Universidad de Valladolid

Facultad de Ciencias

Trabajo de Fin de Grado

Grado en Matemáticas, 2016

Sistemas de Steiner y otros Diseños Combinatorios

Autor: Rubén Villa Muñoz

Tutor: José Enrique Marcos Naveira

Índice general

Introducción

La *teoría de diseños combinatorios* es una rama de la combinatoria que se ocupa de encontrar o crear una cierta regularidad sobre un conjunto de elementos. Este trabajo se centra en una parte (quizás la más importante) de la teoría de diseños combinatorios: La *definición y construcción de bloques*. La idea básica de la definición y construcción de bloques en la teoría de diseños combinatorios es la de *estructura de incidencia*, la cual se pregunta cómo ordenar un conjunto de elementos, también llamados puntos, dentro de otros conjuntos, también llamados bloques, con ciertas características. Este concepto de estructura de incidencia es tan amplio como la imaginación humana y las características que se exigen sobre los bloques y sobre el conjunto de elementos son muy variadas. Nosotros nos restringimos a que todos los bloques tengan el mismo número de elementos. Con esta restricción aparece el concepto de *t-diseño*, que se encarga de preguntar si existe un conjunto de bloques, todos ellos con un mismo número de puntos, en los que t puntos distintos estén en un número determinado de bloques. Esta pregunta se responde creando construcciones específicas de esos t-diseños. También se responde a la pregunta dando teoremas que nieguen la existencia de esos t-diseños o que la garanticen, en la mayoría de los casos, de forma constructiva. Una vez más volvemos a restringirnos al tratar el concepto de t-diseño y nos centramos en los *2-diseños*. A pesar de todas estas restricciones este trabajo no consigue recopilar todos los posibles aspectos a tratar en los 2-diseños. Fijamos nuestra atención en los aspectos más importantes y (a opinión propia) más llamativos, aun sabiendo que muchos otros quedan en el tintero.

En el primer capítulo tratamos los *sistemas triples de Steiner*, que son un caso específico de 2-diseños, posiblemente los más conocidos. Mostramos las propiedades y construcciones más importantes. Este capítulo sirve de introducción, pues nos permite concretar ideas.

El segundo capítulo aborda los 2-diseños. Trabajamos sobre todo en las construcciones y las acompañamos de ejemplos. Mostramos las propiedades fundamentales sin profundizar en ellas.

En el tercer capítulo nos centramos en un tipo específico de 2-diseños, los *2-diseños simétricos*. Ilustramos las propiedades que los caracterizan y exponemos las construcciones más relevantes fijándonos sobre todo en un tipo particular de 2-diseños simétricos, los *biplanos*.

El último capítulo trata brevemente las posibles aplicaciones de los 2-diseños. Aquí es donde reside el origen de esta teoría.

Damos dos apéndices, en los que se recoge, por un lado, una serie de resultados con su correspondiente desarrollo de cuadros latinos, necesarios para tratar con éxito ciertos aspectos del trabajo. Y por otro lado, hacemos una recopilación de todos los 2-diseños utilizados a lo largo del trabajo.

Capítulo 1

Sistemas Triples de Steiner

1.1. Definición y primeras propiedades

Denominaremos *terna* a un conjunto de 3 elementos; no importa el orden en el que los elementos aparezcan.

Definición 1.1 *[23] Un* **sistema triple de Steiner** *de orden v, denotado por STS(v), es un par (X,Λ) donde X es un conjunto con v elementos, o puntos, y Λ es un conjunto de ternas de X (también llamadas bloques) tal que todo par de elementos distintos de X está contenido en una única terna.*

Ejemplo 1 *El sistema triple de Steiner más sencillo posible (el trivial) es el que está formado únicamente por 3 elementos, los mínimos para formar un bloque. Por tanto, tenemos que* $X = \{1, 2, 3\}$ *y* $\Lambda = \{1, 2, 3\}$.

