{2}$ tiene sentido y $\frac{x}{2} = y \in G$ es el elemento tal que $y + y = x$. Otra comprobación necesaria, para que los dos tipos de ternas no solapen dos elementos y podamos construir un STS válido, es la siguiente:

Dados $x, y \in G$, $x \neq y$, tenemos que comprobar que $\frac{x+y}{2} \neq x$, que nos dará el caso análogo $\frac{x+y}{2} \neq y$. Razonemos por reducción al absurdo. Supongamos que $\frac{x+y}{2} = x$, entonces tendríamos $x+y = 2x$ y consecuentemente $x = y$, lo cual es absurdo por la hipótesis $x \neq y$. Esta comprobación es necesaria, ya que si tuviéramos $\frac{x+y}{2} = x$ y el caso $i = 0$, los dos tipos de ternas nos quedarían de la siguiente forma:

$$\{(x, \bar{0}), (x, \bar{1}), (x, \bar{2})\}, \quad \{(x, \bar{0}), (y, \bar{0}), (x, \bar{1})\}.$$

Lo cual no es válido, ya que ambas ternas tienen los elementos $(x, \bar{0}), (x, \bar{1})$.
Por último, para ver que es un STS, falta comprobar que si tenemos dos elementos $\alpha, \beta \in V$ distintos, entonces existe un único elemento $\gamma \in V$ tal que $\{\alpha, \beta, \gamma\}$ es una terna.

- Si $\alpha = (x, i)$, $\beta = (x, j)$ con $i \neq j$, solo queda el caso único $\gamma = (x, k)$ con k distinto de i e j.
- Si $\alpha = (x, i)$, $\beta = (y, j)$ con $x \neq y$, tenemos dos casos. Si $i = j$, vemos que la única opción posible es coger $\gamma = (\frac{x+y}{2}, i + 1)$. Si $i \neq j$, en primer lugar puedo suponer $j = i + 1$, porque sino se daría el caso análogo $i = j+1$. Entonces γ tiene que ser de la forma (z, i) con $\frac{x+z}{2} = y$, es decir, $z = 2y - x$. Como queríamos, z es único, ya que si $z = x$ obtenemos $x = 2y - x$ y $x = y$, absurdo por hipótesis.

Por tanto, hemos probado que dados dos elementos de la terna, existe un tercer elemento único que completa la terna. Además, como el cardinal de V hemos visto que es $6t+3$, hemos construido nuestro $STS(6t + 3)$. Nótese que este STS tiene un v de la forma $v \equiv 3 \mod (6)$. □

El siguiente resultado general nos da una interesante construcción de cómo, a partir de dos STS definidos sobre dos conjuntos, crear un nuevo STS definido sobre el producto de dichos conjuntos.

Proposición 1.1.11. *Sea un $STS(v_1)$ definido sobre un conjunto V_1, y sea un $STS(v_2)$ definido sobre otro conjunto V_2. Entonces existe un $STS(v_1 \cdot v_2)$ definido sobre $V_1 \times V_2$.*

Demostración. Definimos los bloques del $STS(v_1v_2)$ sobre $V_1 \times V_2$ de la siguiente forma :

$$\{(x_1, y_1), (x_2, y_2), (x_3, y_3)\},$$

donde se tiene que cumplir una de las siguientes propiedades:

- $x_1 = x_2 = x_3$ con $\{y_1, y_2, y_3\}$ bloque del $STS(v_2)$.
- $y_1 = y_2 = y_3$ con $\{x_1, x_2, x_3\}$ bloque del $STS(v_1)$.
- $\{x_1, x_2, x_3\}$ bloque del $STS(v_1)$ y $\{y_1, y_2, y_3\}$ bloque del $STS(v_2)$.

Vemos que hemos contruido un $STS(v_1v_2)$, ya que tenemos v_1v_2 elementos y en cada bloque tenemos tres elementos distintos. Veamos, para terminar, que sumando el número de bloques posibles en cada caso nos da el mismo resultado que el obtenido en la Proposición 1.1.5 , es decir, que el número total de bloques es $\frac{v_1v_2(v_1v_2-1)}{6}$. Denotemos por b_1 y b_2 el número de bloques de los $STS(v_1)$ y $STS(v_2)$ respectivamente.

- Fijando un elemento de los v_1 posibles de V_1 y los b_2 bloques totales del $STS(v_2)$, obtenemos v_1b_2 bloques de la primera forma.
- Fijando un elemento de los v_2 posibles de V_2 y los b_1 bloques totales del $STS(v_1)$, obtenemos v_2b_1 bloques de la segunda forma.
- Para cada bloque $\{x_1, x_2, x_3\}$ del $STS(v_1)$ y $\{y_1, y_2, y_3\}$ del $STS(v_2)$, obtenemos seis permutaciones que nos definen distintos bloques del $STS(v_1v_2)$:

$$\{(x_1, y_1), (x_2, y_2), (x_3, y_3)\}, \quad \{(x_1, y_1), (x_2, y_3), (x_3, y_2)\}, \quad \{(x_1, y_2), (x_2, y_1), (x_3, y_3)\},$$

$$\{(x_1,y_2),(x_2,y_3),(x_3,y_1)\},\quad \{(x_1,y_3),(x_2,y_1),(x_3,y_2)\},\quad \{(x_1,y_3),(x_2,y_2),(x_3,y_1)\}.$$

Por lo tanto, hay $6b_1b_2$ bloques de la última forma.

Sumamos los tres casos y aplicamos la Proposición 1.1.5 para obtener el siguiente resultado:

$$\begin{aligned} &v_1b_2 + v_2b_1 + 6b_1b_2 = \\ &= v_1\frac{v_2(v_2-1)}{6} + v_2\frac{v_1(v_1-1)}{6} + 6\frac{v_1(v_1-1)}{6}\frac{v_2(v_2-1)}{6} = \\ &= \frac{v_1v_2}{6}(v_1 - 1 + v_2 - 1 + 6\frac{(v_2-1)(v_1-1)}{6}) = \\ &= \frac{v_1v_2}{6}(v_1 - 1 + v_2 - 1 + (v_2-1)(v_1-1)) = \\ &= \frac{v_1v_2}{6}(v_1v_2 - 1) \end{aligned}$$

Vemos que finalmente nos queda $\frac{v_1v_2(v_1v_2-1)}{6}$, como queríamos. Hemos terminado entonces de construir nuestro $STS(v_1v_2)$.

□

Proposición 1.1.12. *Sea un $STS(v)$ definido sobre un conjunto V. Se puede construir a partir de él un $STS(2v+1)$.*

Demostración. Sea ∞ un elemento que no pertenece a $\{1,2\}\times V$. Definimos el conjunto $G = (\{1,2\}\times V)\cup\{\infty\}$ de $2v+1$ elementos donde vamos a construir nuestro $STS(2v+1)$. Las ternas son de dos tipos:

- $\{(1,x),(2,x),\infty\}$ con $x\in V$.
- $\{(a,x),(b,y),(c,z)\}$ siendo $\{x,y,z\}$ terna del $STS(v)$, $a,b,c\in\{1,2\}$ con $a+b+c$ par.

Tenemos que comprobar que cada par de elementos distintos de G aparece en una única terna. Distingamos varios casos:

- Si uno de los elementos es ∞, observamos que cada elemento va a estar con ∞ en una única terna de la forma $\{(1,x),(2,x),\infty\}$.
- Para los pares de elementos del tipo (a,x), (b,x) con $a\neq b$, completamos la terna con una de las del primer tipo.
- Por último, para los pares (a,x), (b,y) con $x\neq y$, tenemos, por definición de $STS(v)$, que existe una única terna $\{x,y,z\}$ en la que están x e y. Para escoger el tercer elemento $(1,z)$ o $(2,z)$, distingo dos casos acorde con la definición de nuestro segundo tipo de ternas:
  - Si $a+b+1$ es par escojo la terna $\{(a,x),(b,y),(1,z)\}$.

- Si $a+b+2$ es par escojo la terna $\{(a,x),(b,y),(2,z)\}$.

De esta manera, hemos visto que cada par de elementos distintos de nuestro grupo G de $2v+1$ elementos están en una única terna, luego hemos construido nuestro $STS(2v+1)$.

□

1.2. BIBD

Después de haber introducido los $(v,3,1)$-BIBD denominados sistemas triples de Steiner, en esta sección estudiaremos resultados más generales sobre los BIBD. Hasta ahora, solo hemos trabajado con diseños que estaban organizados en ternas, es decir, en subconjuntos de 3 elementos. A partir de ahora, estudiaremos nuevos diseños que están organizados en subconjuntos de k elementos, pudiendo ser k un número mayor que tres. A estos subconjuntos de k elementos los denominamos *bloques*. Por otra parte, estudiaremos también diseños en los que cada par de elementos distintos puedan estar en más de un bloque simultáneamente. Además, veremos cómo representar los BIBD en forma matricial y cómo obtener su diseño dual.

Definición 1.2.1. *Un* (v,k,λ)***-BIBD*** *(" Balanced Incomplete Block Design ") o* 2*-*(v,k,λ) *diseño es un conjunto* V *de* v *elementos junto con una familia* $\mathcal{B}$ *de subconjuntos de* V *denominados bloques. Cada bloque contiene* k *elementos de* V*, de manera que cada par de elementos* $x,y \in V$ *distintos están contenidos simultáneamente en exactamente* λ *bloques.*
Al valor λ *se le denomina* ***índice****.*

Ejemplo 1.2.2. Veamos un primer ejemplo: un $(13,4,1)$-BIBD sobre el conjunto

$$V=\{1,2,3,4,5,6,7,8,9,10,11,12,13\}.$$

Los bloques, en este caso, son cuaternas (conjuntos de 4 elementos). Escogemos la siguiente familia de bloques:

$$\{1,2,4,10\},\ \{1,3,9,13\},\ \{1,5,6,8\},\ \{1,7,11,12\},\ \{2,3,5,11\},\ \{2,6,7,9\},\ \{2,8,12,13\},$$

$$\{3,4,6,12\},\ \{3,7,8,10\},\ \{4,5,7,13\},\ \{4,8,9,11\},\ \{5,9,10,12\},\ \{6,10,11,13\}.$$

Podemos observar que cada par de elementos distintos están simultáneamente en una única cuaterna.

Ejemplo 1.2.3. Vamos a ver ahora una aplicación real en la que este BIBD podría ser útil. Imaginemos que en una ciudad se celebra un concurso para elegir la mejor cerveza artesanal entre las 13 más vendidas actualmente. Las cervezas serán degustadas por varios catadores pero, lógicamente, cada catador no va a poder probar todas las cervezas porque, a partir de un cierto número, su estado y su gusto podrían cambiar. Por tanto, pongamos que cada catador prueba 4 cervezas. Tenemos, a través de este BIBD, lo siguiente:

- $v=13$ es el número total de cervezas.

- $k = 4$ es el número de cervezas que degusta cada catador, es decir, cada catador es un bloque y tenemos en total 13 bloques y catadores.
- $\lambda = 1$ significa que cada par de cervezas distintas será probado por un único catador.
- Podemos observar que cada marca de cerveza va a ser degustada por 4 catadores distintos, ya que cada elemento está contenido en 4 bloques distintos.

Hemos visto un ejemplo que nos da de manera sencilla cómo poder organizar un concurso. Este mismo ejemplo podría aplicarse también a otro caso con un número de personas mayor:

Pongamos que se quiere hacer un muestreo estadístico sobre la opinión que las personas que acuden a ver el concurso de cerveza tienen sobre las 13 cervezas artesanales, para luego poder compararlo con la opinión de los especialistas. Supongamos que elegimos a 520 personas, de esta manera podríamos separarlos en 40 grupos de 13 personas y, con cada grupo, realizar la misma cata que habíamos construido anteriormente gracias al $(13, 4, 1)$-BIBD. Además, cada cerveza sería probada por 160 personas distintas, lo cual nos da una buena muestra para poder hacer nuestro modelo estadístico y sacar una conclusión de la opinión popular sobre cada cerveza, comparada a la vez por la opinión de los catadores.

Ejemplo 1.2.4. Este ejemplo de $(13, 4, 1)$-BIBD nos da, además, una construcción del plano proyectivo sobre el plano afín $\mathbb{F}_3^2$. Como vimos en el Ejemplo 1.1.6 de la sección anterior, en $\mathbb{F}_3^2$ tenemos las siguientes rectas:

- $y = b, \quad b \in \mathbb{Z}/(3)$.
- $x = c, \quad c \in \mathbb{Z}/(3)$.
- $y = x + b, \quad b \in \mathbb{Z}/(3)$.
- $y = 2x + b = -x + b, \quad b \in \mathbb{Z}/(3)$.

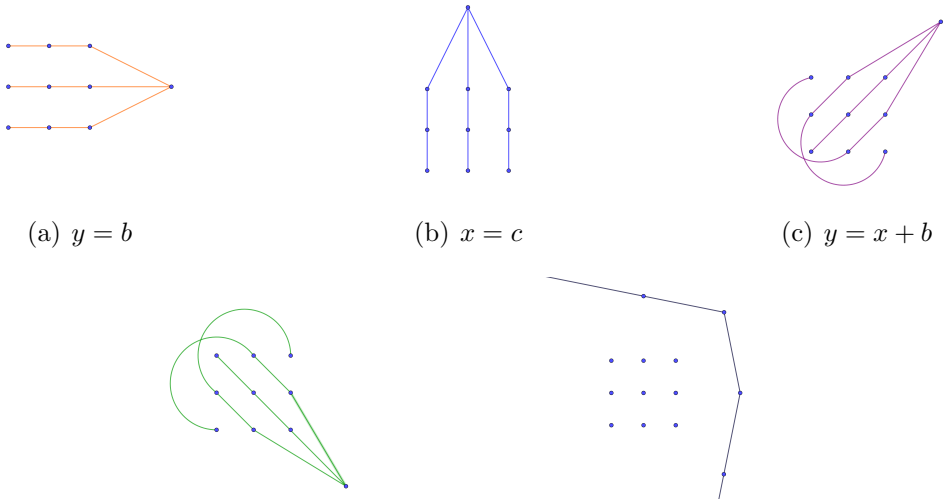
Como estamos en el plano proyectivo, tenemos que añadir a cada una de estas rectas un punto en el infinito (que será distinto para cada clase de rectas paralelas), y además, la recta del infinito que contiene los cuatro puntos del infinito. Luego tenemos $v = 9+4 = 13$ puntos y $b = 12+1 = 13$ rectas que contienen 4 puntos cada una, y que equivalen a los bloques de nuestro $(13, 4, 1)$-BIBD. Se puede comprobar también el valor $\lambda = 1$ ya que cada par de puntos distintos están contenidos en una única recta. Véase la Figura 1.4.

Al igual que hicimos para los sistemas triples de Steiner, estudiemos ahora cómo calcular el número de replicación y el número de bloques de un (v, k, λ)-BIBD.

Proposición 1.2.5. [18]

Sea $(V, \mathcal{B})$ un (v, k, λ)-BIBD. Entonces:

- *Cada elemento $x \in V$ está contenido exactamente en $r = \lambda\frac{v-1}{k-1}$ bloques. Este es el **número de replicación**.*



(a) $y = b$ (b) $x = c$ (c) $y = x + b$

(d) $y = -x + b$ (e) Recta puntos del infinito

Figura 1.4: Rectas del plano proyectivo.

- *El* ***número de bloques*** *es exactamente* $b = \lambda\frac{v(v-1)}{k(k-1)}$.

Demostración. Sea $(V, \mathcal{B})$ un (v, k, λ)-BIBD. Dado $x \in V$, denotemos por r_x al número de bloques que contienen a x. Definamos

$$I = \{(y, S) \ : \ y \in V, \ y \neq x, \ S \in \mathcal{B}, \ \{x, y\} \subseteq S\}.$$

Vamos a calcular el cardinal $|I|$ de dos maneras distintas:
En primer lugar, hay $v - 1$ maneras de elegir $y \in V$ con $y \neq x$. Para cada y, hay λ bloques S tales que $\{x, y\} \subseteq S$. Entonces

$$|I| = \lambda(v - 1).$$

Por otra parte, hay r_x formas de escoger un bloque S tal que $x \in S$. Para cada elección de S hay $k - 1$ formas de escoger $y \in S$ con $y \neq x$. Es decir,

$$|I| = r_x(k - 1).$$

Igualando las dos expresiones obtenemos $r_x = \lambda\frac{v-1}{k-1}$, y como r_x es independiente de cada x, obtenemos nuestra expresión $r = \lambda\frac{v-1}{k-1}$.

Queremos calcular ahora el número de bloques $b = |\mathcal{B}|$. Definimos un nuevo conjunto:

$$J = \{(x, S) \ : \ x \in V, \ S \in \mathcal{B}, \ x \in S\}.$$

Vamos a usar el método anterior calculando el cardinal $|J|$ de dos formas distintas:
En primer lugar, tenemos v posibilidades de elegir $x \in V$, y para cada x hay r bloques S tal que $x \in S$. Entonces

$$|J| = vr.$$

Por otro lado, hay b posibilidades de escoger un bloque $S \in \mathcal{B}$, y para cada elección de S hay k

posibilidades de elegir un $x \in S$. Es decir,

$$|J| = bk.$$

Igualando las dos expresiones nos queda lo siguiente:

$$b = \frac{vr}{k} = \lambda \frac{v^2 - v}{k^2 - k} = \lambda \frac{v(v-1)}{k(k-1)}.$$

□

Nótese que $bk = vr$.

Los BIBD también se denotan como (v, b, r, k, λ)-BIBD.

Veamos ahora una serie de resultados sobre los posibles v en los BIBD cuyos bloques contengan 4 ó 5 elementos. Estos resultados nos serán muy útiles en los próximos capítulos, ya que nos centraremos en construcciones para un v concreto dentro de los BIBD con bloques de tamaño $k = 4$.

Proposición 1.2.6. *Sea un $(v, 4, 1)$-BIBD. Entonces $v \equiv 1$ ó 4 mod (12).*

Demostración. Tenemos $r = \frac{v-1}{4-1} = \frac{v-1}{3}$ un número entero, luego $v \equiv 1 \bmod (3)$.

Es decir, $v \equiv 1$, 4, 7 ó 10 mod (12), lo que nos da $v \in \{12t+1, 12t+4, 12t+7, 12t+10\}$, con t entero.

Si fuese $v = 12t + 7$, entonces $b = \frac{v(v-1)}{4 \cdot 3} = \frac{(12t+7)(12t+6)}{12} = \frac{(12t+7)(2t+1)}{2}$, lo cual es absurdo porque b es un número entero y el numerador es un número impar, y al dividirlo por dos no va a ser entero. Entonces no puede ser $v = 12t + 7$.

Si fuese $v = 12t + 10$, entonces $b = \frac{v(v-1)}{4 \cdot 3} = \frac{(12t+10)(12t+9)}{12} = \frac{(6t+5)(4t+3)}{2}$, lo cual es absurdo porque b es un número entero y el numerador es un número impar, y al igual que en el caso anterior, al dividirlo por dos no va a ser entero. Entonces no puede ser $v = 12t + 10$.

Comprobemos ahora que para $v = 12t + 1$ tenemos b entero: $b = \frac{v(v-1)}{4 \cdot 3} = \frac{(12t+1)(12t)}{12} = (12t + 1)t$, lo cual es entero.

Por último, comprobemos ahora que para $v = 12t+4$ tenemos b entero: $b = \frac{v(v-1)}{4 \cdot 3} = \frac{(12t+4)(12t+3)}{12} = (3t + 1)(4t + 1)$, que también es entero.

Finalmente, obtenemos $v \equiv 1$ ó 4 mod (12). □

Proposición 1.2.7. *Sea un $(v, 5, 1)$-BIBD. Entonces $v \equiv 1$ ó 5 mod (20).*

Demostración. Tenemos $r = \frac{v-1}{5-1} = \frac{v-1}{4}$ un número entero, luego $v \equiv 1 \bmod (4)$.

Es decir, $v \equiv 1$, 5, 9, 13 ó 17 mod (20), luego $v \in \{20t + 1, 20t + 5, 20t + 9, 20t + 13, 20t + 17\}$, con t entero.

Si fuese $v = 20t + 9$, entonces $b = \frac{v(v-1)}{5\cdot 4} = \frac{(20t+9)(20t+8)}{20} = \frac{(20t+9)(5t+2)}{5} = 20t^2 + 8t + 9t + \frac{18}{5}$, lo cual es absurdo porque b es un número entero y esa expresión no es un número entero. Entonces no puede ser $v = 20t + 9$.

Si fuese $v = 20t + 13$, entonces $b = \frac{v(v-1)}{5\cdot 4} = \frac{(20t+13)(20t+12)}{20} = \frac{(20t+13)(5t+3)}{5} = 20t^2 + 12t + 13t + \frac{39}{5}$, lo cual es absurdo, por la misma razón que el caso anterior. Entonces no puede ser $v = 20t + 13$.

Si fuese $v = 20t + 17$, entonces $b = \frac{v(v-1)}{5\cdot 4} = \frac{(20t+17)(20t+16)}{20} = \frac{(20t+17)(5t+4)}{5} = 20t^2 + 16t + 17t + \frac{68}{5}$, y llegamos de nuevo a un absurdo. Entonces no puede ser $v = 20t + 9$.

Comprobemos ahora que para $v = 20t + 1$ tenemos b entero: $b = \frac{v(v-1)}{5\cdot 4} = \frac{(20t+1)(20t)}{20} = (20t + 1)t$, lo cual es entero.

Por último, comprobemos ahora que para $v = 20t+5$ tenemos b entero: $b = \frac{v(v-1)}{5\cdot 4} = \frac{(20t+5)(20t+4)}{20} = (4t + 1)(5t + 1)$, que también es entero.

Por tanto, $v \equiv 1$ ó $5 \bmod (20)$. □

Proposición 1.2.8. *Sea un $(v, 4, 2)$-BIBD. Entonces $v \equiv 1 \bmod (3)$.*

Demostración. Tenemos $r = 2\frac{v-1}{4-1} = 2\frac{v-1}{3}$ un número entero, luego $v \equiv 1 \bmod (3)$, es decir, $v = 3t + 1$ con t entero.

Queda comprobar que se cumple b entero, es decir, que se cumple que $b = 2\frac{(3t+1)3t}{12} = \frac{(3t+1)t}{2}$ es entero. Tenemos que, o bien t, o bien $3t+1$, es par para un t entero, luego el numerador es divisible por 2 y entonces b es entero. Por tanto, $v \equiv 1 \bmod (3)$. □

A lo largo de este documento, estudiaremos, para un mismo v, distintas construcciones de BIBD. Por ello, veamos la definición de isomorfismo entre BIBD, que nos ayudará a diferenciar si dichas construcciones son isomorfas o no.

Definición 1.2.9. *Sean $(V_1, \mathcal{B}_1)$, $(V_2, \mathcal{B}_2)$ dos (v, k, λ)-BIBD con $|V_1| = |V_2|$. (V_1, B_1) y (V_2, B_2) son **isomorfos** si existe una biyección $\alpha : V_1 \longrightarrow V_2$ que envía a cada bloque de $\mathcal{B}_1$ en un bloque de $\mathcal{B}_2$, es decir,*

$$\{\{\alpha(x) \ : \ x \in C\} \ : \ C \in \mathcal{B}_1\} = \mathcal{B}_2.$$

*Esta biyección se denomina **isomorfismo** entre $(V_1, \mathcal{B}_1)$ y $(V_2, \mathcal{B}_2)$.*
*Si $V_1 = V_2$ tenemos que α se denomina **automorfismo**.*

1.3. Matriz de incidencia y diseño dual de un BIBD.

A continuación, veremos cómo podemos representar los BIBD de forma matricial, qué propiedades tendrán estas matrices y qué condiciones tendrá que cumplir una matriz para poder ser la representación de un (v, k, λ)-BIBD. Además, a partir de la representación matricial de un BIBD, estudiaremos cómo obtener de una manera sencilla su diseño dual. También observaremos cómo se relacionan las propiedades del diseño dual y del BIBD inicial.

Definición 1.3.1. *La **matriz de incidencia** de un (v,k,λ)-BIBD $(V,\mathcal{B})$ es una $v \times b$ matriz $M = (m_{i,j})$ donde $m_{i,j} = 1$ si el elemento i-ésimo de V aparece en el j-ésimo bloque de $\mathcal{B}$, y $m_{i,j} = 0$ si no. Tiene varias propiedades:*

1. *Cada columna de M tiene exactamente k unos.*
2. *Cada fila de M tiene exactamente r unos.*
3. *Cada par de filas distintas de M, ambas contienen simultáneamente unos en exactamente λ columnas.*

Ejemplo 1.3.2. Veamos la matriz de incidencia del $(6,3,2)$-BIBD $(V,\mathcal{B})$ con $V = \{1,2,3,4,5,6\}$ y $\mathcal{B} = \{\{1,2,3\},\{1,2,4\},\{1,3,5\},\{1,4,6\},\{1,5,6\},\{2,3,6\},\ \{2,4,5\},\{2,5,6\},\{3,4,5\},\{3,4,6\}\}$.

Tenemos $v = 6$ y $b = 10$ luego es una matriz 6×10:

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \tag{1.1}$$

Observamos que cada columna tiene $k = 3$ unos, cada fila $r = 5$ unos y cada par de filas distintas comparten unos en exactamente $\lambda = 2$ columnas (por ejemplo, la primera y la última fila comparten unos en la cuarta y quinta columna).

Sea I_n la matriz identidad de dimensión $n \times n$, J_n la matriz llena de unos de dimensión $n \times n$ y u_n el vector lleno de unos de longitud n. Denotemos también M^t como la matriz traspuesta de una matriz M.

Teorema 1.3.3. [18] *Sea M una matriz de ceros y unos de dimensión $v \times b$, y sea $2 \leq k < v$. Entonces M es la matriz de incidencia de un (v,b,r,k,λ)-BIBD si y solo si $MM^t = \lambda J_v + (r-\lambda)I_v$ y $u_v M = k u_b$.*

Demostración. En primer lugar, supongamos $(V,\mathcal{B})$ un (v,k,λ)-BIBD donde $V = \{x_1,...,x_v\}$ y $\mathcal{B} = \{A_1,...,A_b\}$. Sea M su matriz de incidencia. El elemento de la posición (i,j) de MM^t es

$$\sum_{h=1}^{b} m_{i,h} m_{j,h} = \begin{cases} r \text{ si } i = l. \\ \\ \lambda \text{ si } i \neq j. \end{cases}$$

De las dos últimas propiedades de las matrices de incidencia deducimos que cada elemento de la diagonal de MM^t es igual a r, y que los demás elementos son igual a λ, luego tenemos $MM^t = \lambda J_v + (r-\lambda)I_v$. Además, el i-ésimo elemento de $u_v M$ es igual al número de unos de la columna i de M, que por la primera propiedad de las matrices de incidencia tenemos que es k. Luego $u_v M = k u_b$.

Supongamos ahora que M es una matriz de ceros y unos de dimensión $v \times b$ tal que $MM^t = \lambda J_v + (r-\lambda)I_v$ y $u_v M = k u_b$. Sea $(V, \mathcal{B})$ el BIBD que queremos comprobar que tiene matriz de incidencia M. Tenemos que $|V| = v$ y $|\mathcal{B}| = b$. De la ecuación $u_v M = k u_b$ obtenemos que cada bloque de $\mathcal{B}$ contiene k elementos. De la ecuación $MM^t = \lambda J_v + (r-\lambda)I_v$ obtenemos que cada par de elementos aparecen a la vez en exactamente λ bloques, y que cada elemento aparece en r bloques.
Luego $(V, \mathcal{B})$ es un (v, b, r, k, λ)-BIBD, como queríamos. □

A partir de la matriz de incidencia de un BIBD dado, definamos su diseño dual y las propiedades de este nuevo diseño, relacionadas con el BIBD inicial.

Definición 1.3.4. *Sea $(V, \mathcal{B})$ un (v, b, r, k, λ)-BIBD con matriz de incidencia M. El diseño cuya matriz de incidencia es M^t se denomina* ***diseño dual*** *de $(V, \mathcal{B})$. Supongamos que $(W, \mathcal{C})$ es el diseño dual de $(V, \mathcal{B})$, entonces $|V| = |\mathcal{C}| = v$ e $|W| = |\mathcal{B}| = b$.*

Teorema 1.3.5. [18] *Sea $(V, \mathcal{B})$ un (v, b, r, k, λ)-BIBD e $(W, \mathcal{C})$ su diseño dual. Entonces se cumplen las siguientes propiedades:*

1. *Cada bloque de $\mathcal{C}$ contiene r elementos.*
2. *Cada elemento de W aparece exactamente en k bloques.*
3. *Cada par de bloques distintos de $\mathcal{C}$ intersectan exactamente en λ elementos.*

Nótese que el teorema anterior no indica que el diseño dual de un BIBD sea necesariamente un BIBD.

Veamos un ejemplo de una construcción de un diseño dual y comprobemos si el diseño resultante es un BIBD.

Ejemplo 1.3.6. A partir del anterior Ejemplo 1.3.2 , veamos el diseño dual del $(6, 10, 5, 3, 2)$-BIBD $(V, \mathcal{B})$. Tenemos que la matriz de incidencia del diseño dual es la matriz traspuesta de la matriz de incidencia del BIBD anterior, luego obtenemos la siguiente matriz:

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix} \tag{1.2}$$

Veamos que esta matriz 10×6 nos proporciona un diseño $(W, \mathcal{C})$ de 10 elementos y 6 bloques:

1. En la matriz observamos que cada columna tiene 5 unos, es decir, cada bloque tiene 5 elementos. Teníamos $r = 5$ en $(V, \mathcal{B})$, luego verificamos la primera propiedad del dual.

2. Observamos que cada fila de la matriz contiene 3 unos, es decir, cada elemento de W aparece en 3 bloques. Coincide con el $k = 3$ de $(V, \mathcal{B})$, luego se cumple también la segunda propiedad del dual.

3. Por último, tenemos que cada par de columnas distintas tienen unos a la vez en exactamente 2 filas, o lo que es lo mismo, cada par de bloques distintos intersectan exactamente en 2 elementos. También teníamos $\lambda = 2$ en $(V, \mathcal{B})$, luego se verifica la última propiedad.

Como hemos comentado anteriormente, el Teorema 1.3.5 no nos aseguraba que el diseño dual tuviera que ser un BIBD, solo nos decía que tenía que cumplir una serie de propiedades, y en este ejemplo mismo lo apreciamos. Tenemos, por ejemplo, que los dos primeros elementos de W están simultáneamente en el primer y segundo bloque, como se aprecia en la matriz. Sin embargo, el quinto y el sexto elemento solo están simultáneamente en el sexto bloque. Luego tenemos que $(W, \mathcal{C})$ no es un BIBD, ya que no tiene un índice λ igual para cada par de elementos distintos.

Para terminar este capítulo, veamos un ejemplo de un BIBD donde su diseño dual sea también un BIBD.

Ejemplo 1.3.7. Volvemos al ejemplo del plano proyectivo de Fano, sea $(V, \mathcal{B})$ un $(7, 3, 1)$-BIBD definido sobre $\mathbb{Z}/(7)$ por las siguientes ternas:

$$\{0,1,3\},\ \{1,2,4\},\ \{2,3,5\},\ \{3,4,6\},\ \{0,4,5\},\ \{1,5,6\},\ \{0,2,6\}.$$

Observemos que $b_V = 7$ y $r_V = 3$, luego su matriz de incidencia es de dimensión 7×7:

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} \tag{1.3}$$

Por tanto, su diseño dual $(W, \mathcal{C})$ está determinado por la matriz de incidencia M^t, también de dimensión 7×7:

$$M^t = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \tag{1.4}$$

De la misma manera que en el ejemplo anterior, observamos que cada columna contiene 3 unos, es decir, cada bloque de $\mathcal{C}$ contiene $r_V = 3$ elementos.
Por otro lado, cada fila contiene 3 unos, es decir, cada elemento de W aparece en $k_V = 3$ bloques.
Por último, apreciamos que cada par de columnas distintas contienen unos simultáneamente en exactamente 1 fila, es decir, cada par de bloques distintos de $\mathcal{C}$ intersectan en $\lambda_V = 1$ elemento.

Por tanto, si esta matriz fuera la matriz de incidencia de un $(v_W, b_W, r_W, k_W, \lambda_W)$-BIBD entonces, por lo observado anteriormente en M^t, tendría que ser un $(7, 7, 3, 3, 1)$-BIBD.

Para comprobar que esta matriz M^t es la matriz de incidencia de un BIBD, veamos si se satisfacen las hipótesis del Teorema 1.3.3 :
Recordemos que I_7 es la matriz identidad de dimensión 7×7, J_7 la matriz llena de unos de dimensión 7×7 y u_7 el vector lleno de unos de longitud 7. En primer lugar, verifiquemos que $M^t M = \lambda J_7 + (r_W - \lambda_W) I_7$:

$$M^t M = \begin{pmatrix} 3 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 3 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 3 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 3 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 3 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 3 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 3 \end{pmatrix} = 1J_7 + (3-1)I_7 = \lambda_W J_7 + (r_W - \lambda_W) I_7. \tag{1.5}$$

Por último, nos queda comprobar que $u_7 M^t = k_W u_7$:

$$u_7 M^t = \begin{pmatrix} 3 & 3 & 3 & 3 & 3 & 3 & 3 \end{pmatrix} = 3u_7 = k_W u_7. \tag{1.6}$$

Por lo tanto, se cumplen las dos hipótesis, y aplicando el Teorema 1.3.3 , obtenemos que M^t es la matriz de incidencia de un $(7, 7, 3, 3, 1)$-BIBD definido sobre $\mathbb{Z}/(7)$, que se puede expresar en ternas de la siguiente manera:

$$\{0, 4, 6\},\ \{0, 1, 5\},\ \{1, 2, 6\},\ \{0, 2, 3\},\ \{1, 3, 4\},\ \{2, 4, 5\},\ \{3, 5, 6\}.$$

Para concluir, podemos comprobar que la biyección

$$\alpha\ :\ V \longrightarrow W, \quad \text{que envía a} \quad (0, 1, 2, 3, 4, 5, 6) \longmapsto (0, 4, 3, 6, 1, 5, 2),$$

envía a cada bloque de $\mathcal{B}$ en un bloque de $\mathcal{C}$.
Luego tenemos un isomorfismo entre $(V, \mathcal{B})$ y su dual $(W, \mathcal{C})$. Además como $V = W = \mathbb{Z}/(7)$, comprobamos que α es automorfismo.

Capítulo 2

Familias de diferencias y familias de diferencias relativas

En este segundo capítulo estudiaremos unos conjuntos ligados a los BIBD denominados familias de diferencias y familias de diferencias relativas. Veremos varios teoremas que nos facilitarán la construcción de nuevos BIBD y, gracias al desarrollo de las familias de diferencias, podremos expresar estos diseños de una forma simple y breve.

2.1. Familias de diferencias

Antes de definir las familias de diferencias, recordemos que los multiconjuntos, denotados entre corchetes [ ], son como unos conjuntos en los que no importa el orden en el que escribamos los elementos, pero sí importa la cantidad de veces que aparece un mismo elemento.

Por ejemplo, $[2,1,7,4,2,7,1,2] = [1,1,2,2,2,4,7,7]$.

Definición 2.1.1. *Sea $(G,+)$ un grupo conmutativo de orden v con elemento neutro 0. Una (v,k,λ)-**familia de diferencias** definida sobre el grupo G es una familia de subconjuntos de k elementos de G, sean $A_1, A_2, ..., A_l$, de forma que el multiconjunto*

$$\bigcup_{i=1}^{l} [x-y,\ y-x\ :\ x,y \in A_i,\ x \neq y]$$

contiene cada elemento de $G \setminus \{0\}$ exactamente λ veces.

Denotemos también $\Delta A_i = [x-y,\ y-x\ :\ x,y \in A_i,\ x \neq y]$.

*Si la familia de diferencias está formada por un único conjunto, se denomina **conjunto de diferencias**.*

Observemos que el cardinal de cada ΔA_i es $k(k-1)$. Además, el cardinal del multiconjunto es igual a $\lambda(v-1)$, es decir, el número de elementos de $G \setminus \{0\}$ multiplicado por el número de veces que aparece cada elemento en el multiconjunto, que es λ. Luego si consideramos una familia de

diferencias $A_1, A_2, ..., A_l$ obtenemos la fórmula

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

Empecemos por un ejemplo sencillo en el que se expone una familia de diferencias.

Ejemplo 2.1.2. [7] Sea el grupo $(G,+) = (\mathbb{Z}/(19),+)$ y la $(19,4,2)$-familia de diferencias, sea $\{A_1, A_2, A_3\}$ con

$$A_1 = \{0,1,7,11\}, \quad A_2 = \{0,2,3,14\}, \quad A_3 = \{0,4,6,9\}.$$

Restando resulta que

$$\Delta A_1 = [1,7,11,18,12,8,6,13,10,9,4,5], \qquad \Delta A_2 = [2,3,14,17,16,5,1,18,12,7,11,8],$$

$$\Delta A_3 = [4,6,9,15,13,10,2,17,5,14,3,16].$$

Por lo tanto, $\Delta A_1 \cup \Delta A_2 \cup \Delta A_3$ nos queda igual a

$$[1,7,11,18,12,8,6,13,10,9,4,5,2,3,14,17,16,5,1,18,12,7,11,8,4,6,9,15,13,10,2,17,5,14,3,16],$$

que ordenado queda

$$[1,1,2,2,3,3,4,4,5,5,6,6,7,7,8,8,9,9,10,10,11,11,12,12,13,13,14,14,15,15,16,16,17,17,18,18].$$

Comprobamos que cada elemento de $G \setminus \{0\}$ está contenido exactamente $\lambda = 2$ veces en el multiconjunto, por tanto, se verifica la fórmula $\lambda(v-1) = lk(k-1)$, que es igual a 36.

Concluimos entonces que $\{A_1, A_2, A_3\}$ es una $(19,4,2)$-familia de diferencias.

Nótese, que para un mismo grupo, puede haber más de una familia de diferencias distinta. Por ejemplo, para este caso tenemos que también lo es la familia $\{A_1, A_2, A_3\}$ con

$$A_1 = \{0,1,3,12\}, \quad A_2 = \{0,1,5,13\}, \quad A_3 = \{0,4,6,9\}.$$

Estudiemos un importante teorema sobre la construcción de BIBD a partir de una familia de diferencias, aplicándolo después al ejemplo anterior.

Teorema 2.1.3. *Sea $(G,+)$ un grupo de orden v. Sea $A_1, A_2, ..., A_l$ una (v,k,λ)-familia de diferencias sobre G, entonces la familia de subconjuntos*

$$g + A_i \quad : \quad g \in G, i = 1,2,...,l$$

es un (v,k,λ)-BIBD definido sobre G.

A este BIBD se le denomina el ***desarrollo de la familia de diferencias****.*

Demostración. Veamos que $\{g + A_i \ : \ g \in G, \ i = 1,2,...,l\}$ son los bloques de un (v,k,λ)-BIBD

definido sobre G. Para ello, veamos que cada par de elementos distintos de G están a la vez en exactamente λ bloques.
Sean $x, y \in G$, $x \neq y$. Tenemos que $x - y \in G \setminus \{0\}$, luego al ser un elemento de $G \setminus \{0\}$ tenemos que $x - y$ aparece λ veces en el multiconjunto $\bigcup_{i=1}^{l}[x - y,\ y - x\ :\ x, y \in A_i,\ x \neq y]$. Entonces existen exactamente λ conjuntos ΔA_{i_j} con $a_{i_j}, b_{i_j} \in \Delta A_{i_j}$, $j = 1, ..., \lambda$, tales que

$$x - y = a_{i_1} - b_{i_1} \in \Delta A_{i_1},\quad x - y = a_{i_2} - b_{i_2} \in \Delta A_{i_2},\quad \ldots\quad x - y = a_{i_\lambda} - b_{i_\lambda} \in \Delta A_{i_\lambda}.$$

Operando obtenemos que

$$x - a_{i_1} = y - b_{i_1} = g_1 \in G,\quad x - a_{i_2} = y - b_{i_2} = g_2 \in G,\quad \ldots\quad x - a_{i_\lambda} = y - b_{i_\lambda} = g_\lambda \in G.$$

Por último,

$$x = g_1 + a_{i_1} \in g_1 + A_{i_1},\quad y = g_1 + b_{i_1} \in g_1 + A_{i_1},$$

$$\ldots$$

$$x = g_\lambda + a_{i_\lambda} \in g_\lambda + A_{i_\lambda},\quad y = g_\lambda + b_{i_\lambda} \in g_\lambda + A_{i_\lambda}.$$

Luego se tiene que cada par de elementos $x, y \in G$ con $x \neq y$ aparecen a la vez en exactamente λ bloques, como se quería demostrar.

□

Aplicando este teorema a la familia de diferencias del ejemplo anterior, observamos que los bloques

$$g + A_i\quad :\quad g \in \mathbb{Z}/(19),\ i = 1, 2, 3,$$

siendo

$$A_1 = \{0, 1, 7, 11\},\quad A_2 = \{0, 2, 3, 14\},\quad A_3 = \{0, 4, 6, 9\},$$

constituyen un $(19, 4, 2)$-BIBD definido sobre $\mathbb{Z}/(19)$.

Gracias al teorema anterior, podemos observar que una familia de diferencias es una forma bastante sencilla y útil de describir un BIBD, mucho más compacta y breve que tener que escribir todos los bloques de un BIBD. Debido a esto, esta forma de expresar BIBD será utilizada a menudo a lo largo de este trabajo.

Cabe resaltar que si el grupo sobre el que construimos la familia de diferencias es cíclico (como lo es $\mathbb{Z}/(19)$ en el caso anterior), se dice que la familia de diferencias es **cíclica** y, a su vez, el BIBD asociado se dice que es **cíclico**.

2.2. Familia de diferencias relativas

En primer lugar, denotemos por $\bigsqcup$ a la unión disjunta. En esta nueva sección estudiaremos unas familias de conjuntos disjuntos, que al relacionarlos con un subgrupo concreto y sus clases laterales, obtendremos resultados que nos ayudarán a construir nuevos diseños.

Definición 2.2.1. *Sea $(G,+)$ un grupo de orden v. Sea $H \subseteq G$ un subgrupo de G.*

*Una $(v,k,1)$-**familia de diferencias relativa** al subgrupo H es una colección de subconjuntos de G, sean*

$$B_1, B_2, ..., B_l \quad con \quad |B_i| = k \quad para\ i = 1, 2, ..., l$$

de forma que

$$G \setminus H = \bigsqcup_{i=1}^{l} \Delta B_i$$

siendo $\Delta B_i = \{x - y,\ y - x\ :\ x, y \in B_i,\ x \neq y\}$.

Nótese, que al estar ultilizando la unión disjunta, tenemos que $\Delta B_i \cap \Delta B_j = \emptyset$ para cada $i \neq j$.

Dados un grupo G de cardinal v y un subgrupo H de G de cardinal k, tenemos que existen $\frac{|G|}{|H|} = \frac{v}{k}$ clases laterales o cogrupos del subgrupo H en G. Los denotamos como

$$\{t + H\ :\ t \in \{g_1, g_2, ..., g_{\frac{v}{k}}\}\}$$

Por ejemplo, si $H = \{\bar{0}, \bar{4}, \bar{8}, \bar{12}\} \subseteq \mathbb{Z}/(16)$, los $\frac{16}{4} = 4$ cogrupos de H son $\{\bar{t} + H\ :\ \bar{t} \in \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}\}$.

Apliquemos el concepto de cogrupos para que, junto con las familias de diferencias relativas, podamos construir distintos BIBD.

Teorema 2.2.2. *Sea $(G,+)$ un grupo de orden v. Sea $H \subseteq G$ un subgrupo de G. Sea $B_1, B_2, ..., B_l$ con $|B_i| = k$ para cada $i = 1, 2, ..., l$ una $(v,k,1)$-familia de diferencias relativa a H.*

Si tenemos también $|H| = k$, entonces el desarrollo

$$\{g + B_i\ :\ g \in G, \quad i = 1, 2, ..., l\} \cup \{t + H\}$$

constituye un $(v,k,1)$-BIBD definido sobre el conjunto G.

*Denominaremos a los bloques de la forma $\{t + H\}$ como **bloques de ciclo corto**.*

Demostración. Queremos demostrar que el desarrollo formado por los bloques de la forma $\{g+B_i\ : g \in G, \quad i = 1, 2, ..., l\}$ y por las clases laterales $\{t + H\}$ constituye un $(v,k,1)$-BIBD sobre G. Para ello, veamos que cada par de elementos distintos de G están a la vez en un único bloque.

Sean $x, y \in G$ con $x \neq y$, tenemos dos opciones:

- Si $x - y \in G \setminus H$, entonces $x - y$ pertenece a un único ΔB_i, ya que, por hipótesis, $G \setminus H$ es igual a la unión disjunta de los ΔB_i. Por tanto, $x - y = a_{i_1} - a_{i_2}$ con $a_{i_1}, a_{i_2} \in B_i$, operando obtenemos que $x - a_{i_1} = y - a_{i_2} = g \in G$. Finalmente,

  $$x = g + a_{i_1} \in g + B_i, \quad y = g + a_{i_2} \in g + B_i,$$

  luego x, y pertenecen a un único bloque de la forma $\{g + B_i\ :\ g \in G, \quad i = 1, 2, ..., l\}$.

- Si $x - y \in H$, entonces $x + H = y + H$, es decir, x e y pertenecen a la misma clase lateral. Supongamos que es la clase lateral $t_i + H$, entonces $t_i + H = x + H = y + H$, lo que implica

que $x, y \in t_i + H$. Luego x e y pertenecen a un único bloque de la forma $\{t + H\}$.

Por tanto, hemos probado que el desarrollo $\{g + B_i \ : \ g \in G, \quad i = 1, 2, ..., l\} \cup \{t + H\}$ constituye un $(v, k, 1)$-BIBD definido sobre el conjunto G.

□

Veamos un ejemplo en el que se aplica el teorema anterior.

Ejemplo 2.2.3. [7] Sea $G = \mathbb{Z}/(21)$, desarrollemos un $(21, 3, 1)$-BIBD a partir de una $(21, 3, 1)$-familia de diferencias relativa definida sobre G.

Sea $H = \{0, 7, 14\}$ un subgrupo de G. Una $(21, 3, 1)$-familia de diferencias relativa a H es $\{B_1, B_2, B_3\}$ con

$$B_1 = \{0, 1, 3\}, \quad B_2 = \{0, 4, 12\}, \quad B_3 = \{0, 5, 11\}.$$

Comprobémoslo. Operando obtenemos que

$$\Delta B_1 = \{1, 3, 20, 18, 2, 19\}, \quad \Delta B_2 = \{4, 12, 17, 9, 8, 13\}, \quad \Delta B_3 = \{5, 11, 16, 10, 6, 15\}.$$

Podemos observar que $\mathbb{Z}/(21) \setminus \{0, 7, 14\} = \bigsqcup_{i=1}^{3} \Delta B_i$, por lo tanto, $\{B_1, B_2, B_3\}$ es una $(21, 3, 1)$-familia de diferencias relativa a H.

Aplicando el Teorema 2.2.2, concluimos que el desarrollo formado por los bloques

$$\{g + B_i \quad : \quad g \in \mathbb{Z}/(21), \ i = 1, 2, 3\},$$

junto con los bloques de ciclo corto

$$\{t + \{0, 7, 14\} \ : \ t \in \{0, 1, 2, 3, 4, 5, 6\}\},$$

constituye un $(21, 3, 1)$-BIBD definido sobre $\mathbb{Z}/(21)$.
Al ser un $(21, 3, 1)$-BIBD, tiene que tener $\frac{21 \cdot 20}{3 \cdot 2} = 70$ bloques. Comprobamos que hay $21 \cdot 3 = 63$ bloques de la forma $\{g + B_i\}$, y 7 bloques de ciclo corto, luego 70 bloques en total.

Definamos ahora el elemento ∞, este elemento nos será útil en el siguiente teorema ya que, a partir de un grupo G y una familia de diferencias relativa a un subgrupo H, construiremos un BIBD definido sobre $G \cup \{\infty\}$. Este elemento cumple que $\infty \notin G$ y que $g + \infty = \infty$ para cada $g \in G$.

Teorema 2.2.4. *Sea $(G, +)$ un grupo de orden v. Sea $H \subseteq G$ un subgrupo de G de orden $k - 1$. Sea $B_1, B_2, ..., B_l$ con $|B_i| = k$ para cada $i = 1, 2, ..., l$ una $(v, k, 1)$-familia de diferencias relativa a H. Sea también el elemento $\infty \notin G$ definido anteriormente. Entonces el desarrollo*

$$\{g + B_i \ : \ g \in G, \quad i = 1, 2, ..., l\} \bigcup \{\{\infty\} \cup (t + H)\}$$

constituye un $(v + 1, k, 1)$-BIBD definido sobre el conjunto $G \cup \{\infty\}$.

Demostración. De una manera similar a la demostración anterior, veremos que el desarrollo forma-

do por los bloques de la forma $\{g+B_i \ : \ g \in G, \quad i = 1, 2, ..., l\}$ y por los bloques $\{\{\infty\} \cup (t+H)\}$, siendo $(t+H)$ las clases laterales, constituye un $(v+1, k, 1)$-BIBD sobre $G \cup \{\infty\}$. Para ello, veamos que cada par de elementos distintos de $G \cup \{\infty\}$ están a la vez en un único bloque.

Sean $x, y \in G \cup \{\infty\}$ con $x \neq y$, tenemos varias opciones:

- Si $x, y \in G$, $x - y \in G \setminus H$, entonces de la misma manera que en la demostración anterior obtenemos que x, y pertenecen a un único bloque de la forma $\{g+B_i \ : \ g \in G, \quad i = 1, 2, ..., l\}$.
- Si $x, y \in G$, $x - y \in H$, entonces, por demostración anterior, obtenemos que x, y aparecen a la vez en una única clase lateral $(t + H)$, luego x e y pertenecen a un único bloque de la forma $\{\{\infty\} \cup (t + H)\}$.
- Veamos ahora el caso en el que x ó y son ∞, supongamos $x = \infty$ e $y \in G$ (el caso contrario es análogo). Recordemos una propiedad de las clases laterales: sea $H \subseteq G$ un subgrupo de G, si un elemento $y \in G$, entonces existe una única clase lateral de H en G tal que y pertenece a esa clase lateral. Luego tenemos que y pertenece a una única clase lateral de la forma $(t + H)$, es decir, x e y aparecen a la vez en un único bloque de la forma $\{\{\infty\} \cup (t + H)\}$.

Por tanto, hemos probado que el desarrollo $\{g + B_i \ : \ g \in G, \quad i = 1, 2, ..., l\} \bigcup \{\{\infty\} \cup (t + H)\}$ constituye un $(v + 1, k, 1)$-BIBD definido sobre el conjunto $G \cup \{\infty\}$.

□

Veamos dos ejemplos que representan de manera clara los resultados expuestos anteriormente.

Ejemplo 2.2.5. [19] Construyamos un $(16, 4, 1)$-BIBD a partir de una $(15, 4, 1)$-familia de diferencias relativa.

Sea $G = \mathbb{Z}/(15)$ y sea $H = \{0, 5, 10\} \subseteq G$. Sea también la familia de diferencias relativa $B_1 = \{0, 2, 3, 11\}$. Tenemos que $\Delta B_1 = \{2, 3, 11, 13, 12, 4, 1, 14, 9, 6, 8, 7\}$. Comprobamos que $\Delta B_1 = G \setminus H$, luego B_1 es una familia de diferencias relativa al grupo H.

Por el teorema anterior, el desarrollo

$$\{g + \{0, 2, 3, 11\} \ : \ g \in \mathbb{Z}/(15)\} \bigcup \{\{\infty\} \cup (t + \{0, 5, 10\}) \ : \ t \in \{0, 1, 2, 3, 4\}\}$$

constituye un $(16, 4, 1)$-BIBD definido sobre $\mathbb{Z}/(15) \bigcup \{\infty\}$.

Al ser un $(16, 4, 1)$-BIBD tiene que tener $\frac{16 \cdot 15}{4 \cdot 3} = 20$ bloques. Comprobamos que hay 15 bloques de la forma $\{g+\{0, 2, 3, 11\} \ : \ g \in \mathbb{Z}/(15)\}$, y 5 de la forma $\{\{\infty\} \cup (t+\{0, 5, 10\}) \ : \ t \in \{0, 1, 2, 3, 4\}\}$, luego 20 bloques en total.

Ejemplo 2.2.6. [19] Desarrollemos ahora un $(25, 5, 1)$-BIBD a partir de una $(24, 4, 1)$-familia de diferencias relativa.

Sea $G = \mathbb{Z}/(24)$ y sea $H = \{0, 6, 12, 18\} \subseteq G$. En esta ocasión, escogemos la familia de diferencias relativa $B_1 = \{0, 2, 3, 7, 16\}$. Tenemos que

$$\Delta B_1 = \{2, 3, 7, 16, 22, 21, 17, 8, 1, 5, 14, 23, 19, 10, 4, 13, 20, 11, 9, 15\}.$$

Comprobamos que $\Delta B_1 = G \setminus H$, luego B_1 es una familia de diferencias relativa al grupo H.

Por el teorema anterior, el desarrollo

$$\{g + \{0, 2, 3, 7, 16\} \ : \ g \in \mathbb{Z}/(24)\} \bigcup \{\{\infty\} \cup (t + \{0, 6, 12, 18\}) \ : \ t \in \{0, 1, 2, 3, 4, 5\}\}$$

constituye un $(25, 5, 1)$-BIBD definido sobre $\mathbb{Z}/(24) \bigcup \{\infty\}$.

Al ser un $(25, 5, 1)$-BIBD tiene que tener $\frac{25 \cdot 24}{5 \cdot 4} = 30$ bloques. Comprobamos que hay 24 bloques de la forma $\{g + \{0, 2, 3, 7, 16\} \ : \ g \in \mathbb{Z}/(24)\}$, y 6 de la forma $\{\{\infty\} \cup (t + \{0, 6, 12, 18\}) \ : \ t \in \{0, 1, 2, 3, 4, 5\}\}$, luego 30 bloques en total.

Capítulo 3

$(v, 4, 1)$-BIBD

A partir de este capítulo empezaremos a profundizar sobre diferentes construcciones acerca de los $(v, 4, 1)$-BIBD, es decir, nos centraremos en los BIBD con $\lambda = 1$ y bloques de tamaño $k = 4$. En un comienzo, estudiaremos varios teoremas sobre los cuerpos finitos que nos ayudarán, en una segunda parte, a desarrollar nuevos BIBD con un v más concreto definidos sobre distintos cuerpos finitos. También expondremos algún ejemplo concreto de cómo los BIBD son utilizados en aplicaciones reales.

Para comenzar, recordemos la Proposición 1.2.6: si tenemos un $(v, 4, 1)$-BIBD, entonces

$$v \equiv 1 \text{ ó } 4 \mod (12).$$

Luego v es de la forma $12t + 1$ ó $12t + 4$ para cada $t \in \mathbb{N}$. Mostramos, a continuación, una tabla con los posibles valores de v hasta 100, junto con el número de bloques y el número de replicación.

v	**b**	**r**
4	1	1
13	13	4
16	20	5
25	50	8
28	63	9
37	111	12
40	130	13
49	196	16
52	221	17
61	305	20
64	336	21
73	438	24
76	475	25
85	595	28
88	638	29
97	776	32
100	825	33

Cuadro 3.1: $(v, 4, 1)$-BIBD

3.1. Cuerpos finitos y $(v, 4, 1)$-BIBD

En resultados y construcciones posteriores necesitaremos el concepto de cuerpo finito o campo de Galois, por ello, en esta sección definiremos los cuerpos finitos y mostraremos algún resultado teórico que nos pueda ayudar a posteriori.

Sea p un número primo. Los enteros módulo p forman un cuerpo de p elementos denotado por $\mathbb{Z}/(p) \cong \mathbb{Z}_p \cong \mathbb{F}_p$.

Definición 3.1.1. *Sea p un número primo y n un número entero positivo, definamos $q = p^n$ la potencia de un primo. Si tenemos que el polinomio $g(x) = x^n + a_{n-1}x^{n-1} + \ ... \ + a_1x + a_0 \in \mathbb{F}_p[x]$ ($a_i \in \mathbb{F}_p$ para cada $0 \leq i \leq n-1$) es un polinomio irreducible de grado n, entonces se define el cuerpo finito de $q = p^n$ elementos y característica p como $GF(p^n) \cong \dfrac{\mathbb{F}_p[x]}{(g(x))} \cong \mathbb{F}_q$.*

Estudiemos a continuación un teorema sobre el grupo finito multiplicativo $(GF(p^n)^*, \cdot)$ que nos ayudará a construir $(12t + 1, 4, 1)$-BIBD, y otro teorema sobre la existencia y unicidad de los cuerpos finitos.

Teorema 3.1.2. [13] *Todo grupo finito multiplicativo dentro de un cuerpo finito F es cíclico.*

Demostración. Sea G un grupo finito multiplicativo dentro de F, en particular, tenemos que G es subgrupo del grupo multiplicativo F^* de todos los elementos distintos de 0 de F. Como G es un grupo finito abeliano, tenemos que G es producto de $\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}$ grupos cíclicos, donde $s = m_1 \cdots m_k$ es el orden de G y $m_1 = m$ es el mínimo común múltiplo de los órdenes de todos los elementos de G. Entonces tenemos que todo elemento $a \in G$ satisface $a^m = 1$. Finalmente, el polinomio $x^m - 1$ de grado m tiene como mucho m raíces a en el cuerpo F, mientras que G tiene $s = m \cdot m_2 \cdots m_k$ elementos a. Luego obtenemos $s = m$ y $G \cong \mathbb{Z}_{m_1}$ es cíclico. □

De este teorema se deduce que si $GF(p^n)$ es un cuerpo finito de orden p^n, entonces su grupo multiplicativo $(GF(p^n)^*, \cdot)$ es un grupo cíclico de orden $p^n - 1$. Es decir, en $GF(p^n)^*$ hay algún elemento de orden $p^n - 1$.

A continuación, mostramos, sin demostración, el teorema fundamental sobre la existencia de cuerpos finitos.

Teorema 3.1.3. [13] *Todo cuerpo finito tiene p^n elementos, donde p es la característica y n un entero positivo. Recíprocamente, para cada primo p y cada n se tiene que existe, salvo isomorfismo, un único cuerpo finito $GF(p^n) = \mathbb{F}_{p^n}$ de p^n elementos. En particular, $GF(p^n)$ es el cuerpo de descomposición $x^{p^n} - x$ sobre $\mathbb{F}_p$.*

Estudiemos un importante teorema para construir $(v, 4, 1)$-BIBD sobre cuerpos finitos que fue demostrado por R. C. Bose [4].

Teorema 3.1.4. [10] *Sea $v = p^n = 12t + 1$ potencia de un número p primo, t un número natural. Si x es una raíz primitiva en $GF(p^n)$ tal que $x^{4t} - 1 = x^h$, siendo h un número impar, entonces el desarrollo de la familia de diferencias*

$$\{0, x^0, x^{4t}, x^{8t}\},\ \{0, x^2, x^{2+4t}, x^{2+8t}\},\ \ldots, \{0, x^{2i}, x^{2i+4t}, x^{2i+8t}\},\ \ldots, \{0, x^{2t-2}, x^{6t-2}, x^{10t-2}\}$$

define sobre el grupo aditivo $(GF(p^n), +)$ *un* $(v, 4, 1)$*-BIBD con* $v = 12t + 1$*,* $b = t(12t + 1)$ *y* $r = 4t$*.*

Demostración. Nuestro objetivo es demostrar que la familia de conjuntos anterior es una $(12t + 1, 4, 1)$-familia de diferencias. En primer lugar, sea x una raíz primitiva en $GF(p^n)$, es decir, el orden de x es $p^n - 1$ y $x^{p^n-1} = x^{12t} = 1$. Luego tenemos que $x^{6t} = -1$. Sea $A = \{0, x^0, x^4, x^8\} = \{0, 1, x^4, x^8\}$, sus 12 diferencias son

$$\Delta A = [1, x^{4t}, x^{8t}, x^{4t} - 1, x^{8t} - 1, x^{8t} - x^{4t}, -1, -x^{4t}, -x^{8t}, 1 - x^{4t}, 1 - x^{8t}, x^{4t} - x^{8t}].$$

Aplicando la hipótesis $x^{4t} - 1 = x^h$ y también $x^{6t} = -1$, tenemos que $x^{8t} - 1 = x^{8t}(1 - x^{4t}) = x^{8t}(-x^h) = x^{8t}x^{6t}x^h = x^{14t+h} = x^{2t+h}$. Además, $x^{8t} - x^{4t} = x^{4t}(x^{4t} - 1) = x^{4t+h}$. Desarrollando las demás de la misma manera obtenemos que

$$\Delta A = [1, x^{4t}, x^{8t}, x^h, x^{2t+h}, x^{4t+h}, x^{6t}, x^{10t}, x^{2t}, x^{6t+h}, x^{8t+h}, x^{10t+h}].$$

Como hemos supuesto h impar, tenemos que las 12 diferencias anteriores son distintas. Hemos hallado las diferencias del primer conjunto de la familia. Dada la familia de conjuntos $x^{2i}A$, $i = 0, 1, 2, \ldots, t - 1$, definida en el enunciado, obtenemos que

$$\bigcup_{i=0}^{t-1} \Delta(x^{2i}A) = \bigcup_{i=0}^{t-1} x^{2i}(\Delta A) = \bigcup_{i=0}^{t-1} x^{2i}[1, x^{2t}, x^{4t}, x^{6t}, x^{8t}, x^{10t}, x^h, x^{2t+h}, x^{4t+h}, x^{6t+h}, x^{8t+h}, x^{10t+h}]$$

Nótese, que estando en módulo 12,

$$\bigcup_{i=0}^{t-1} [2i, 2t+2i, \ldots, 10t+2i, h+2i, h+2t+2i, \ldots, h+10t+2i] = [0, 1, 2, \ldots, 12t-1] = [0, 1, 2, \ldots, p^n-2],$$

luego, teniendo en cuenta lo anterior, y como tenemos x raíz primitiva de orden p^n-1 que engendra $GF(p^n)^*$ por el Teorema 3.1.2 , entonces nos queda finalmente

$$\bigcup_{i=0}^{t-1} \Delta(x^{2i}A) = \bigcup_{j=0}^{p^n-2} [x^j] = \bigcup_{j=0}^{p^n-2} \{x^j\} = GF(p^n) \setminus \{0\}.$$

En este caso el multiconjunto es igual al conjunto, ya que no se repite ningún elemento.
Luego hemos probado que $x^{2i}A$, $i = 0, 1, ..., t - 1$, es una familia de diferencias. Finalmente, aplicando el Teorema 2.1.3 , obtenemos el desarrollo de la familia de diferencias, el cual nos proporciona un $(12t + 1, 4, 1)$-BIBD.

□

De acuerdo con [2, pág. 491] , en el teorema anterior, la hipótesis $x^{4t} - 1 = x^h$ es equivalente a

$(-3)^{\frac{p^n-1}{4}} \neq 1$ en $GF(p^n)$. Por ejemplo, este teorema se puede aplicar para $v = 25,\ 73,\ 97$, pero no para $v = 37$ ó 49.

Veamos un ejemplo en el que este teorema puede ser aplicado.

Ejemplo 3.1.5. Sea el cuerpo finito $\mathbb{F}_{13}$, $v = 12 \cdot 1 + 1 = 13$ es un número primo, luego potencia de un número primo. Queremos ver, en primer lugar, que 2 es raíz primitiva. Tenemos que $2^{13-1} = 2^{12} = 4096$, y al estar en un cuerpo de característica 13, se tiene entonces que $2^{12} = 1$, luego tenemos que el orden de 2 divide a 12. En $\mathbb{F}_{13}$,

$$2^6 = 64 = 12 \neq 1, \quad 2^4 = 16 = 3 \neq 1,$$

es decir, el orden de 2 no es ni 4 ni 6. Por tanto, como teníamos que el orden de 2 divide a 12, deducimos que el orden de 2 tiene que ser 12 y 2 es raíz primitiva en $\mathbb{F}_{13}$. Para comprobar la última hipótesis, vemos que $2^4 - 1 = 15 = 2 \bmod 13$. Luego aplicando el teorema anterior tenemos que el desarrollo de la familia de diferencias $A = \{0, 1, 2^4, 2^8\} = \{0, 1, 3, 9\}$, es decir,

$$g \ + \ \{0, 1, 3, 9\} \ : \ g \in \mathbb{F}_{13}$$

constituye un $(13, 4, 1)$-BIBD sobre $\mathbb{F}_{13}$.

3.2. Construcciones concretas de $(v, 4, 1)$-BIBD

Estudiaremos ahora construcciones concretas de $(v, 4, 1)$-BIBD para valores pequeños de v y mostraremos, en ciertos casos, las representaciones gráficas de cómo están representados los bloques dentro de, por ejemplo, el plano afín o el plano proyectivo. Además, expondremos algún ejemplo de cómo se podrían integrar estos BIBD en aplicaciones reales.

Recordemos que dos $(v, 4, 1)$-BIBD, $(V_1, \mathcal{B}_1)$ y $(V_2, \mathcal{B}_2)$, son isomorfos si existe una biyección $\alpha : V_1 \longrightarrow V_2$ que envía a cada bloque de $\mathcal{B}_1$ en un bloque de $\mathcal{B}_2$. De acuerdo con [16], mostramos en el Cuadro 3.2 el número de $(v, 4, 1)$-BIBD no isomorfos $(N(v))$ para cada v. Respecto al crecimiento de $N(v)$, Doyen fue el primero en demostrar que $N(v)$ tiende a infinito cuando v tiende a infinito.

v	**N(v)**
13	1
16	1
25	18
28	$\geqslant 4653$
37	$\geqslant 51402$
40	$\geqslant 1108800$
49	$\geqslant 769$
52	$\geqslant 206$
61	$\geqslant 18132$
64	$\geqslant 14 \cdot 10^{30}$

Cuadro 3.2: $(v, 4, 1)$-BIBD no ismorfos.

Empecemos a describir los $(v, 4, 1)$-BIBD empezando por valores de v pequeños e incrementando

su valor progresivamente. En algunos casos, para un mismo valor de v, estudiaremos distintos $(v, 4, 1)$-BIBD no isomorfos.

- De manera trivial, para $\mathbf{v = 4}$, el $(4, 4, 1)$-BIBD definido sobre $\mathbb{Z}/(4)$ está compuesto por un único bloque $\{1, 2, 3, 4\}$.

- El caso $\mathbf{v = 13}$ fue estudiado en el primer capítulo, en el Ejemplo 1.2.2 , en el que vimos que este $(13, 4, 1)$-BIBD nos daba una construcción del plano proyectivo sobre el plano afín $\mathbb{F}_3^2$. Como podemos observar en el Cuadro 3.2, solo hay un $(13, 4, 1)$-BIBD no isomorfo. Luego el $(13, 4, 1)$-BIBD obtenido aplicando un teorema sobre cuerpos finitos que acabamos de ver en el Ejemplo 3.1.5 es isomorfo al anterior.

3.2.1. $(16, 4, 1)$-BIBD

Como se puede observar en [11], el caso $\mathbf{v = 16}$ nos da una construcción sobre el plano afín $\mathbb{F}_4^2$. Recordemos el cuerpo finito $\mathbb{F}_4 = \frac{\mathbb{F}_2[x]}{(x^2+x+1)} = \{a + bx \quad : \quad a, b \in \mathbb{F}_2\}$. En este cuerpo de característica 2 se definen las operaciones considerando que $x^2 = x + 1$. Por ejemplo, tenemos que $x^3 = x^2x = (x + 1)x = x^2 + x = x + 1 + x = 2x + 1 = 1$.

Con las operaciones descritas anteriormente representaremos sobre el plano afín $\mathbb{F}_4^2$ este $(16, 4, 1)$-BIBD. Como en anteriores ocasiones, los elementos están representados como puntos y los bloques como rectas. Los elementos que representan nuestro $(16, 4, 1)$-BIBD los expresaremos de la forma (g, h) con $g = a_0 + a_1x$, $h = b_0 + b_1x$, $a_0, a_1, b_0, b_1 \in \mathbb{F}_2$. Los 20 bloques son los siguientes:

- 4 bloques de la forma $\{(0, h), (1, h), (x, h), (x^2, h)\}$, $h \in \mathbb{F}_4$.

- 4 bloques de la forma $\{(g, 0), (g, 1), (g, x), (g, x^2)\}$, $g \in \mathbb{F}_4$.

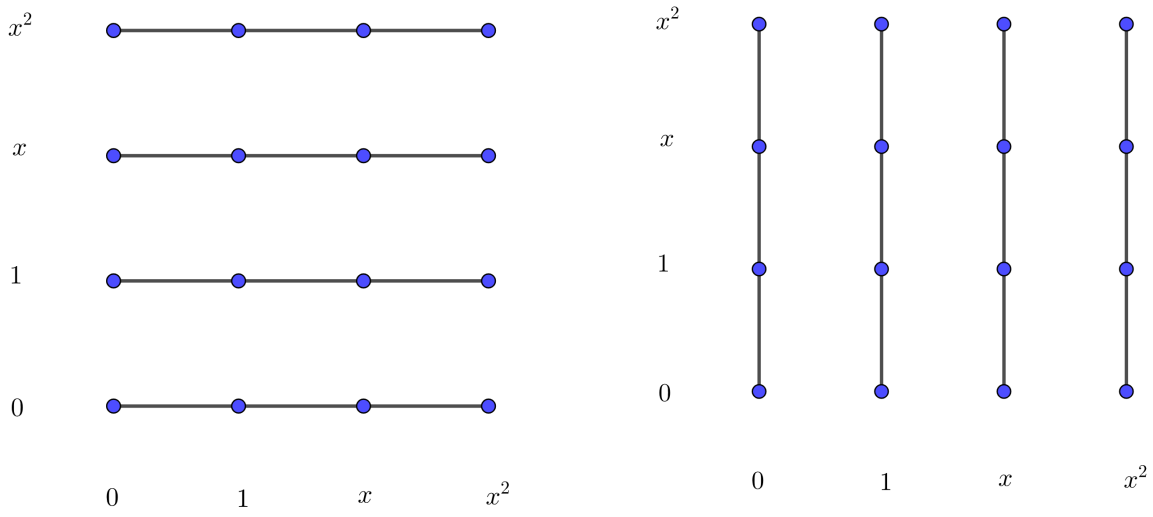
- 12 bloques de la forma $\{(g, 0), (g + x^\beta, 1), (g + x^{\beta+1}, x), (g + x^{\beta+2}, x^2)\}$, $g \in \mathbb{F}_4$, $\beta = 0, 1, 2$.

Observemos la representación de los tres tipos de rectas en las Figuras 3.1 y 3.2 . Como estamos en el plano afín $\mathbb{F}_4^2$, tenemos las coordenadas marcadas por 0, 1, x y $x^2 = x + 1$. En cada una de las cinco gráficas vemos que por cada punto pasa una única recta, y como tenemos 5 gráficas confirmamos que el número de replicación es $r = 5$. Además, observando cada par de puntos distintos con detenimiento, podemos apreciar que cada par de puntos distintos sólo está contenido en una única recta de las 20 totales, es decir, $\lambda = 1$.

A partir de este ejemplo, tomando los puntos como elementos y las rectas conteniendo 4 elementos como los bloques, podemos construir dos nuevos $(v, 4, 1)$-BIBD:

- En $\mathbb{F}_4^3$ tenemos un $(4^3, 4, 1)$-BIBD, es decir, un $(64, 4, 1)$-BIBD.

- En $\mathbb{F}_4^4$ tenemos un $(4^4, 4, 1)$-BIBD, es decir, un $(256, 4, 1)$-BIBD.



(a) $\{(0,h),(1,h),(x,h),(x^2,h)\}$ (b) $\{(g,0),(g,1),(g,x),(g,x^2)\}$

Figura 3.1: Rectas horizontales y verticales.

3.2.2. $(25,4,1)$-BIBD

Observemos ahora el caso $\mathbf{v = 25}$, en el que, de acuerdo con [4], aplicaremos el Teorema 3.1.4 sobre cuerpos finitos de la sección anterior para construir el desarrollo de una familia de diferencias. Sea el cuerpo finito $\mathbb{F}_{25} = \frac{\mathbb{F}_5[x]}{(x^2-3x-2)} = \{a+bx \ : \ a,b \in \mathbb{F}_5\}$ de característica 5 donde se cumple que $x^2 = 3x+2$.

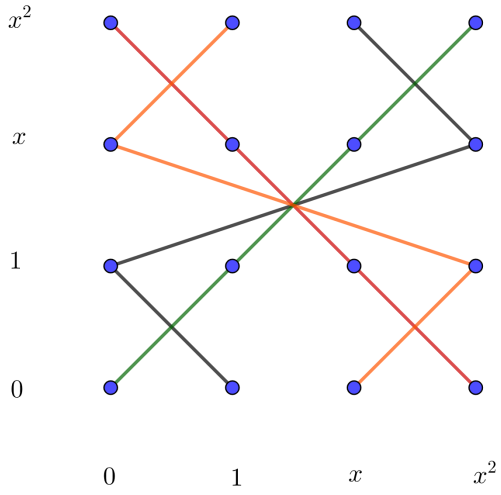
Tenemos que x y x^5 son las dos raíces del polinomio primitivo $x^2-3x-2 \in \mathbb{F}_5[x]$. Tomemos x, que es una raíz primitiva en $\mathbb{F}_{25}$, para aplicar el Teorema 3.1.4 anterior. Nos falta comprobar que $x^8-1 = x^h$ siendo h un número impar. Comprobémoslo teniendo en cuenta que $x^2 = 3x+2$ y que estamos en un cuerpo de característica 5:

$$x^4 = (3x+2)^2 = 9x^2+12x+4 = 4x^2+2x+4 = 12x+8+2x+4 = 4x+2$$
$$x^8-1 = (x^4-1)(x^4+1) = (4x+1)(4x+3) = 16x^2+16x+3 = x^2+x+3 = 4x$$
$$x^{13} = (x^4)^3x = (4x+2)^4x = \ldots = 4x$$

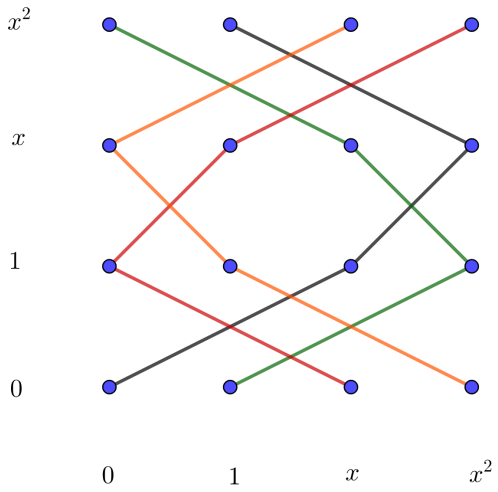
Es decir, tenemos $x^8-1 = x^{13}$, y 13 es un número impar, luego aplicando el Teorema 3.1.4 concluimos que el desarrollo de la familia de diferencias $\{A_1,A_2\}$ con $A_1 = \{0,1,x^8,x^{16}\} = \{0,1,4x+1,x+3\}$, $A_2 = \{0,x^2,x^{10},x^{18}\} = \{0,3x+2,2x+1,2\}$ forma un $(25,4,1)$-BIBD. Tomando los elementos $g \in \mathbb{F}_{25}$ como $g = ax+b$ con $a,b \in \{0,1,2,3,4\}$, podemos expresar este desarrollo como

$$g \ + \ A_i \ : \ g \in \mathbb{F}_{25}, \ i = 1,2,$$

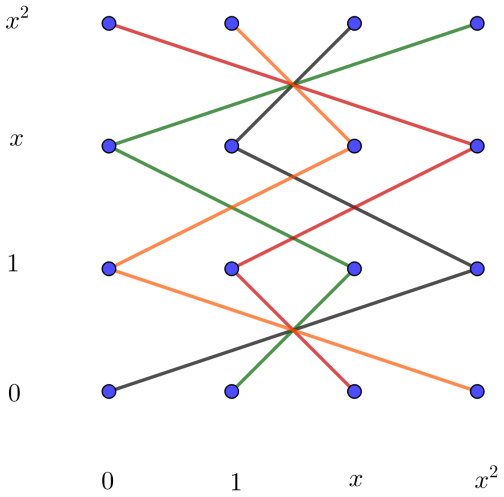
por lo que nuestro $(25,4,1)$-BIBD ya está construido.



(a) $\beta = 0$



(b) $\beta = 1$



(c) $\beta = 2$

Figura 3.2: Rectas de la forma $\{(g, 0), (g + x^{\beta}, 1), (g + x^{\beta+1}, x), (g + x^{\beta+2}, x^2)\}$.

3.2.3. $(28, 4, 1)$-BIBD

En este capítulo ya hemos representado un $(v, 4, 1)$-BIBD sobre el plano proyectivo, otro sobre el plano afín, y hemos construido uno gracias a un teorema sobre los cuerpos finitos. Estudiaremos ahora, para $\mathbf{v = 28}$, un $(28, 4, 1)$-BIBD desarrollado gracias al Teorema 2.2.4, en el que hallaremos el desarrollo que forma un BIBD gracias a una familia de diferencias relativa (véase [2]).

Sea $G = \mathbb{Z}/(27) = \mathbb{Z}/(3) \times \mathbb{Z}/(3) \times \mathbb{Z}/(3)$. Las ternas $\{x, y, z\}$ las abreviaremos escribiendo xyz. Sea el subgrupo $H = \{00a \ : \ a \in \mathbb{Z}/(3)\} = \{0\} \times \{0\} \times \mathbb{Z}/(3)$ contenido en G, veamos que $B_1 = \{000, 020, 111, 211\}$, $B_2 = \{000, 102, 012, 110\}$ es una $(27, 4, 1)$-familia de diferencias relativa a H, es decir, que $G \setminus H = \Delta B_i \sqcup \Delta B_2$, unión disjunta. Operando, tenemos que

$$\Delta B_1 = \{020, 111, 211, 010, 222, 122, 121, 212, 221, 112, 100, 200\},$$
$$\Delta B_2 = \{102, 012, 110, 201, 021, 220, 120, 210, 022, 011, 101, 202\}.$$

Luego podemos apreciar que $G \setminus H = \Delta B_i \sqcup \Delta B_2$, es decir, B_1, B_2 constituyen una $(27, 4, 1)$-familia de diferencias relativas a H y, por el Teorema 2.2.4, concluimos que el desarrollo formado por los bloques

$$\{g + B_i \ : \ g \in \mathbb{Z}/(3) \times \mathbb{Z}/(3) \times \mathbb{Z}/(3), \quad i = 1, 2\},$$

junto con los bloques construidos gracias a las clases laterales de H

$$\{\{\infty\} \cup (t + H) \ : \ t \in \mathbb{Z}/(3) \times \mathbb{Z}/(3) \times \{0\}\},$$

constituye un $(28, 4, 1)$ BIBD definido sobre $G \cup \{\infty\}$.

Al ser un $(28, 4, 1)$-BIBD tiene que tener $\frac{28 \cdot 27}{4 \cdot 3} = 63$ bloques. Comprobamos que hay $27 \cdot 2 = 54$ bloques de la forma $\{g + B_i \ : \ g \in \mathbb{Z}/(3) \times \mathbb{Z}/(3) \times \mathbb{Z}/(3), \quad i = 1, 2\}$, y $\frac{|G|}{|H|} = 9$ bloques de la forma $\{\{\infty\} \cup (t + H)\}$, es decir, 63 bloques en total.

3.2.4. $(37, 4, 1)$-BIBD

Siguiendo con [2], veamos dos ejemplos de $(37, 4, 1)$-BIBD que han sido obtenidos de manera distinta y que nos dan dos BIBD no isomorfos. Sea, en ambos casos, $G = \mathbb{Z}/(37)$ el cuerpo donde vamos a definir nuestros BIBD.

1. En primer lugar, sea $B_1 = \{0, 1, 3, 24\}$, y sea la familia de diferencias $\{B_1, B_2, B_3\} = \{B_1, 10B_1, 26B_1\}$ obtenida al multiplicar B_1 por dos escalares. Operando y reduciendo en $\mathbb{Z}/(37)$ obtenemos lo siguiente:

   $$B_1 = \{0, 1, 3, 24\}, \ B_2 = 10B_1 = \{0, 10, 18, 30\}, \ B_3 = 26B_1 = \{0, 4, 26, 32\}.$$

   En $\mathbb{Z}/(37)$, se tiene $10^2 = 26$, luego esta familia se puede escribir como $\{B_1, 10B_1, 10^2B_1\}$. Además, $10^3 = 1$, es decir, $10^3B_1 = B_1$. Cuando se construye de esta manera una familia de diferencias, se denomina a 10 un *multiplicador*.

Hallemos ahora $\Delta B_1, \Delta B_2, \Delta B_3$:

$\Delta B_1 = [1, 3, 24, 36, 34, 13, 2, 35, 23, 14, 21, 16],\ \Delta B_2 = [10, 18, 30, 27, 19, 17, 8, 29, 20, 17, 12, 25],$

$$\Delta B_3 = [4, 26, 32, 33, 11, 5, 22, 15, 28, 9, 6, 31].$$

Podemos observar que $\Delta B_1 \cup \Delta B_2 \cup \Delta B_3$ contiene a cada elemento de $G \setminus \{0\}$ una única vez. Por lo tanto, por el Teorema 2.1.3, concluimos que el desarrollo

$$g + B_i \quad : \quad g \in \mathbb{Z}/(37),\ i = 1, 2, 3,$$

constituye un $(37, 4, 1)$-BIBD definido sobre $\mathbb{Z}/(37)$.

2. Para esta segunda construcción, escogemos una familia de diferencias $\{A_1, A_2, A_3\}$ en la que los tres conjuntos no se obtienen al multiplicar uno por un escalar, sino que no tienen una relación clara. Sean $A_1 = \{0, 1, 3, 24\}$, $A_2 = \{0, 4, 9, 15\}$, $A_3 = \{0, 7, 17, 25\}$. Nótese que $A_1 = B_1$, conjunto del ejemplo anterior. Operamos de igual manera que en el caso anterior y obtenemos que

$$\Delta A_1 = [1, 3, 24, 36, 34, 13, 2, 35, 23, 14, 21, 16],\ \Delta A_2 = [4, 9, 15, 33, 28, 22, 5, 32, 11, 26, 6, 31],$$

$$\Delta A_3 = [7, 17, 25, 30, 20, 12, 10, 27, 18, 19, 8, 29].$$

Podemos observar que $\Delta A_1 \cup \Delta A_2 \cup \Delta A_3$ también contiene a cada elemento de $G \setminus \{0\}$ una única vez. Por lo tanto, por el Teorema 2.1.3 concluimos que el desarrollo

$$g + B_i \quad : \quad g \in \mathbb{Z}/(37), i = 1, 2, 3,$$

nos proporciona otro $(37, 4, 1)$-BIBD definido sobre $\mathbb{Z}/(37)$.

Ambas familias de diferencias contienen el conjunto $\{0, 1, 3, 24\}$. La primera ha sido formada al multiplicar por 10 y por 10^2 a este conjunto, mientras que en la segunda no tenemos una relación significativa entre los tres conjuntos que constituyen la familia de diferencias. Por ello, los desarrollos de las familias de diferencias también son notablemente distintos, y podemos concluir que hemos encontrado dos desarrollos que constituyen dos $(37, 4, 1)$-BIBD no isomorfos.

3.2.5. $(40, 4, 1)$-BIBD

Estudiemos ahora una aplicación del Teorema 2.2.2 donde desarrollaremos un $(40, 4, 1)$-BIBD a partir de una $(40, 4, 1)$-familia de diferencias relativa definida sobre $\mathbb{Z}/(40)$ (véase [7]).

Sea $H = \{0, 10, 20, 30\}$ un subgrupo de $\mathbb{Z}/(40)$. Una $(40, 4, 1)$-familia de diferencias relativa a H es $\{B_1, B_2, B_3\}$ con

$$B_1 = \{0, 1, 4, 13\}, \quad B_2 = \{0, 2, 7, 24\}, \quad B_3 = \{0, 6, 14, 25\}.$$

Comprobémoslo. Operando obtenemos que

$$\Delta B_1 = \{1, 4, 13, 39, 36, 27, 3, 37, 12, 28, 9, 31\}, \quad \Delta B_2 = \{2, 7, 24, 38, 33, 16, 5, 35, 22, 18, 17, 23\},$$

$$\Delta B_3 = \{6, 14, 25, 34, 26, 15, 8, 32, 19, 21, 11, 29\}.$$

Podemos observar que $\mathbb{Z}/(40) \setminus H = \bigsqcup_{i=1}^{3} \Delta B_i$, por lo tanto, $\{B_1, B_2, B_3\}$ es una $(40, 4, 1)$-familia de diferencias relativa a H.

Aplicando el Teorema 2.2.2, concluimos que el desarrollo formado por los bloques

$$\{g + B_i \quad : \quad g \in \mathbb{Z}/(40),\ i = 1, 2, 3\},$$

junto con los bloques de ciclo corto

$$\{t + \{0, 10, 20, 30\} \ : \ t \in \{0, 1, 2, \ldots 8, 9\}\},$$

constituye un $(40, 4, 1)$-BIBD definido sobre $\mathbb{Z}/(40)$.
Al ser un $(40, 4, 1)$-BIBD, tiene que tener $\frac{40 \cdot 39}{4 \cdot 3} = 130$ bloques. Comprobamos que hay $40 \cdot 3 = 120$ bloques de la forma $\{g + B_i\}$, y 10 bloques de ciclo corto, luego 130 bloques en total.

3.2.6. $(49, 4, 1)$-BIBD

El siguiente BIBD lo obtendremos a partir de una familia de diferencias formada de una manera interesante que no habíamos visto hasta ahora, gracias a [6]. Construiremos un $(49, 4, 1)$-BIBD sobre $\mathbb{Z}/(49)$. Dado un conjunto $B_1 = \{0, 1, 3, 15\}$, obtenemos $B_2 = 18B_1 = \{0, 5, 18, 25\}$ a partir de B_1, $B_3 = 18B_2 = \{0, 9, 30, 41\}$ a partir de B_2 y, por último, $B_4 = \{0, 4, 10, 26\}$ sin ser producto por un escalar de ninguno de los anteriores ni guardar ninguna relación significativa con ellos. Operando, hallamos los $\Delta B_i,\ i = 1, 2, 3, 4$:

$$\Delta B_1 = [1, 3, 15, 48, 46, 34, 2, 47, 14, 35, 12, 37], \ \Delta B_2 = [5, 18, 25, 44, 31, 24, 13, 36, 20, 29, 7, 42],$$

$$\Delta B_3 = [9, 30, 41, 40, 19, 8, 21, 28, 32, 17, 11, 38], \ \Delta B_4 = [4, 10, 26, 45, 39, 23, 6, 43, 22, 27, 16, 33].$$

Si observamos con detalle, podemos ver que $\bigcup_{i=1}^{4} \Delta B_i$ contiene a todos los elementos de $\mathbb{Z}/(49) \setminus \{0\}$ y, por tanto, $\{B_1, B_2, B_3, B_4\}$ es una familia de diferencias definida sobre $\mathbb{Z}/(49)$. Como es un número relativamente alto para poder comprobarlo a simple vista, hemos hecho un pequeño programa de Matlab que nos comprueba si tenemos realmente una familia de diferencias. Véase el Apéndice. Como hemos comprobado que $\{B_1, B_2, B_3, B_4\}$ es una $(49, 4, 1)$-familia de diferencias, por el Teorema 2.1.3, concluimos que el desarrollo

$$g + B_i \quad : \quad g \in \mathbb{Z}/(49),\ i = 1, 2, 3, 4,$$

constituye un $(49, 4, 1)$-BIBD definido sobre $\mathbb{Z}/(49)$.

3.2.7. $(52, 4, 1)$-BIBD

Veamos ahora, de acuerdo con [7], otra aplicación del Teorema 2.2.2, en la que desarrollaremos un $(52, 4, 1)$-BIBD a partir de una $(52, 4, 1)$-familia de diferencias relativa definida sobre $\mathbb{Z}/(52)$.

Sea $H = \{0, 13, 26, 39\}$ un subgrupo de $\mathbb{Z}/(52)$. Tenemos una $(52, 4, 1)$-familia de diferencias relativa a H formada por $\{B_1, B_2, B_3, B_4\}$:

$$B_1 = \{0, 1, 3, 7\}, \quad B_2 = \{0, 5, 19, 35\}, \quad B_3 = \{0, 8, 20, 31\}, \quad B_4 = \{0, 9, 24, 34\}.$$

Ya que empezamos a tener valores de v altos, hemos creado un programa de Matlab, similar al de las familias de diferencias, para calcular los ΔB_i y comprobar una familia de diferencias relativa. Véase el Apéndice.
Se tiene que $(\mathbb{Z}/(52)) \setminus H = \bigsqcup_{i=1}^{4} \Delta B_i$, por lo tanto, $\{B_1, B_2, B_3, B_4\}$ es una $(52, 4, 1)$-familia de diferencias relativa a H.

Aplicando el Teorema 2.2.2, concluimos que el desarrollo formado por los bloques

$$\{g + B_i \quad : \quad g \in \mathbb{Z}/(52),\ i = 1, 2, 3, 4\},$$

junto con los bloques de ciclo corto

$$\{t + \{0, 13, 26, 39\} \ : \ t \in \{0, 1, 2, \ldots 11, 12\}\},$$

constituye un $(52, 4, 1)$-BIBD definido sobre $\mathbb{Z}/(52)$.
Por ser un $(52, 4, 1)$-BIBD, tiene que tener $\frac{52 \cdot 51}{4 \cdot 3} = 221$ bloques. Comprobamos que hay $52 \cdot 4 = 208$ bloques de la forma $\{g + B_i\}$, y 13 bloques de ciclo corto, luego 221 bloques en total.

3.2.8. $(61, 4, 1)$-BIBD

Volvemos a [6], y construimos un $(61, 4, 1)$-BIBD a partir de una familia de diferencias. En este caso, la familia de diferencias está definida sobre $\mathbb{Z}/(61)$. Dado $B_1 = \{0, 1, 5, 11\}$, obtenemos los demás B_i a partir de B_1 de la siguiente manera:

$$B_1 = \{0, 1, 5, 11\}, \quad B_{i+1} = 9^i B_1,\ i = 1, 2, 3, 4.$$

Además, en $\mathbb{Z}/(61)$, $9^5 = 1$, luego el elemento $9 \in \mathbb{Z}/(61)$ se denomina multiplicador de la familia de diferencias.

Operando en $\mathbb{Z}/(61)$ obtenemos los siguientes conjuntos:

$$B_1 = \{0, 1, 5, 11\},\ B_2 = \{0, 9, 38, 45\},\ B_3 = \{0, 20, 37, 39\},$$

$$B_4 = \{0, 28, 46, 58\},\ B_5 = \{0, 8, 34, 48\}.$$

Al igual que en el $(49, 4, 1)$-BIBD, en el Apéndice hemos programado todas las diferencias, y hemos comprobado que $\{B_1, B_2, B_3, B_4, B_5\}$ es una $(61, 4, 1)$-familia de diferencias. Por tanto, de nuevo

por el Teorema 2.1.3 , concluimos que el desarrollo

$$g + B_i \quad : \quad g \in \mathbb{Z}/(61),\ i = 1, 2, 3, 4, 5,$$

constituye un $(61, 4, 1)$-BIBD definido sobre $\mathbb{Z}/(61)$.

3.2.9. $(64, 4, 1)$-BIBD

En la Sección 3.2.1, vimos que en el espacio afín $\mathbb{F}_4^3$ se puede construir un $(64, 4, 1)$-BIBD tomando los bloques como rectas. Veamos ahora otra manera de formar un $(64, 4, 1)$-BIBD.

De acuerdo con [7], y para terminar con las construcciones concretas de $(v, 4, 1)$-BIBD, vamos a desarrollar un $(64, 4, 1)$-BIBD a partir de una $(64, 4, 1)$-familia de diferencias relativa definida sobre $\mathbb{Z}/(64)$.

Sea $H = \{0, 16, 32, 48\}$ un subgrupo de $\mathbb{Z}/(64)$. Una $(64, 4, 1)$-familia de diferencias relativa a H es $\{B_1, B_2, B_3, B_4, B_5\}$ con

$$B_1 = \{0, 1, 3, 7\}, \quad B_2 = \{0, 5, 18, 47\}, \quad B_3 = \{0, 8, 33, 44\},$$

$$B_4 = \{0, 9, 19, 43\}, \quad B_5 = \{0, 12, 26, 49\}.$$

Al igual que en el $(52, 4, 1)$-BIBD, podemos comprobar en el Apéndice que $(\mathbb{Z}/(64)) \setminus H = \bigsqcup_{i=1}^{5} \Delta B_i$, por lo tanto, $\{B_1, B_2, B_3, B_4, B_5\}$ es una $(64, 4, 1)$-familia de diferencias relativa a H.

Aplicando de nuevo el Teorema 2.2.2, concluimos que el desarrollo formado por los bloques

$$\{g + B_i \quad : \quad g \in \mathbb{Z}/(64),\ i = 1, 2, 3, 4, 5\},$$

junto con los bloques de ciclo corto

$$\{t + \{0, 16, 32, 48\} \ : \ t \in \{0, 1, 2, \ldots 14, 15\}\},$$

constituye un $(64, 4, 1)$-BIBD definido sobre $\mathbb{Z}/(64)$.
Como es un $(64, 4, 1)$-BIBD, tiene exactamente $\frac{64 \cdot 63}{4 \cdot 3} = 336$ bloques. Comprobamos que hay $64 \cdot 5 = 320$ bloques de la forma $\{g + B_i\}$, y 16 bloques de ciclo corto, luego 336 bloques en total.

3.2.10. Aplicación real

En el campo de los BIBD, he encontrado que, además de todas éstas construcciones teóricas relacionadas con planos o cuerpos finitos, también hay numerosos estudios con intención de aplicar los BIBD en temas muy variados: comida, las preocupaciones por las enfermedades que causa el tabaco, análisis en medicina, o también para analizar temas de consumo en una sociedad.

Este último me resulta especialmente interesante. Hay estudios que demuestran que, al encuestar a un consumidor con distintas preguntas sobre un producto o un tema cualquiera, el consumidor no responde con el mismo interés en las primeras preguntas que en las últimas, ya sea por cansancio

o aburrimiento. Es aquí donde entra la utilidad de aplicar un BIBD, ya que podemos reducir el número de preguntas a cada consumidor pero a la vez seguir obteniendo un amplio número de respuestas, y además más significativas al no afectar tanto la fatiga. Otro aspecto que afecta a las encuestas es que las respuestas también están condicionadas por las preguntas anteriores recién respondidas. Aplicando los BIBD tendremos que a cada consumidor se le preguntarán distintas combinaciones de preguntas, y cada par de preguntas distintas serán preguntadas juntas de manera equivalente para todas las preguntas. Pongamos un ejemplo.

Ejemplo 3.2.1. Imaginemos que somos los dueños de un prestigioso restaurante y queremos averiguar qué factor influye más al cliente a la hora de elegir un vino, y después, interpretando los resultados, podríamos cambiar la manera de exponer los distintos vinos al cliente y vender más un vino de acuerdo a nuestros intereses.

En este tipo de encuestas, v es el número de preguntas. En este caso, les mostraremos distintos factores de por qué eligen un vino, y ellos tendrán que elegir los que ellos consideren más significativos. En nuestro caso v será 16, y unos ejemplos de los factores posibles son los siguientes: la descripción del sabor del vino en el menú, el orden en que aparece el vino en la carta, la afinidad del vino con la comida elegida, el tipo de uva, el precio, si el camarero me lo ha recomendado, etc.

Si mostráramos los 16 factores a cada cliente, les sería difícil leerlos bien todos y elegir. Además, puede ser un poco molesto hacer una encuesta así a un cliente después de comer, sin embargo, le resultaría más fácil si sólo le ponemos $k = 4$ factores para elegir. Cada cliente será un bloque, y se hará la encuesta a 400 clientes, es decir, 20 grupos de 20 bloques, lo cual es equivalente a aplicar 20 veces un $(16, 4, 1)$-BIBD.

El valor $\lambda = 1$ es también un dato interesante ya que, en las 400 encuestas, cada par de factores distintos solo aparecerán juntos en 20 ocasiones, lo que propicia que un factor no eclipse siempre a otro. Por último, tenemos que cada factor aparecerá en $r = 5$ ocasiones por BIBD, es decir, cada factor aparecerá en 100 de las 400 encuestas.

Como hemos podido observar en [9] y en [20], hay estudios que aplican la estadística en el campo de los diseños y comparan distintos BIBD variando, por ejemplo, el número de elementos por bloques, para después interpretar qué BIBD nos dan los resultados más interesantes y significativos en nuestro proyecto. Recíprocamente, los BIBD también son utilizados en la estadística, por ejemplo, cuando se quieren hacer estudios en medicina sobre el efecto de distintos medicamentos ante una enfermedad. Es inviable administrar todos los medicamentos a cada persona, por lo que se hacen estudios aplicando a cada paciente una combinación distinta de un pequeño número de medicamentos y así, después, poder sacar conclusiones del efecto ocasionado por cada medicamento.

Capítulo 4

Construcciones inductivas de $(v, 4, 1)$-BIBD

En el primer capítulo introdujimos una serie de construcciones inductivas para los sistemas triples de Steiner. En el capítulo anterior hemos empezado a profundizar en los $(v, 4, 1)$-BIBD, en el que hemos desarrollado, con distintos métodos, $(v, 4, 1)$-BIBD para ciertos valores de v. En este capítulo seguiremos centrándonos en los $(v, 4, 1)$-BIBD, pero en vez formar estos diseños para un v fijo, estudiaremos cómo desarrollar distintos BIBD a partir de otros dados, sin importar el valor de v. Es decir, desarrollaremos varias construcciones inductivas de $(v, 4, 1)$-BIBD. Además, introduciremos los transversal designs que, a pesar de ser un tipo de diseño distinto a los BIBD, nos ayudarán en el desarrollo de ciertos bloques para poder completar varias construcciones inductivas de $(v, 4, 1)$-BIBD.

Antes de comenzar con las construcciones, veamos la definición de un concepto que nos será útil en ciertos BIBD de este capítulo, los subsistemas.

Definición 4.0.1. *Sea $(V, \mathcal{B})$ un (v, k, λ)-BIBD. Sea $W \subseteq V$ con $|W| = w$, y sea $\mathcal{C} \subseteq \mathcal{B}$. Se define $(W, \mathcal{C})$ como un **subsistema** de $(V, \mathcal{B})$ si se cumple que $(W, \mathcal{C})$ es un (w, k, λ)-BIBD.*

4.1. $(v \cdot w, 4, 1)$-BIBD

En esta primera construcción estudiaremos cómo, a partir de un $(v, 4, 1)$-BIBD y un $(w, 4, 1)$-BIBD, formar un $(v \cdot w, 4, 1)$-BIBD. Sea $(V, \mathcal{B})$ un $(v, 4, 1)$-BIBD y $(W, \mathcal{C})$ un $(w, 4, 1)$-BIBD. Denotemos por b y c el número de bloques del $(v, 4, 1)$-BIBD y del $(w, 4, 1)$-BIBD respectivamente.

Dados $x_i \in V$, $y_i \in W$, $i = 1, 2, 3, 4$, identificamos cada conjunto $\{x_1, x_2, x_3, x_4\} \times \{y_1, y_2, y_3, y_4\}$ con el plano afín $\mathbb{F}_4^2$. Véase la página 35 donde se define un $(16, 4, 1)$-BIBD sobre $\mathbb{F}_4^2$.
Definimos los bloques del $(v \cdot w, 4, 1)$-BIBD definido sobre $V \times W$ de la siguiente manera:

$$\{(x_1, y_1), (x_2, y_2), (x_3, y_3), (x_4, y_4)\},$$

donde se tiene que cumplir una de las siguientes condiciones:

- $x_1 = x_2 = x_3 = x_4 \in V$ con $\{y_1, y_2, y_3, y_4\}$ bloque del $(w, 4, 1)$-BIBD. Estos bloques se representan como rectas verticales en el plano $\{x_1, x_2, x_3, x_4\} \times \{y_1, y_2, y_3, y_4\}$. Fijando un elemento de los v posibles de V y los c bloques totales del $(w, 4, 1)$-BIBD, obtenemos $v \cdot c$ bloques de la primera forma.

- $y_1 = y_2 = y_3 = y_4 \in W$ con $\{x_1, x_2, x_3, x_4\}$ bloque del $(v, 4, 1)$-BIBD. Estos bloques se representan como rectas horizontales en el plano $\{x_1, x_2, x_3, x_4\} \times \{y_1, y_2, y_3, y_4\}$.
  Fijando un elemento de los w posibles de W y los b bloques totales del $(v, 4, 1)$-BIBD, obtenemos $w \cdot b$ bloques de la segunda forma.

- Por último, queremos ver cuántos bloques posibles hay para cada $\{x_1, x_2, x_3, x_4\} \in \mathcal{B}$, $\{y_1, y_2, y_3, y_4\} \in \mathcal{C}$. Sea $\{x_1, x_2, x_3, x_4\} \times \{y_1, y_2, y_3, y_4\}$ el plano que identificamos con el plano afín $\mathbb{F}_4^2$.
  En el $(16, 4, 1)$-BIBD definido sobre $\mathbb{F}_4^2$, las rectas representan a los bloques del BIBD. Como ya tenemos las rectas horizontales y verticales incluidas en los dos anteriores casos, solo estamos interesados en las 12 rectas inclinadas restantes que nos determinan los bloques de esta forma (véase la página 37). Es decir, para cada $\{x_1, x_2, x_3, x_4\} \in \mathcal{B}$, $\{y_1, y_2, y_3, y_4\} \in \mathcal{C}$, tenemos 12 bloques distintos de esta forma.

  Por tanto, hay $12 \cdot b \cdot c$ bloques construidos de esta manera.

Se puede observar que hemos construido un $(v \cdot w, 4, 1)$-BIBD sobre $V \times W$, ya que tenemos $v \cdot w$ elementos y en cada bloque tenemos cuatro elementos distintos de $V \times W$. Además, se han definido los bloques de manera que cada par de elementos distintos de $V \times W$ esté contenido en un único bloque.
Comprobemos, para terminar, que sumando el número de bloques posibles de los tres casos obtenemos el mismo resultado que en la Proposición 1.1.5, es decir, que el número total de bloques es $\frac{vw(vw-1)}{12}$:

$$vc + wb + 12bc =$$

$$= v\frac{w(w-1)}{12} + w\frac{v(v-1)}{12} + 12\frac{v(v-1)}{12}\frac{w(w-1)}{12} =$$

$$= \frac{vw}{12}(v - 1 + w - 1 + (w-1)(v-1)) =$$

$$= \frac{vw}{12}(vw - 1)$$

Finalmente, comprobamos que nos queda $\frac{vw(vw-1)}{12}$, como queríamos. Hemos terminado entonces de construir nuestro $(v \cdot w, 4, 1)$-BIBD definido sobre $V \times W$.

En particular, dado $(V, \mathcal{B})$ un $(v, 4, 1)$-BIBD y el $(4, 4, 1)$-BIBD definido sobre $\mathbb{Z}/(4)$ y formado por la cuaterna $\{1, 2, 3, 4\}$, podemos formar un $(4v, 4, 1)$-BIBD definido sobre $V \times \mathbb{Z}/(4)$.

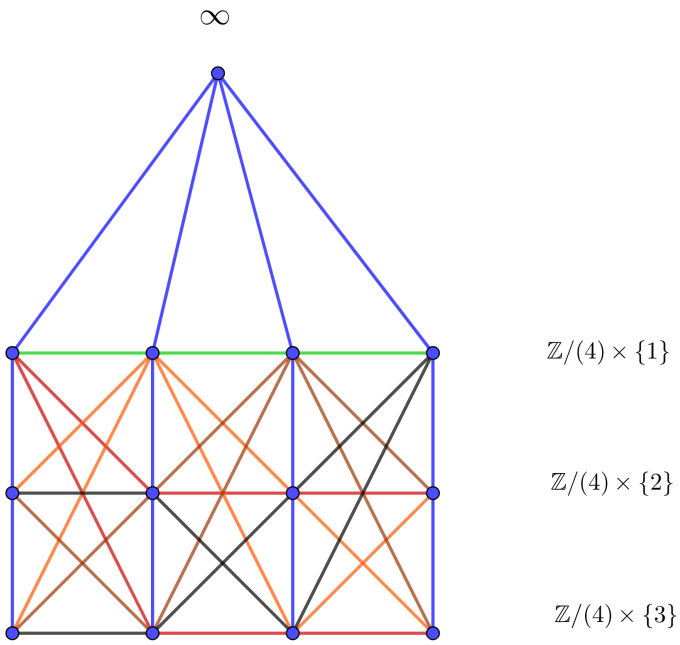


Figura 4.1: Bloques definidos sobre $(\mathbb{Z}/(4) \times \{1,2,3\}) \cup \{\infty\}$.

4.2. $(3v+1,4,1)$-BIBD

Describiremos ahora una segunda construcción inductiva, en este caso un $(3v+1,4,1)$-BIBD formado a partir de un $(v,4,1)$-BIBD. Ésta es una construcción clásica que puede verse en [11]. Dado un $(v,4,1)$-BIBD $(V,\mathcal{B})$, definiremos nuestro $(3v+1,4,1)$-BIBD sobre $W = (V \times \{1,2,3\}) \cup \{\infty\}$, siendo ∞, como en otras ocasiones, $\infty \notin V \times \{1,2,3\}$.

En primer lugar, describamos un $(3 \cdot 4+1,4,1)$-BIBD definido sobre $(\mathbb{Z}/(4) \times \{1,2,3\}) \cup \{\infty\}$, es decir, un $(13,4,1)$-BIBD, a partir del $(4,4,1)$-BIBD definido sobre $\mathbb{Z}/(4)$ formado únicamente por la cuaterna $\{1,2,3,4\}$. En total, nuestro $(13,4,1)$-BIBD contiene $\frac{13\cdot 12}{12} = 13$ bloques o cuaternas. Definimos estos bloques, representados en la Figura 4.1, de la siguiente manera:

- 4 bloques de la forma $\{(x,1),(x,2),(x,3),\infty\},\ x \in \mathbb{Z}/(4)$. Gráficamente se expresan en azul como rectas verticales incluyendo el ∞.
- 1 bloque de la forma $\{(1,1),(2,1),(3,1),(4,1)\}$, que podemos observar que es la cuaterna de nuestro $(4,4,1)$-BIBD representada sobre $\mathbb{Z}/(4) \times \{1\}$. Gráficamente es una recta verde.
- Por último, los 8 bloques restantes vienen dados por la estructura del $(13,4,1)$-BIBD, no se pueden describir de una forma tan clara como los anteriores, como se puede observar gráficamente con colores oscuros. En este caso, éstos son los 8 bloques restantes:

$$\{(1,1),(2,2),(3,2),(4,2)\}, \quad \{(1,1),(2,3),(3,3),(4,3)\},$$

$$\{(2,1),(1,2),(3,2),(4,3)\}, \quad \{(2,1),(4,2),(1,3),(3,3)\},$$

$$\{(3,1),(1,2),(4,2),(2,3)\}, \quad \{(3,1),(2,2),(1,3),(4,3)\},$$

$$\{(4,1),(1,2),(2,2),(3,3)\},\quad \{(4,1),(3,2),(1,3),(2,3)\}.$$

Podemos observar que cada par de elementos distintos de $(\mathbb{Z}/(4)\times\{1,2,3\})\cup\{\infty\}$ están contenidos simultáneamente en un único bloque y, gráficamente, en una única recta. También podemos comprobar que el bloque $\{(1,1),(2,1),(3,1),(4,1)\}$ es un $(4,4,1)$-BIBD definido sobre $\mathbb{Z}/(4)\times\{1\}$, es decir, es un subsistema del $(13,4,1)$-BIBD definido sobre $(\mathbb{Z}/(4)\times\{1,2,3\})\cup\{\infty\}$. Esta descripción de los bloques del $(13,4,1)$-BIBD nos va a ayudar para construir y entender de una manera más clara nuestro $(3v+1,4,1)$-BIBD.

A partir de este caso con $v=4$ más sencillo, estudiemos a continuación cómo construir un $(3v+1,4,1)$-BIBD $(W,\mathcal{C})$ a partir de un $(v,4,1)$-BIBD $(V,\mathcal{B})$. En primer lugar, definimos $(W,\mathcal{C})$ sobre $W=(V\times\{1,2,3\})\cup\infty$, es decir, $|W|=3v+1$. Las cuaternas de $(W,\mathcal{C})$ son de la siguiente forma:

- v bloques de la forma $\{(x,1),(x,2),(x,3),\infty\},\ x\in V$.
- $\frac{v(v-1)}{12}$ bloques de la forma $\{(x_1,1),(x_2,1),(x_3,1),(x_4,1)\}$, siendo $\{x_1,x_2,x_3,x_4\}$ los bloques del $(v,4,1)$-BIBD inicial.
- Por último, los $\frac{(3v+1)3v}{12}-v-\frac{v(v-1)}{12}=\frac{2v(v-1)}{3}$ bloques restantes vienen dados por la estructura del $(3v+1,4,1)$-BIBD, no los podemos describir de una manera clara, como se ha visto en el $(13,4,1)$-BIBD anterior.

Éstos son los bloques que determinan nuestro $(3v+1,4,1)$-BIBD, por lo que hemos acabado con nuestra segunda construcción inductiva.

Para terminar, se puede observar que el segundo tipo de bloques, es decir, los bloques de la forma $\{(x_1,1),(x_2,1),(x_3,1),(x_4,1)\}$, siendo $\{x_1,x_2,x_3,x_4\}$ los bloques del $(v,4,1)$-BIBD, forman un subsistema del $(3v+1,4,1)$-BIBD, que es un $(v,4,1)$-BIBD definido sobre $V\times\{1\}$.

4.3. Transversal designs

En esta sección estudiaremos, en primer lugar, unos nuevos diseños combinatorios denominados *transversal designs*. Definiremos el concepto de transversal design y comprobaremos que son distintos a los diseños estudiados hasta el momento, los BIBD. Por otro lado, a pesar de su diferencia, veremos cómo podemos relacionar estos nuevos diseños con los BIBD, y cómo se pueden formar varias construcciones inductivas de $(v,4,1)$-BIBD gracias a los transversal designs.

Definición 4.3.1. [18] *Sea $k\geq 2$, $n\geq 1$. Un **transversal design** $TD(k,n)$ es una tripleta $(X,\mathcal{G},\mathcal{B})$ que cumple las siguientes propiedades:*

1. *X es un conjunto de $k\cdot n$ elementos denominados puntos.*
2. *$\mathcal{G}$ es una partición de X en k subconjuntos de cardinal n, denominados grupos:*

$$\mathcal{G}=\{G_1,G_2,\ldots,G_k\}.$$

3. *$\mathcal{B}$ es una familia de bloques de cardinal k,*

$$\mathcal{B} = \{B_1, B_2, \ldots, B_s\},$$

de manera que

- $|G_j \cap B_i| = 1,\ \ 1 \leq j \leq n,\ \ 1 \leq i \leq s.$
- *Cada par de puntos $x, y \in X$, $x \neq y$, x e y de distintos grupos, está contenido en un único bloque. Es decir, dados dos puntos de X distintos, si no están en un mismo grupo de $\mathcal{G}$, entonces están en un único bloque de $\mathcal{B}$.*

Nótese que el concepto de grupo que hemos descrito no tiene que ver con el concepto algebraico, en este caso sólo son subconjuntos de X. En nuestro caso, trabajaremos con TD$(4, n)$, es decir, con transversal designs que contengan $k = 4$ grupos, $\mathcal{G} = \{G_1, G_2, G_3, G_4\}$, y con bloques de cardinal $k = 4$, $|B_i| = 4$, $1 \leq i \leq s$.
Veamos para qué valores de n podemos construir TD$(4, n)$ y cómo definir los bloques en cada caso.

4.3.1. TD$(4, n)$ siendo n impar

Sea n impar, definimos nuestro TD$(4, n)$ sobre $\mathbb{Z}/(n) \times \{1, 2, 3, 4\}$. Los bloques de este transversal design están definidos de la siguiente forma:

$$\{(a, 1),\ (b, 2),\ (a + b, 3),\ (a - b, 4)\ :\ a, b \in \mathbb{Z}/(n)\}.$$

1. $|X| = 4 \cdot n$, luego la primera propiedad de los transversal designs se cumple.

2. $\mathcal{G} = \{\mathbb{Z}/(n) \times \{i\},\ i = 1, 2, 3, 4\}$ es una partición de X en 4 subconjuntos de cardinal n, luego también se cumple la segunda condición.

3. Para la última propiedad, vemos que la definición de los bloques determina que en cada bloque hay un único elemento de cada grupo $\mathbb{Z}/(n) \times \{i\}$. Por otra parte, sean dos elementos $(x, j),\ (y, h)$ distintos de distintos grupos, es decir, $j \neq h$. Supongamos, por ejemplo, $j = 1,\ h = 4$, entonces tomando $a = x,\ a - b = y$, obtenemos $b = x - y,\ a + b = 2x - y$.
   Por tanto, los elementos $(x, 1),\ (y, 4)$ van a estar simultáneamente en el único bloque

   $$\{(x, 1),\ (x - y, 2),\ (2x - y, 3),\ (y, 4)\}.$$

   Si, por ejemplo, hubiera sido $h = 3$, eligiendo $a + b = y$ habríamos obtenido el bloque buscado.

Al estar operando en $\mathbb{Z}/(n)$ con n impar, ningún elemento $\bar{z} \in \mathbb{Z}/(n)$ cumple que $\bar{z} = -\bar{z}$, luego esta definición de los bloques no nos da ningún problema para satisfacer la tercera propiedad. Sin embargo, veamos cómo esta descripción de los bloque no nos vale para todo n par.

Sea $\mathbb{Z}/(10)$, donde tenemos que $\bar{5} = -\bar{5}$. Con la descripción anterior de los bloques, si tomamos $a = 0,\ b = 5$ nos queda el siguiente bloque:

$$\{(0,1),\ (5,2),\ (5,3),\ (5,4)\}.$$

Si tomamos $a = 5,\ b = 0$, el bloque que nos queda en esta ocasión es

$$\{(5,1),\ (0,2),\ (5,3),\ (5,4)\}.$$

Luego los elementos $(5,3),\ (5,4)$ están simultáneamente en dos bloques, es decir, no se cumple la tercera propiedad.

Veamos un ejemplo sencillo de TD$(4,n)$ con n impar para entender mejor este diseño y sus propiedades.

Ejemplo 4.3.2. Dado $X = \mathbb{Z}/(5) \times \{1,2,3,4\}$, describiremos un TD$(4,5)$.
Los bloques de este diseño son de la siguiente forma:

$$\{(a,1),\ (b,2),\ (a+b,3),\ (a-b,4)\ :\ a,b \in \mathbb{Z}/(5)\}.$$

Tenemos $|X| = 4 \cdot 5 = 20$, y $\mathcal{G}$ distribuido en $k = 4$ grupos, $\mathbb{Z}/(5) \times \{i\},\ \ i = 1,2,3,4$. También hemos descrito los bloques de manera que son subconjuntos de $k = 4$ elementos. Nos falta comprobar la última propiedad de la definición de transversal design para concluir que tenemos realmente un TD$(4,5)$.
Dados dos elementos distintos $(x,j),\ (y,h)$, de distintos grupos, es decir, $j \neq h$, tienen que estar, por definición, en un único bloque. Supongamos $j = 1,\ h = 3$. En este caso, denotando $a = x$, $a + b = y$, obtenemos que $b = y - x,\ \ a - b = 2x - y$, es decir, los elementos de la forma $(x,1)$, $(y,3)$ están en el bloque

$$\{(x,1),\ (y-x,2),\ (y,3),\ (2x-y,4)\}.$$

Podemos observar, representado de una manera sencilla, un bloque de este TD$(4,5)$ en la Figura 4.2.

4.3.2. TD$(4,n)$ siendo n múltiplo de 4 y no múltiplo de 8

Veamos cómo relacionar la anterior definición de los bloques que forman un TD$(4,n)$ con n impar con la construcción de transversal designs para cierto n par. Si tenemos n múltiplo de 4 pero no múltiplo de 8, podemos escribir $n = 4 \cdot h$ siendo h impar. Como h es impar, podemos relacionar esta construcción con la anterior:
En primer lugar, se fija un elemento $w \in \mathbb{F}_4$, siendo $w \neq 0,\ w \neq 1$. A continuación, los bloques de un TD$(4,n)$ con n múltiplo de 4 pero no múltiplo de 8, se pueden definir sobre $(\mathbb{F}_4 \times \mathbb{Z}/(h)) \times \{1,2,3,4\}$ de la siguiente manera:

$$\{(\alpha,a,1),\ (\beta,b,2),\ (\alpha+\beta,a+b,3),\ (\alpha+w\beta,a-b,4)\ :\ \alpha,\beta \in \mathbb{F}_4,\ a,b \in \mathbb{Z}/(h)\}$$

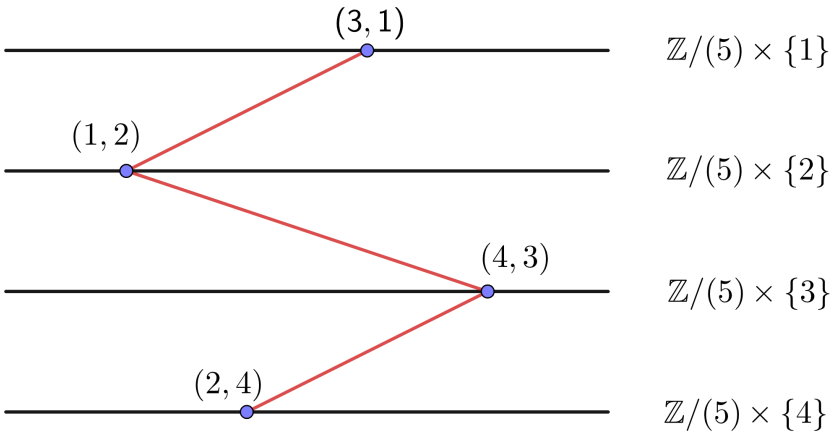


Figura 4.2: Bloque definido sobre $\mathbb{Z}/(5) \times \{1, 2, 3, 4\}$.

Los bloques de este TD$(4, n)$ son $\mathcal{G} = \{(\mathbb{F}_4 \times \mathbb{Z}/(h)) \times \{i\},\ i = 1, 2, 3, 4\}$.
Al igual que con el caso n impar, se comprueba que se cumplen las tres propiedades de este transversal design definido sobre $(\mathbb{F}_4 \times \mathbb{Z}/(h)) \times \{1, 2, 3, 4\}$, siendo h impar.

4.3.3. TD$(4, n)$ siendo n múltiplo de 8

Gracias a la construcción anterior, hemos encontrado una manera de formar TD$(4, n)$ sucesivamente, para un n múltiplo de 8. Por ejemplo, para un n múltiplo de 8 pero no múltiplo de 16 tenemos $n = 8 \cdot h$ con h impar, es decir, podemos definir de la misma manera un TD$(4, n)$ sobre $(\mathbb{F}_8 \times \mathbb{Z}/(h)) \times \{1, 2, 3, 4\}$, siendo h impar.

Por lo tanto, de manera sucesiva, se puede construir un TD$(4, n)$ para cierto $n = 2^k \cdot h,\ k \geq 2$, h impar, es decir, para un n múltiplo de 2^k pero no múltiplo de 2^{k+1}.
Este TD$(4, n)$ está definido sobre $(\mathbb{F}_{2^k} \times \mathbb{Z}/(h)) \times \{1, 2, 3, 4\}$. Tenemos que los cuatro grupos de este TD$(4, n)$ son $\mathcal{G} = \{(\mathbb{F}_{2^k} \times \mathbb{Z}/(h)) \times \{i\} \ :\ i = 1, 2, 3, 4\}$.

A continuación, desarrollaremos dos construcciones inductivas formadas con ayuda de estos nuevos diseños, los transversal designs.

4.4. $(4v - 3, 4, 1)$-BIBD

De acuerdo con [23], vamos a construir un $(4v - 3, 4, 1)$-BIBD $(W, \mathcal{C})$. En primer lugar, sea un $(v, 4, 1)$-BIBD. Como v es de la forma $12t + 1$ ó $12t + 4$ entonces $v - 1$ es $12t$ ó $12t + 3$, luego $v - 1$ es, o bien impar, o bien de la forma $2^k \cdot h$ con h impar. Es decir, tenemos que existe un TD$(4, v - 1)$, que aplicaremos más adelante.
A continuación, tomamos cuatro copias del BIBD inicial y, para cada copia, dejamos aparte un elemento. Sin perder la estructura de $(v, 4, 1)$-BIBD, identificamos estos cuatro elementos que hemos dejado aparte entre sí en un único elemento, que denotamos como ∞. Este elemento ∞

no pertenece al conjunto donde los $(v, 4, 1)$-BIBD estaban definidos, pero sustituye al elemento apartado de cada uno de los cuatro BIBD. A los cuatro subconjuntos de $v - 1$ elementos los denotamos como G_1, G_2, G_3, G_4.

Por tanto, nuestro diseño definido sobre $W = G_1 \cup G_2 \cup G_3 \cup G_4 \cup \{\infty\}$ tiene $4(v-1)+1 = 4v-3$ elementos, y dados dos elementos distintos de uno de los cuatro $(v, 4, 1)$-BIBD, tenemos que están simultáneamente en una única cuaterna, ya sea con el elemento ∞ o sin él. Es decir, en cada $G_i \cup \{\infty\}$, $i = 1, 2, 3, 4$, seguimos teniendo la estructura de $(v, 4, 1)$-BIBD, y tenemos $4\frac{v(v-1)}{12} = \frac{v(v-1)}{3}$ bloques de esta forma. A esta familia de bloques la denominamos $\mathcal{B}$.

Por la estructura de los $(v, 4, 1)$-BIBD, tenemos que el elemento ∞ está contenido con cada uno de los $4(v-1)$ elementos restantes de W en un único bloque. Por tanto, para poder completar un $(4v-3, 4, 1)$-BIBD, nos falta relacionar los puntos entre los G_i, $i = 1, 2, 3, 4$. Es ahora cuando aplicamos nuestro TD$(4, v-1)$, $(W \setminus \{\infty\},\ \mathcal{G},\ \mathcal{D})$, ya que si tomamos a $\mathcal{G} = \{G_1, G_2, G_3, G_4\}$ como los grupos de este transversal design, obtenemos, por la definición de transversal design, lo siguiente:

- Para cada bloque D_j de $\mathcal{D}$, para cada $i = 1, 2, 3, 4$, $|G_i \cap D_j| = 1$.
- Cada par de puntos $x, y \in \bigcup_{i=1}^{4} G_i$, $x \neq y$, x e y de distintos grupos, está contenido en un único bloque de $\mathcal{D}$. Es decir, dados dos puntos de $\bigcup_{i=1}^{4} G_i$ distintos, si no están en un mismo G_i, $i = 1, 2, 3, 4$, entonces están en un único bloque de $\mathcal{D}$.

Podemos observar que en cada cuaterna de $\mathcal{D}$ de este TD$(4, v-1)$ tenemos a un elemento de cada G_i, $i = 1, 2, 3, 4$. Además, dados dos puntos de distintos grupos, están simultáneamente en un único bloque.

Por lo tanto, como tenemos que cada par de elementos distintos de cada $G_i \cup \{\infty\}$, $i = 1, 2, 3, 4$, está contenido en un único bloque de $\mathcal{B}$, y acabamos de estudiar los bloques de D que relacionan a los elementos de G_i distintos, concluimos que tomando $\mathcal{C} = \mathcal{B} \cup \mathcal{D}$ obtenemos los bloques de nuestro $(4v-3, 4, 1)$-BIBD $(W, \mathcal{C})$.

Por último, vale la pena destacar que, dado que cada uno de los cuatro diseños definidos sobre $G_i \cup \{\infty\}$, $i = 1, 2, 3, 4$, conserva su estructura de $(v, 4, 1)$-BIBD, obtenemos cuatro subsistemas del $(4v-3, 4, 1)$-BIBD $(W, \mathcal{C})$.

Desarrollemos ahora un ejemplo de un $(61, 4, 1)$-BIBD construido a partir de un $(16, 4, 1)$-BIBD y un TD$(4, 15)$. De esta manera, podremos definir y explicar más concretamente los bloques de este diseño.

Ejemplo 4.4.1. En el Ejemplo 2.2.5 vimos que $\{0, 2, 3, 11\}$ era una $(15, 4, 1)$-familia de diferencias relativa a $\{0, 5, 10\}$, definida sobre $\mathbb{Z}/(15)$. Por tanto, teníamos que el desarrollo

$$\{g + \{0, 2, 3, 11\} \ :\ g \in \mathbb{Z}/(15)\} \bigcup \{\{\infty\} \cup (t + \{0, 5, 10\}) \ :\ t = 0, 1, 2, 3, 4\}$$

constituye un $(16, 4, 1)$-BIBD definido sobre $\mathbb{Z}/(15) \bigcup \{\infty\}$, siendo $\{\infty\}$ un elemento ajeno a $\mathbb{Z}/(15)$.

Como hemos explicado anteriormente, tomamos cuatro copias de este BIBD y separamos el elemento ∞ de cada BIBD, de manera que identificamos los cuatro ∞ en un único elemen-

to ∞, que forma parte de los cuatro $(16, 4, 1)$-BIBD. Es decir, hemos definido un diseño sobre $V = (\mathbb{Z}/(15) \times \{1, 2, 3, 4\}) \bigcup \{\infty\}$, y seguimos teniendo la estructura de $(16, 4, 1)$-BIBD en cada $(\mathbb{Z}/(15) \times \{i\}) \bigcup \{\infty\}$, $i = 1, 2, 3, 4$. Por tanto, ya hemos definido los bloques que relacionan los elementos de cada $(\mathbb{Z}/(15) \times \{i\}) \bigcup \{\infty\}$, $i = 1, 2, 3, 4$, entre sí.

A continuación, defino un TD$(4, 15)$ sobre $\mathbb{Z}/(15) \times \{1, 2, 3, 4\}$, donde los grupos son los $\mathbb{Z}/(15) \times \{i\}$, $i = 1, 2, 3, 4$, y los bloques los definimos de la siguiente manera:

$$\{(a, 1),\ (b, 2),\ (a + b, 3),\ (a - b, 4)\ :\ a, b \in \mathbb{Z}/(15)\}.$$

De esta forma, hemos definido las cuaternas que tienen un elemento de cada $\mathbb{Z}/(15) \times \{i\}$, $i = 1, 2, 3, 4$. Como explicamos en la Sección 4.3.1, tenemos que cada par de elementos de distintos grupos va a estar contenido en un único bloque. Por ejemplo, para el par de elementos $(x, 1), (y, 4)$, $x, y \in \mathbb{Z}/(15)$, tomando $x = a$, $y = a - b$, obtenemos $x - y = b$, $2x - y = a + b$, luego estos dos elementos están contenidos en el bloque único

$$\{(x, 1), (x - y, 2), (2x - y, 3), (y, 4)\}.$$

Finalmente, concluimos que con los bloques del TD$(4, 15)$ junto con los obtenidos en los cuatro $(16, 4, 1)$-BIBD, hemos definido sobre $V = (\mathbb{Z}/(15) \times \{1, 2, 3, 4\}) \bigcup \{\infty\}$ un $(4(16 - 1) + 1, 4, 1)$-BIBD, es decir, un $(61, 4, 1)$-BIBD.

Además, tenemos que los cuatro diseños definidos sobre $(\mathbb{Z}/(15) \times \{i\}) \bigcup \{\infty\}$, $i = 1, 2, 3, 4$, conservan su estructura de $(16, 4, 1)$-BIBD, luego son cuatro subsistemas del $(61, 4, 1)$-BIBD.

4.5. $(4v - 12, 4, 1)$-BIBD

Nuestra última construcción inductiva de este capítulo es un $(4(v - 4) + 4, 4, 1)$-BIBD $(W, \mathcal{C})$, es decir, un $(4v - 12, 4, 1)$-BIBD, construido a partir de un $(v, 4, 1)$-BIBD.
En primer lugar, tomamos cuatro copias de un $(v, 4, 1)$-BIBD dado. Separamos, de cada copia del $(v, 4, 1)$-BIBD, un bloque concreto, el mismo de los cuatro. Es decir, apartamos de cada copia 4 elementos que forman un bloque. Al igual que hacíamos en la construcción anterior con el elemento ∞, identificamos ahora entre sí a los cuatro bloques separados, de manera que cada copia del $(v, 4, 1)$-BIBD inicial siga manteniendo su estructura de BIBD. A estos cuatro elementos que forman el bloque los denotamos como $a_i,\ i = 1, 2, 3, 4$. A los cuatro subconjuntos de $v - 4$ elementos, que han resultado de apartar cuatro elementos de cada copia del $(v, 4, 1)$-BIBD, los denotamos como G_1, G_2, G_3, G_4.

Por lo tanto, tenemos un diseño definido sobre $W = G_1 \cup G_2 \cup G_3 \cup G_4 \cup \{a_1, a_2, a_3, a_3\}$, que contiene $4(v - 4) + 4 = 4v - 12$ elementos. Cada $G_i \cup \{a_1, a_2, a_3, a_3\}$, $i = 1, 2, 3, 4$, conserva la estructura de $(v, 4, 1)$-BIBD. Tenemos entonces $4\frac{v(v-1)}{12} - 3$ bloques de este tipo, ya que el bloque $\{a_1, a_2, a_3, a_3\}$ se cuenta una única vez. A esta familia de bloques la denominamos $\mathcal{B}$. Veamos ahora, para cada par de elementos distintos $x, y \in W$, en qué tipo bloque están contenidos dichos elementos:

- Si $x, y \in \{a_1, a_2, a_3, a_3\}$, entonces están contenidos simultáneamente en el bloque $\{a_1, a_2, a_3, a_3\}$.

- Si $x \in \{a_1, a_2, a_3, a_3\}$, $y \in G_i$, al igual que si tenemos $x, y \in G_i$ para cualquier $i = 1, 2, 3, 4$, como cada $G_i \cup \{a_1, a_2, a_3, a_3\}$ conserva la estructura de $(v, 4, 1)$-BIBD, existe un único bloque en el que están contenidos simultáneamente x, y.

- Nos queda comprobar el caso en el que $x \in G_i$, $y \in G_j$, $i \neq j$, $i, j \in \{1, 2, 3, 4\}$. Es en este momento cuando aplicamos un TD$(4, v-4)$, $(W \setminus \{a_1, a_2, a_3, a_4\},\ \mathcal{G},\ \mathcal{D})$, donde $\mathcal{G} = \{G_1, G_2, G_3, G_4\}$. Podemos asegurar, como en la construcción anterior, que este TD$(4, v-4)$ existe, ya que $v-4$ es de la forma $12t$ ó $12t-3$.
  Por definición de transversal design, obtenemos que cada par de elementos de distintos bloques están contenido simultáneamente en un único bloque de $\mathcal{D}$. Es decir, en este caso obtenemos que x, y están simultáneamente en un único bloque de $\mathcal{D}$, como queríamos.

Por lo tanto, tomando $\mathcal{C} = \mathcal{B} \cup \mathcal{D}$, hemos comprobado que cada par de elementos distintos de W están contenidos simultáneamente en un único bloque de $\mathcal{C}$. Es decir, concluimos que hemos construido un $(4v-12, 4, 1)$-BIBD definido sobre W.

Por último, como cada uno de los cuatro diseños definidos sobre $G_i \cup \{a_1, a_2, a_3, a_4\},\ i = 1, 2, 3, 4$, conserva su estructura de $(v, 4, 1)$-BIBD, obtenemos cuatro subsistemas del $(4v-3, 4, 1)$-BIBD $(W, \mathcal{C})$.

4.6. Tabla de construcciones inductivas

Para terminar este capítulo, hemos construido la Tabla 4.1. En ella, podemos observar, para cada v y para cada $(v, 4, 1)$-BIBD construido en el capítulo anterior, las nuevos $(v, 4, 1)$-BIBD que se pueden construir gracias a estas construcciones inductivas.
Cabe resaltar que hay valores de v que se repiten en la tabla, como $40, 52, 112, 148 \ldots$ En estos casos, como para esos v se han construido $(v, 4, 1)$-BIBD de distintas maneras, seguramente los diseños obtenidos sean no isomorfos.

Esta forma de construir BIBD, ya sea con estas construcciones inductivas o con otras que no hemos estudiado aquí, es una manera muy útil y sencilla de poder obtener una gran cantidad de $(v, 4, 1)$-BIBD.

Anteriormente, hemos estudiado que si un $(v, 4, 1)$-BIBD existe entonces $v \equiv 1$ ó $4 \mod (12)$. Gracias a [11], se tiene que el recíproco también es cierto:

$$\text{Sea } v \geq 4,\ v \equiv 1 \text{ ó } 4 \mod (12),\ \text{entonces existe algún } (v, 4, 1)\text{-BIBD.}$$

Es tal la importancia de estas construcciones inductivas, que quizá, con reiteradas aplicaciones de estas reglas inductivas, puedan construirse un ejemplo de un $(v, 4, 1)$-BIBD para casi todos los $v = 12t + 1$ y los $v = 12t + 4$.

v	**3v+1**	**4v-12**	**4v-3**	**4v**	**13v**
13	40	40	49	52	169
16	49	52	61	64	208
25	76	88	97	100	325
28	85	100	109	112	364
37	112	136	145	148	481
40	121	148	157	160	520
49	148	184	193	196	637
52	157	196	205	208	676
61	184	232	241	244	793
64	193	244	253	256	832

Cuadro 4.1: $(v, 4, 1)$-BIBD obtenidos gracias a las contrucciones inductivas.

Capítulo 5

$(v, 4, \lambda)$-BIBD con índice $\lambda \geq 2$

Hasta ahora nos hemos centrado en los $(v, 4, 1)$-BIBD, es decir, en los BIBD con índice $\lambda = 1$. Para terminar, en este último capítulo queremos introducir los $(v, 4, \lambda)$-BIBD con índice $\lambda \geq 2$. Para ello, estudiaremos distintos resultados para ver en qué condiciones se pueden encontrar estos BIBD, y también distintos métodos para obtener estos diseños. Nos centraremos mayormente en la construcción de $(v, 4, \lambda)$-familias de diferencias, ya que con su desarrollo sabemos construir $(v, 4, \lambda)$-BIBD. Se expondrán varios ejemplos ilustrativos para entender mejor los distintos resultados y, a su vez, para conocer estos diseños.

Para comenzar, recordemos la definición de $(v, 4, \lambda)$-BIBD:

Definición 5.0.1. *Un $(v, 4, \lambda)$-BIBD es un conjunto V de v elementos junto con una familia $\mathcal{B}$ de subconjuntos de V denominados bloques o cuaternas. Cada bloque contiene 4 elementos de V, de manera que cada par de elementos $x, y \in V$ distintos están contenidos simultáneamente en exactamente λ bloques.*

Veamos un teorema importante probado por primera vez por Hanani (véase [11]), que nos da dos condiciones necesarias y suficientes sobre la existencia de $(v, 4, \lambda)$-BIBD.

Teorema 5.0.2. *Un $(v, 4, \lambda)$-BIBD existe si y solo si*

$$\lambda(v-1) \equiv 0 \mod (3) \quad \text{y} \quad \lambda v(v-1) \equiv 0 \mod (12).$$

La demostración de este teorema requiere distinguir varios casos y se desvía del objetivo de este trabajo, por lo que he considerado no probarla aquí y dejarla a disposición del lector (véase [11, pág. 370]).

5.1. $(v, 4, 2)$-BIBD

Empezaremos estudiando los $(v, 4, \lambda)$-BIBD con índice $\lambda = 2$, es decir, los BIBD donde cada par de elementos $x, y \in V$ distintos están contenidos simultáneamente en exactamente 2 cuaternas o bloques.
En esta sección, demostraremos un teorema que se apoya en las $(v, 4, 1)$-familias de diferencias y

que nos facilitará la construcción de $(v, 4, 2)$-BIBD. A su vez, expondremos varios ejemplos, tanto de familias de diferencias como de $(v, 4, 2)$-BIBD.

Gracias al Teorema 5.0.2 se tiene que un $(v, 4, 2)$-BIBD existe si y solo si

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

Es decir, v es de la forma $3t + 1$ para cada $t \in \mathbb{N}$.

Veamos un ejemplo característico de los $(v, 4, 2)$-BIBD:

Ejemplo 5.1.1. En el Ejemplo 1.1.2 estudiamos un $(7, 3, 1)$-BIBD $(V, \mathcal{B})$ que se representa como el plano proyectivo de Fano. A partir de este ejemplo, vamos a construir un $(7, 4, 2)$-BIBD $(V, \mathcal{C})$. Como cada bloque de $(V, \mathcal{B})$ tiene 3 elementos, si cogemos los cuatro elementos complementarios de cada bloque de $\mathcal{B}$ como un bloque de $\mathcal{C}$, obtenemos un nuevo diseño $(V, \mathcal{C})$ con bloques de tamaño $k_{\mathcal{C}} = 4$.

En $(V, \mathcal{B})$ tenemos que dos elementos distintos $x, y \in V$ están simultáneamente en un único bloque y, como $r_{\mathcal{B}} = \frac{6}{2} = 3$, cada uno de ellos está en otros dos bloques distintos. Por lo tanto, como además $b_{\mathcal{B}} = \frac{7 \cdot 6}{3 \cdot 2} = 7$, hay exactamente $7 - 5 = 2$ bloques en $\mathcal{B}$ en los que no están ni x ni y. Entonces, escogiendo los elementos complementarios de esos dos bloques, obtenemos que hay exactamente $\lambda_{\mathcal{C}} = 2$ bloques en los que están simultáneamente x e y.

En resumen, tenemos que $v_{\mathcal{C}} = v_{\mathcal{B}} = 7$, $k_{\mathcal{C}} = 4$ y $\lambda_{\mathcal{C}} = 2$. Además, como los bloques de $(V, \mathcal{C})$ se obtienen cogiendo los elementos complementarios de los bloques de $(V, \mathcal{B})$, tenemos que $b_{\mathcal{C}} = b_{\mathcal{B}} = 7$, comprobando que es igual a $2\frac{7 \cdot 6}{4 \cdot 3}$, como queríamos.

Por tanto, hemos terminado de construir nuestro $(7, 4, 2)$-BIBD a partir de un $(7, 3, 1)$-BIBD.

Sabemos, gracias al Teorema 2.1.3, cómo construir un (v, k, λ)-BIBD a partir de una (v, k, λ)-familia de diferencias. Veamos, a continuación, un teorema que nos facilite la construcción de una $(v, 4, 2)$-familia de diferencias a partir de una $(v, 4, 1)$-familia de diferencias. De esa manera, con el desarrollo de la $(v, 4, 2)$-familia de diferencias, obtendremos un $(v, 4, 2)$-BIBD.

Teorema 5.1.2. *Sea $(G, +)$ un grupo de orden $v = 12t+1$ con elemento neutro 0. Sea $A_1, A_2, ..., A_l$ una $(v, 4, 1)$-familia de diferencias definida sobre G donde $0 \in A_i$ para cada $i = 1, 2, \dots l$.*
Entonces la familia

$$\{A_1, A_2, \dots A_l, -A_1, -A_2, \dots - A_l\}$$

es una $(v, 4, 2)$-familia de diferencias definida sobre G.

Demostración. Como $A_1, A_2, ..., A_l$ es una $(v, 4, 1)$-familia de diferencias sobre G, entonces el multiconjunto

$$\bigcup_{i=1}^{l} [x - y,\ y - x\ :\ x, y \in A_i,\ x \neq y]$$

contiene cada elemento de $G \setminus \{0\}$ exactamente 1 vez. Se observa entonces que el multiconjunto

$$\bigcup_{i=1}^{l} ([x - y,\ y - x\ :\ x, y \in A_i,\ x \neq y] \cup [x - y,\ y - x\ :\ x, y \in -A_i,\ x \neq y])$$

contiene cada elemento de $G \setminus \{0\}$ exactamente 2 veces.
La única manera de que esto no sea cierto es si $h + A_i = k - A_j$ para algún $h, k \in G$, $i, j \in \{1, 2, \dots l\}$, ya que las diferencias de A_i y $-A_j$ serían las mismas. Por reducción al absurdo, probemos que esta igualdad no se puede dar:

- Sea $i = j$, es decir, $h + A_i = k - A_i$ para algún $h, k \in G$. Sea $A_i = \{0, a_1, a_2, a_3\}$.
  - Si $h \neq k$, entonces $(h - k) + A_i = -A_i$. Escogiendo el elemento $0 \in A_i$, se tiene que $h - k + 0 = -a_n$ para algún $n \in \{1, 2, 3\}$. A su vez, escogiendo ese mismo elemento $a_n \in A_i$ se obtiene la segunda igualdad $h - k + a_n = -a_m$, $m \neq n$, $m, n \in \{1, 2, 3\}$. Restando ambas igualdades nos queda que $a_n - 0 = a_n - a_m$, lo que contradice que $A_1, A_2, ..., A_l$ sea una $(v, 4, 1)$-familia de diferencias, ya que un elemento de $G \setminus \{0\}$ estaría contenido en el multiconjunto más de 1 vez.
  - Si $h = k$, tenemos

    $$A_i = -A_i, \quad a_1 = -a_n, \quad a_2 = -a_m, \quad n, m \in \{1, 2, 3\}.$$

    Nótese que como G tiene orden $v = 12t + 1$ impar, ningún $a \in G$ cumple $a = -a$, salvo el 0. Luego restando ambas expresiones llegamos de nuevo a un absurdo.
- Veamos ahora qué pasa si $i \neq j$. Sea $A_i = \{0, a_1, a_2, a_3\}, A_j = \{0, b_1, b_2, b_3\}$.
  Tomando de nuevo los elementos $0, a_1 \in A_i$, obtenemos las siguientes expresiones:

  $$h + 0 = k - b_n, \quad h + a_1 = k - b_m, \ n \neq m, \ n, m \in \{1, 2, 3\}.$$

  Restando nos queda que $a_1 - 0 = b_m - b_n$, lo que vuelve a contradecir que $A_1, A_2, ..., A_l$ sea una $(v, 4, 1)$-familia de diferencias.

Por tanto, hemos probado que $h + A_i \neq k - A_j$ para todo $h, k \in G$, $i, j \in \{1, 2, \dots l\}$.
Es decir, finalmente concluimos que $\{A_1, A_2, \dots A_l, -A_1, -A_2, \dots - A_l\}$ es una $(v, 4, 2)$-familia de diferencias definida sobre G. □

Veamos dos casos concretos en los que se puede aplicar este teorema.

Ejemplo 5.1.3. En la Sección 3.2.6 se estudió que $\mathcal{F} = \{B_1, B_2, B_3, B_4\}$ con

$$B_1 = \{0, 1, 3, 15\}, \quad B_2 = \{0, 5, 18, 25\}, \quad B_3 = \{0, 9, 30, 41\}, \quad B_4 = \{0, 4, 10, 26\},$$

es una $(49, 4, 1)$-familia de diferencias definida sobre $\mathbb{Z}/(49)$.
Aplicando el Teorema 5.1.2 anterior, se obtiene que $\mathcal{H} = \{B_1, B_2, B_3, B_4, -B_1, -B_2, -B_3, -B_4\}$ es una $(49, 4, 2)$-familia de diferencias. Por último, aplicando el Teorema 2.1.3 se observa que el desarrollo de esta familia de diferencias es un $(49, 4, 2)$-BIBD, es decir,

$$g + H \quad : \quad g \in \mathbb{Z}/(49), \ H \in \mathcal{H},$$

constituye un $(49, 4, 2)$-BIBD definido sobre $\mathbb{Z}/(49)$.

Ejemplo 5.1.4. Dados $B_1 = \{0, 1, 5, 11\}$, $B_{i+1} = 9^i B_1$, $i = 1, 2, 3, 4$, se comprobó en la Sección 3.2.8 que $\mathcal{F} = \{B_i \ : \ i = 1, 2, 3, 4, 5\}$ es una $(61, 4, 1)$-familia de diferencias definida sobre $\mathbb{Z}/(61)$. De la misma manera que en el ejemplo anterior, aplicamos el Teorema 5.1.2 y obtenemos que la familia $\mathcal{H} = \{B_i, -B_i \ : \ i = 1, 2, 3, 4, 5\}$ es una $(61, 4, 2)$-familia de diferencias.
Para terminar, se aplica el Teorema 2.1.3 y se concluye que el desarrollo de esta familia de diferencias es un $(61, 4, 2)$-BIBD, es decir,

$$g + H \quad : \quad g \in \mathbb{Z}/(61), \ H \in \mathcal{H},$$

constituye un $(61, 4, 2)$-BIBD definido sobre $\mathbb{Z}/(61)$.

Acabamos de comprobar, con estos dos ejemplos, lo útil que es el Teorema 5.1.2 para construir, de una manera sencilla, un $(v, 4, 2)$-BIBD a partir de una $(v, 4, 1)$-familia de diferencias.

Para terminar con los $(v, 4, 2)$-BIBD, veamos la construcción de un $(19, 4, 2)$-BIBD de una forma directa, a partir de una $(19, 4, 2)$-familia de diferencias.

Ejemplo 5.1.5. [7] Sea $G = \mathbb{Z}/(19)$. En primer lugar, veamos que la familia de subconjuntos $\{A_1, A_2, A_3\}$ donde

$$A_1 = \{0, 1, 3, 12\}, \quad A_2 = \{0, 1, 5, 13\}, \quad A_3 = \{0, 4, 6, 9\},$$

es una $(19, 4, 2)$-familia de diferencias definida sobre G.
Operando, obtenemos que

$$\Delta A_1 = [1, 3, 12, 18, 16, 7, 2, 17, 11, 8, 9, 10], \quad \Delta A_2 = [1, 5, 13, 18, 14, 6, 4, 15, 12, 7, 8, 11],$$

$$\Delta A_3 = [4, 6, 9, 15, 13, 10, 2, 17, 5, 14, 3, 16].$$

Observamos que el multiconjunto $\Delta A_1 \cup \Delta A_2 \cup \Delta A_3$ contiene cada elemento de $G \setminus \{0\}$ exactamente 2 veces, es decir, tenemos que $\{A_1, A_2, A_3\}$ es una $(19, 4, 2)$-familia de diferencias definida sobre G.
Por último, se aplica el Teorema 2.1.3 y se concluye que el desarrollo

$$g + A_i \quad : \quad g \in \mathbb{Z}/(19), \ i = 1, 2, 3,$$

constituye un $(19, 4, 2)$-BIBD definido sobre $\mathbb{Z}/(19)$.

5.2. $(v, 4, 3)$-BIBD

Veamos ahora el caso $\lambda = 3$, es decir, los $(v, 4, 3)$-BIBD.
Como en otras ocasiones, veremos varios ejemplos de $(v, 4, 3)$-BIBD. Por otra parte, estudiaremos un teorema importante que nos facilitará la construcción $(v, 4, 3)$-familias de diferencias definidas sobre cuerpos finitos.

Gracias al Teorema 5.0.2 se tiene que un $(v, 4, 3)$-BIBD existe si y solo si

$$v \equiv 0, 1 \mod (4).$$

Por lo tanto, v es de la forma $4t$ ó $4t + 1$ para cada $t \in \mathbb{N}$.

Estudiemos a continuación un teorema que nos dará una condición necesaria y suficiente sobre la existencia de ciertas $(v, 4, 3)$-familias de diferencias. A su vez, en la demostración veremos cómo hallar al menos una $(v, 4, 3)$-familia de diferencias en los casos en los que sea posible.

Teorema 5.2.1. [2] *Sea q la potencia de un primo impar. Una $(q, 4, 3)$-familia de diferencias existe en $(\mathbb{F}_q, +)$ si y solo si*

$$q \equiv 1 \mod (4).$$

Demostración. Sea $q \equiv 1 \mod (4)$ la potencia de un primo impar. Sea $H = (\mathbb{F}_q^*, \cdot)$ con $|H| = q - 1$ el grupo multiplicativo de $\mathbb{F}_q$. Sea $w \in \mathbb{F}_q^*$ una raíz primitiva. Como w tiene orden $q - 1$, sea $\epsilon = w^{\frac{q-1}{4}}$ una raíz primitiva cuarta de la unidad, es decir, ϵ tiene orden 4.
Sea $A = \{1, \epsilon, \epsilon^2, \epsilon^3\}$. Teniendo en cuenta que $\epsilon^4 = 1$, $\epsilon^2 = -1$ y $\epsilon^3 = -\epsilon$, calculemos sus diferencias:

$$\Delta A = [\epsilon - 1, 1 - \epsilon, \epsilon^2 - 1, 1 - \epsilon^2, \epsilon^3 - 1, 1 - \epsilon^3, \epsilon^2 - \epsilon, \epsilon - \epsilon^2, \epsilon^3 - \epsilon, \epsilon - \epsilon^3, \epsilon^3 - \epsilon^2, \epsilon^2 - \epsilon^3] =$$

$$= [\epsilon{-}1, \epsilon^2(\epsilon{-}1), \epsilon^2{-}1, \epsilon^2(\epsilon^2{-}1), \epsilon^3{-}1, \epsilon^2(\epsilon^3{-}1), \epsilon(\epsilon{-}1), \epsilon^3(\epsilon{-}1), \epsilon(\epsilon^2{-}1), \epsilon^3(\epsilon^2{-}1), \epsilon(\epsilon^3{-}1), \epsilon^3(\epsilon^3{-}1)] =$$

$$= A \cdot [\epsilon - 1, \epsilon^2 - 1, \epsilon^3 - 1]$$

A continuación, probemos que la familia $S = \{w^i \cdot A \ : \ i = 0, 1, 2, \ldots \frac{q-1}{4} - 1\}$ es una $(q, 4, 3)$-familia de diferencias. Para ello, veamos que el multiconjunto de las diferencias ΔS contiene a cada elemento de $\mathbb{F}_q^*$ tres veces:

$$\Delta S = \bigcup_{i=0}^{\frac{q-1}{4}-1} w^i \cdot \Delta A = \bigcup_{i=0}^{\frac{q-1}{4}-1} w^i \cdot A \cdot [\epsilon - 1, \epsilon^2 - 1, \epsilon^3 - 1] = [\epsilon - 1, \epsilon^2 - 1, \epsilon^3 - 1] \cdot (\bigcup_{i=0}^{\frac{q-1}{4}-1} w^i \cdot A)$$

Observemos el conjunto $\bigcup_{i=0}^{\frac{q-1}{4}-1} w^i \cdot A$, recordando que $\epsilon = w^{\frac{q-1}{4}}$:

$$\bigcup_{i=0}^{\frac{q-1}{4}-1} w^i \cdot A = \{w^i \cdot \epsilon^j \ : \ i = 0, 1, 2, \ldots \frac{q-1}{4} - 1, \ j = 1, 2, 3, 4\} =$$

$$= \{w^{i + \frac{q-1}{4} j} \ : \ i = 0, 1, 2, \ldots \frac{q-1}{4} - 1, \ j = 1, 2, 3, 4\} =$$

$$= \{w^k \ : \ k = 0, 1, 2, \ldots (q-1) - 1\} = \mathbb{F}_q^*$$

Ésta última igualdad se debe a que, al ser w raíz primitiva en $\mathbb{F}_q^*$, w engendra $\mathbb{F}_q^*$.
Finalmente obtenemos que $\Delta S = [\epsilon - 1, \epsilon^2 - 1, \epsilon^3 - 1] \cdot \mathbb{F}_q^*$, es decir, cada elemento de $\mathbb{F}_q^*$ está contenido en ΔS tres veces. Hemos probado entonces que S es una $(q, 4, 3)$-familia de diferencias. Por tanto, hemos visto que $q \equiv 1 \mod (4)$ es una condición suficiente para la existencia de $(q, 4, 3)$-familia de diferencias.

Por el Teorema 2.1.3 sabemos que si tenemos una $(v, 4, 3)$-familia de diferencias entonces podemos

desarrollar un $(v, 4, 3)$-BIBD. Por contrarrecíproco, si no existe ningún $(v, 4, 3)$-BIBD, no existe tampoco ninguna $(v, 4, 3)$-familia de diferencias.
Hemos probado justo antes de este teorema que un $(v, 4, 3)$-BIBD existe si y solo si $v \equiv 0, 1 \bmod (4)$. En este teorema trabajamos con $v = q$ potencia de un primo impar, es decir, la condición $q \equiv 0 \bmod (4)$ no es posible. Finalmente, dado q la potencia de un primo impar, se concluye que la condición $q \equiv 1 \bmod (4)$ es necesaria para la existencia de $(q, 4, 3)$-BIBD y, por consiguiente, para la existencia de $(q, 4, 3)$-familias de diferencias. □

Nótese que el teorema anterior no es solo un teorema sobre la existencia de las $(q, 4, 3)$-familias de diferencias, sino que, gracias a la demostración, sabemos cómo formar al menos una $(q, 4, 3)$-familia de diferencias.
Veamos dos ejemplos en los que se aplica el teorema anterior:

Ejemplo 5.2.2. Sea $q = 5^2 = 25$. Tenemos que q es potencia de un primo impar y $q \equiv 1 \bmod (4)$, luego aplicando el Teorema 5.2.1 anterior, tenemos que existe una $(25, 4, 3)$-familia de diferencias definida sobre $\mathbb{F}_{25} = \frac{\mathbb{F}_5[x]}{(x^2-3x-2)} = \{a + bx \ : \ a, b \in \mathbb{F}_5\}$. Sigamos la demostración de dicho teorema para obtener una $(25, 4, 3)$-familia de diferencias.

Como vimos en la Sección 3.2.2, $x \in \mathbb{F}_{25}^*$ es una raíz primitiva. Por tanto, x tiene orden 24 y $x^{\frac{24}{4}} = x^6$ tiene orden 4. Sea $A = \{1, x^6, x^{12}, x^{18}\}$.
Por la demostración del teorema anterior, se tiene que

$$S = \{x^i \cdot A \ : \ i = 0, 1, 2, 3, 4, 5\}$$

es una $(25, 4, 3)$-familia de diferencias. Denotemos por $B_i = \{x^i \cdot A\}$, $i = 0, 1, 2, 3, 4, 5$, a cada subconjunto de la familia de diferencias.

Por último, aplicando el Teorema 2.1.3, concluimos que el desarrollo

$$g + B_i \quad : \quad g \in \mathbb{F}_{25}, \quad i = 0, 1, 2, 3, 4, 5,$$

constituye un $(25, 4, 3)$-BIBD.

Hagamos una pequeña comprobación:

- Sabemos que un $(25, 4, 3)$-BIBD tiene exactamente $b = 3\frac{25 \cdot 24}{4 \cdot 3} = 150$ bloques.
- S está compuesto por 6 subconjuntos, luego el desarrollo de S tiene $25 \cdot 6 = 150$ bloques, como queríamos.

Por tanto, hemos terminado de construir una $(25, 4, 3)$-familia de diferencias y un $(25, 4, 3)$-BIBD definidos sobre $(\mathbb{F}_{25}, +)$.

Ejemplo 5.2.3. Al igual que en el ejemplo anterior, sea $q = 7^2 = 49$ potencia de un primo impar y $q \equiv 1 \bmod (4)$. Aplicando el Teorema 5.2.1 anterior, obtenemos que existe una $(49, 4, 3)$-familia de diferencias definida sobre $\mathbb{F}_{49} = \frac{\mathbb{F}_7[x]}{(x^2+x+3)} = \{a + bx \quad : \quad a, b \in \mathbb{F}_7\}$. Sigamos, de nuevo, la demostración de dicho teorema para formar una $(49, 4, 3)$-familia de diferencias.

En primer lugar, tenemos que $x \in \mathbb{F}_{49}^*$ es una raíz primitiva. Por tanto, x tiene orden 48 y $x^{\frac{48}{4}} = x^{12}$ tiene orden 4. Sea $A = \{1, x^{12}, x^{24}, x^{36}\}$.
Por la demostración del teorema anterior, se tiene que

$$S = \{x^i \cdot A \ : \ i = 0, 1, 2, \dots 11\}$$

es una $(49, 4, 3)$-familia de diferencias. Denotemos por $B_i = \{x^i \cdot A\}$, $i = 0, 1, 2, \dots 11$, a cada subconjunto de la familia de diferencias.

Finalmente, aplicando el Teorema 2.1.3, se concluye que el desarrollo

$$g + B_i \quad : \quad g \in \mathbb{F}_{49}, \quad i = 0, 1, 2, \dots 11,$$

constituye un $(49, 4, 3)$-BIBD.

Para acabar, realicemos una pequeña comprobación:

- Sabemos que un $(49, 4, 3)$-BIBD tiene exactamente $b = 3\frac{49 \cdot 48}{4 \cdot 3} = 588$ bloques.
- S está compuesto por 12 subconjuntos, luego el desarrollo de S tiene $49 \cdot 12 = 588$ bloques, como queríamos.

Por tanto, hemos terminado de construir una $(49, 4, 3)$-familia de diferencias y un $(49, 4, 3)$-BIBD definidos sobre $(\mathbb{F}_{49}, +)$.

A continuación, estudiemos un ejemplo de $(21, 4, 3)$-BIBD construido a partir de una $(21, 4, 3)$-familias de diferencias.

Ejemplo 5.2.4. [7] Sea $G = \mathbb{Z}/(21)$. En primer lugar, comprobemos que $\{A_1, A_2, A_3, A_4, A_5\}$ donde

$$A_1 = \{0, 2, 3, 7\}, \quad A_2 = \{0, 3, 5, 9\}, \quad A_3 = \{0, 1, 7, 11\}, \quad A_4 = \{0, 2, 8, 11\}, \quad A_5 = \{0, 1, 9, 14\},$$

es una $(21, 4, 3)$-familia de diferencias definida sobre G. Operando, obtenemos las siguientes diferencias:

$$\Delta A_1 = [2, 3, 7, 19, 18, 14, 1, 20, 5, 16, 4, 17], \quad \Delta A_2 = [3, 5, 9, 18, 16, 12, 2, 19, 6, 15, 4, 17],$$

$$\Delta A_3 = [1, 7, 11, 20, 14, 10, 6, 15, 10, 11, 4, 17], \quad \Delta A_4 = [2, 8, 11, 19, 13, 10, 6, 15, 9, 12, 3, 18],$$

$$\Delta A_5 = [1, 9, 14, 20, 12, 7, 8, 13, 13, 8, 5, 16].$$

Se puede observar que $\bigcup_{i=1}^{5} A_i$ contiene cada elemento de $G \setminus \{0\}$ exactamente 3 veces. Es decir, hemos comprobado que $\{A_1, A_2, A_3, A_4, A_5\}$ es una $(21, 4, 3)$-familia de diferencias.

Finalmente, aplicando el Teorema 2.1.3, se concluye que el desarrollo

$$g + A_i \quad : \quad g \in \mathbb{Z}/(21), \quad i = 1, 2, 3, 4, 5,$$

constituye un $(21, 4, 3)$-BIBD.

Se puede realizar una pequeña comprobación sobre el número de bloques:
Por una parte, se sabe que un $(21, 4, 3)$-BIBD contiene $b = 3\frac{21\cdot 20}{4\cdot 3} = 105$ bloques. Por otra parte, se observa que el desarrollo anterior está formado por $21 \cdot 5 = 105$ bloques, como queríamos.

Para terminar con este capítulo, vamos a introducir unas familias de conjuntos similares a las familias de diferencias, denominadas *rotacionales*, que nos ayudarán en la construcción de $(v, 4, 3)$-BIBD. Para ello, desarrollemos dos ejemplos en los que explicaremos los rotacionales.

Definimos, como en otras ocasiones, un elemento $\infty \notin G$, siendo G el grupo donde estamos trabajando. Este elemento cumple que $\infty + g = \infty$ para cada $g \in G$.

Ejemplo 5.2.5. [7] Sea $G = \mathbb{Z}/(7)$. Consideremos en $G \cup \{\infty\}$ la familia de conjuntos $\{A_1, A_2\}$ con $A_1 = \{\infty, 3, 5, 6\}$, $A_2 = \{0, 1, 2, 4\}$.
Operando, hallamos sus diferencias:

$$\Delta A_1 = [\infty, \infty, \infty, \infty, \infty, \infty, 2, 5, 3, 4, 1, 6], \quad \Delta A_2 = [1, 2, 4, 6, 5, 3, 1, 6, 3, 4, 2, 5].$$

Se observa que en $\Delta A_1 \cup \Delta A_2$ aparecen $\lambda = 3$ veces cada elemento de $\mathbb{Z}/(7)$ y 6 veces el elemento ∞, por lo que no tenemos una familia de diferencias.
A pesar de que parezca haber un problema con el elemento ∞, veamos que el desarrollo

$$g + A_i \quad : \quad g \in \mathbb{Z}/(7), \quad i = 1, 2,$$

constituye un $(8, 4, 3)$-BIBD.

En un $(8, 4, 3)$-BIBD se cumple que $r = 3\frac{8-1}{4-1} = 7$ y $b = 3\frac{8\cdot 7}{4\cdot 3} = 14$.
Por una parte, observamos que en el desarrollo $g + \{\infty, 3, 5, 6\}$ se tiene $g + \infty = \infty$ para cada $g \in \mathbb{Z}/(7)$, luego ∞ está contenido en $r = 7$ bloques. Por otra parte, $g + 3$, $g + 5$ y $g + 6$ recorren todo $\mathbb{Z}/(7)$, es decir, cada elemento de $\mathbb{Z}/(7)$ aparece con ∞ en exactamente $\lambda = 3$ bloques.
Por último, se puede comprobar que el desarrollo anterior contiene $7 \cdot 2 = 14$ bloques, que coincide con el valor de b anterior.

Por lo tanto, hemos comprobado que el elemento ∞ no nos supone ningún problema en la construcción de este BIBD. Podemos concluir que hemos desarrollado un $(8, 4, 3)$-BIBD definido sobre $\mathbb{Z}/(7) \cup \{\infty\}$.
A la familia $\{A_1, A_2\}$ se la denomina *rotacional*.

Ejemplo 5.2.6. [7] Sea $G = \mathbb{Z}/(19)$. Terminemos este capítulo construyendo un $(20, 4, 3)$-BIBD definido sobre $G \cup \{\infty\}$. Sea la familia $\{A_1, A_2, A_3, A_4, A_5\}$ donde

$$A_1 = \{\infty, 8, 12, 18\}, \quad A_2 = \{0, 2, 3, 14\}, \quad A_3 = \{1, 4, 13, 16\},$$

$$A_4 = \{7, 9, 15, 17\}, \quad A_5 = \{5, 6, 10, 11\}.$$

Operando, hallamos sus diferencias:

$$\Delta A_1 = [\infty, \infty, \infty, \infty, \infty, \infty, 4, 15, 10, 9, 6, 13], \quad \Delta A_2 = [2, 3, 14, 17, 16, 5, 1, 18, 12, 7, 11, 8]$$

$$\Delta A_3 = [3, 16, 12, 7, 15, 4, 9, 10, 12, 7, 3, 16], \quad \Delta A_4 = [2, 17, 8, 11, 10, 9, 6, 13, 8, 11, 2, 17],$$

$$\Delta A_5 = [1, 18, 5, 14, 6, 13, 4, 15, 5, 14, 1, 18].$$

Se observa que en $\bigcup_{i=1}^{5} A_i$ aparecen $\lambda = 3$ veces cada elemento de $\mathbb{Z}/(19)$ y 6 veces el elemento ∞, por lo que no tenemos una familia de diferencias.
Comprobemos que el desarrollo

$$g + A_i \quad : \quad g \in \mathbb{Z}/(19), \quad i = 1, 2, 3, 4, 5,$$

constituye un $(20, 4, 3)$-BIBD.

En un $(20, 4, 3)$-BIBD se cumple que $r = 3\frac{20-1}{4-1} = 19$ y $b = 3\frac{20 \cdot 19}{4 \cdot 3} = 95$.
Por una parte, observamos que en el desarrollo $g + \{\infty, 8, 12, 18\}$ se tiene $g + \infty = \infty$ para cada $g \in \mathbb{Z}/(19)$, luego ∞ está contenido en $r = 19$ bloques. Por otra parte, $g + 8$, $g + 12$ y $g + 18$ recorren todo $\mathbb{Z}/(19)$, es decir, cada elemento de $\mathbb{Z}/(19)$ aparece con ∞ en exactamente $\lambda = 3$ bloques.
Por último, se puede comprobar que el desarrollo anterior contiene $19 \cdot 5 = 95$ bloques, que coincide con el valor de b anterior.

Por lo tanto, hemos comprobado de nuevo que el elemento ∞ no nos supone ningún problema en la construcción de este BIBD. Concluimos que hemos desarrollado un $(20, 4, 3)$-BIBD definido sobre $\mathbb{Z}/(19) \cup \{\infty\}$.
Al igual que en el ejemplo anterior, a la familia $\{A_1, A_2, A_3, A_4, A_5\}$ se la denomina *rotacional*.

Apéndice

En este apéndice, mostramos un programa sencillo realizado en Matlab para calcular las diferencias dentro de una familia de subconjuntos, y así poder comprobar si son realmente una $(v, k, 1)$-familia de diferencias. Dicho programa lo podemos observar en la Figura 5.1. En él, introducimos la variable de entrada v que se identifica con el cuerpo $\mathbb{Z}/(v)$ donde estamos trabajando, y a su vez, con la $(v, k, 1)$-familia de diferencias que se quiere comprobar. La otra variable de entrada es B, una matriz en la que introducimos por filas los subconjuntos que forman la supuesta familia de diferencias. Por último, al ejecutar el programa, éste nos devuelve el vector dif, que son todas las diferencias de la familia de subconjuntos. Además, nos devuelve el valor vof que es 1 si verdaderamente es una familia de diferencias y 0 si no. Si realmente estamos ante una $(v, k, 1)$-familia de diferencias, entonces comprobaremos que dif contiene a todos los elementos de $(\mathbb{Z}/(v)) \setminus \{0\}$ y que $vof = 1$.

Este programa ha sido aplicado, concretamente, en las secciones 3.2.6 y 3.2.8, para comprobar una $(49, 4, 1)$-familia de diferencias y una $(61, 4, 1)$-familia de diferencias, respectivamente. Véase la Figura 5.2 . Se puede comprobar que dif es igual a $(\mathbb{Z}/(49)) \setminus \{0\}$ y $(\mathbb{Z}/(61)) \setminus \{0\}$, respectivamente en cada caso, y $vof = 1$ en ambos. Es decir, concluimos que esas familias de conjuntos sí que son familias de diferencias.

Por otro lado, hemos modificado ligeramente el programa anterior para poder comprobar también si se tiene una $(v, k, 1)$-familia de diferencias relativa. Además de todas las variables del anterior programa, se introduce un nuevo vector H, ya que estamos comprobando una familia de diferencias relativa a un subgrupo H. En la variable de salida dif podemos comprobar las diferencias de la familia, es decir, todos los elementos de $\mathbb{Z}/(v)$ salvo los elementos de H. Dicho de otra manera, comprobamos que $(\mathbb{Z}/(v)) \setminus H = \bigsqcup_{i=1}^{l} \Delta B_i$, siendo $\{B_1, B_2, \dots B_l\}$ la familia de diferencias relativa a H. De esta manera, concluimos que $\{B_1, B_2, \dots B_l\}$ es una familia de diferencias relativa a H, y podemos aplicar el Teorema 2.2.2 para desarrollar un $(v, k, 1)$-BIBD definido sobre $\mathbb{Z}/(v)$. Véase en la Figura 5.3 dicho programa.

Este programa ha sido aplicado en las secciones 3.2.7 y 3.2.9 para comprobar una $(52, 4, 1)$-familia de diferencias relativa y una $(64, 4, 1)$-familia de diferencias relativa, respectivamente. Podemos apreciar en la Figura 5.4 ambos casos, y comprobar que el vector dif nos da todos los elementos de $(\mathbb{Z}/(v)) \setminus H$. El valor de vof es 1, es decir, en ambos casos tenemos una familia de diferencias relativa.

```
function [dif,vof] = familiadiferencias(v,B)
dif=[];
[m,k]=size(B);
for i=1:m
    for j=1:k
        for s=1:k
            if s~=j
                dif=[dif, mod(B(i,s)-B(i,j), v)];
            end
        end
    end
end
dif=sort(dif);

a=1:(v-1);
vof=1;
for i=1:(v-1)
    if dif(i)~=a(i)
        vof=0;
    end
end
end
```

Figura 5.1: Programa para las familias de diferencias.

```
>> [dif,vof]=familiadiferencias(49, [0,1,3,15; 0,5,18,25; 0,9,30,41; 0,4,10,26])

dif =

  Columns 1 through 20

     1     2     3     4     5     6     7     8     9    10    11    12    13    14    15    16    17    18    19    20

  Columns 21 through 40

    21    22    23    24    25    26    27    28    29    30    31    32    33    34    35    36    37    38    39    40

  Columns 41 through 48

    41    42    43    44    45    46    47    48

vof =

     1
```

(a) $(49, 4, 1)$-familia de diferencias.

```
>> [dif,vof]=familiadiferencias(61, [0,1,5,11; 0,9,38,45; 0,20,37,39; 0,28,46,58; 0,8,34,48])

dif =

  Columns 1 through 20

     1     2     3     4     5     6     7     8     9    10    11    12    13    14    15    16    17    18    19    20

  Columns 21 through 40

    21    22    23    24    25    26    27    28    29    30    31    32    33    34    35    36    37    38    39    40

  Columns 41 through 60

    41    42    43    44    45    46    47    48    49    50    51    52    53    54    55    56    57    58    59    60

vof =

     1
```

(b) $(61, 4, 1)$-familia de diferencias.

Figura 5.2: Ejemplos aplicando el programa.

```
function [dif,vof] = familiarelativa(v,B,H)
dif=[];
comp=[];
[m,k]=size(B);
for i=1:m
    for j=1:k
        for s=1:k
            if s~=j
                dif=[dif, mod(B(i,s)-B(i,j), v)];
            end
        end
    end
end
comp=[dif,H];
comp=sort(comp);
dif=sort(dif);

a=0:(v-1);
vof=1;
for i=1:v
    if comp(i)~=a(i)
        vof=0;
    end
end
end
```

Figura 5.3: Programa para las familias de diferencias relativas.

```
>> [dif,vof]=familiarelativa(52, [0,1,3,7; 0,5,19,35; 0,8,20,31; 0,9,24,34],[0,13,26,39])

dif =

  Columns 1 through 20

     1     2     3     4     5     6     7     8     9    10    11    12    14    15    16    17    18    19    20    21

  Columns 21 through 40

    22    23    24    25    27    28    29    30    31    32    33    34    35    36    37    38    40    41    42    43

  Columns 41 through 48

    44    45    46    47    48    49    50    51

vof =

     1
```

(a) $(52, 4, 1)$-familia de diferencias relativa.

```
>> [dif,vof]=familiarelativa(64, [0,1,3,7; 0,5,18,47; 0,8,33,44; 0,9,19,43; 0,12,26,49; ],[0,16,32,48])

dif =

  Columns 1 through 20

     1     2     3     4     5     6     7     8     9    10    11    12    13    14    15    17    18    19    20    21

  Columns 21 through 40

    22    23    24    25    26    27    28    29    30    31    33    34    35    36    37    38    39    40    41    42

  Columns 41 through 60

    43    44    45    46    47    49    50    51    52    53    54    55    56    57    58    59    60    61    62    63

vof =

     1
```

(b) $(64, 4, 1)$-familia de diferencias relativa.

Figura 5.4: Ejemplos aplicando el programa.

Bibliografía

[1] Ian Anderson, *Combinatorial Designs and Tournaments*, Clarendon Press, 1997.

[2] Thomas Beth, Dieter Jungnickel, Hanfried Lez, *Design Theory, Second Edition*, Cambridge University Press, 1999.

[3] Jian Bi, *Computer-intensive methods for sensory data analysis, exemplified by Durbin's rank test,* Food Quality and Preference, Elsevier, Vol. 20 (2009), págs 195-202.

[4] R. C. Bose, *On the construction of Balanced Incomplete Block Designs,* Annals of Eugenics, Vol. 9 (1939), N. 4, págs 353-358.

[5] M. Buratti, *Improving Two Theorems of Bose on Difference Families,* Journal of Combinatorial Designs, Vol. 3, (1995), N. 1, págs 15-24.

[6] M. J. Colbourn y C. Colbourn, *Cyclic Block Designs With Block Size 3,* European Journal of Combinatorics, Vol. 2 (1981), págs 21-26.

[7] Charles J. Colbourn y Jeffrey H. Dinitz, *The CRC Handbook of Combinatorial Designs, First Edition*, CRC Press, 1996.

[8] Armando Maria Corsia, Juan Ignacio Modroño, Petr Mariel, Justin Cohen, Larry Lockshin, *How are personal values related to choice drivers? An application with Chinese wine consumers,* Food Quality and Preference, Elsevier, Vol. 96 (2020).

[9] Angela Dean, Daniel Voss, Danel Draguljić, *Design and Analysis of Experiments, Second Edition*, Springer, 2017.

[10] Marshall Hall, Jr, *Combinatorial Theory, Second Edition*, John Wiley and Sons, 1986.

[11] Haim Hanani, *The Existence and Construction of Balanced Incomplete Block Designs,* The Annals of Mathematical Statistics, Vol. 32 (1961), N. 2, págs. 361-386.

[12] Sanpei Kageyama, *Note on Takeuchi´s Table of Difference Sets Generating Balanced Incomplete Block Designs,* Review of the International Statistical Institute, Vol. 40 (1972), N. 3, págs. 275-276.

[13] S. MacLane, G. Birkhoff, *Algebra, Third Edition*, Chelsea, 1988.

[14] J. E. Marcos Naveira, *Apuntes de diseños combinatorios*, Valladolid, 2019.

[15] Takeshi Mori, Takahiro Tsuge, *Best–worst scaling survey of preferences regarding the adverse effects of tobacco use in China,* SSM - Population Health, Elsevier, Vol. 3 (2017), págs 624-632.

[16] Colin Reid, Alex Rosa, *Steiner systems S(2, 4, v) - a survey,* The Electronic Journal of Combinatorics, DS18 (2010).

[17] G. P. Sillito, *Note on Takeuchi´s Table of Difference Sets Generating Balanced Incomplete Block Designs,* Review of the International Statistical Institute, Vol. 32 (1964), N. 3, pág 251.

[18] Douglas R. Stinson, *Combinatorial Designs: Constructions and Analysis*, Springer-Verlag, 2004.

[19] K. Takeuchi, *A Table of Difference Sets Generating Balanced Incomplete Block Designs,* Review of the International Statistical Institute, Vol. 30 (1962), N. 3, págs. 361-366.

[20] Helge Toutenburg, Shalabh, *Statistical Analysis of Designed Experiments, Third Edition*, Springer, 2009.

[21] J. H. van Lint y R. M. Wilson, *A Course in Combinatorics, Second Edition*, Cambridge University Press, 2001.

[22] Ian N. Wakeling, Dominic Buck, *Balanced incomplete block designs useful for consumer experimentation,* Food Quality and Preference, Elsevier, Vol. 12 (2001), págs 265-268.

[23] H. Zeitler, *About special classes of Steiner systems S(2, 4, v),* Discrete Mathematics, Vol. 97 (1991), págs 399-407.