Ejemplo 2 *[19] Sea* $X = \{1, 2, 3, 4, 5, 6, 7\}$ *un conjunto de 7 elementos y* $\Lambda = \{\{1, 2, 5\}, \{1, 3, 6\}, \{1, 4, 7\}, \{2, 3, 7\}, \{2, 4, 6\}, \{3, 4, 5\}, \{5, 6, 7\}\}$ *un conjunto de ternas, formadas todas ellas por 3 elementos distintos; podemos comprobar como 2 elementos distintos de X están en un único bloque. A este sistema triple de Steiner suele asociarse la siguiente representación gráfica, conocida por plano de Fano:*

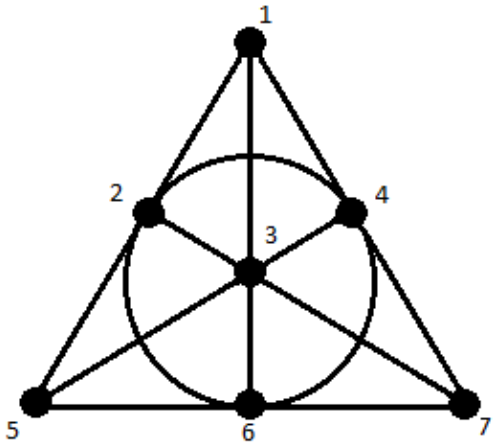

Figura 1.1: Plano de Fano

Esta representación gráfica se corresponde con el STS(7) previamente descrito, siendo los elementos de X los puntos y las ternas de Λ las rectas y la circunferencia.

Claramente, no todos los conjuntos de números naturales nos permiten formar un sistema triple de Steiner, por ejemplo $\{1, 2\}$, pues no podemos ni siquiera formar un bloque con tres elementos distintos. Por tanto, tenemos que dar condiciones de existencia para poder hablar en rigor de un STS(v). Para ello calculamos el número de veces que está contenido un elemento en los distintos bloques y el número de bloques que tiene un STS(v).

Proposición 1.2 *[19] En un sistema triple de Steiner de v elementos todo elemento está contenido en exactamente*

$$r = \frac{v-1}{2} \tag{1.1}$$

ternas.

Demostración: Tomemos un STS(v). Denotemos por X al conjunto de elementos y por Λ al conjunto de ternas del STS(v). Tomemos un elemento x de X y denotemos por r_x el número de ternas en los que aparece x. Definimos el siguiente conjunto:

$$\mathbf{I} = \{(y, A) : y \neq x, A \in \Lambda, \{x, y\} \subset A\}.$$

Calculamos el cardinal de $\mathbf{I}$ de dos formas distintas. Por un lado, puesto que $y \in$ X, $y \neq x$, tenemos $v-1$ posibles elecciones para y. Además, como estamos en un STS(v) tenemos una única elección de A $\in \Lambda$ tal que $\{x, y\} \subset$ A (definición 1.1). Luego, por un lado tenemos que $|\mathbf{I}| = v - 1$.
Por otro lado, tenemos r_x posibles ternas A $\in \Lambda$ en los que aparece x. Para cada terna tenemos dos posibles elecciones de y distintas de x. Luego $|\mathbf{I}| = 2r_x$. En consecuencia, $r_x = \frac{v-1}{2}$. Como el resultado obtenido no depende de la elección que hemos hecho del elemento x, concluimos que todo elemento está contenido en exactamente

$$r = \frac{v-1}{2}$$

ternas. ■

Luego, para que r sea un entero, v debe ser impar y tiene que ser mayor o igual que tres. A r lo denominamos *número de replicación.*

Proposición 1.3 *[19] Un sistema triple de Steiner de v elementos tiene exactamente*

$$b = \frac{vr}{3} = \frac{v(v-1)}{6} \tag{1.2}$$

ternas.

Demostración: Tomemos un STS(v). Sea $b = |\Lambda|$. Consideramos el conjunto

$$\mathbf{I} = \{(x, A) : x \in X, x \in A, A \in \Lambda\}.$$

Como en la demostración previa, calculamos $|\mathbf{I}|$ de dos formas diferentes. Por un lado, como en un STS(v) tenemos v formas posibles de seleccionar un elemento x, y por la proposición 1.2 sabemos que cada elemento x aparece en r ternas, tenemos $|\mathbf{I}| = vr$.
Por otro lado, como cada terna tiene 3 elementos tenemos que $|\mathbf{I}| = 3b$. Concluimos

$$vr = 3b \;\Rightarrow\; b = \frac{vr}{3} = \frac{v(v-1)}{6}$$

■

Para que b sea entero, *v(v-1)* tiene que ser múltiplo de 6. Además, como v es impar, tiene que ser de la forma $6h+3$ o $6h+1$, con $h \in \mathbb{N}$. Por tanto, estas dos proposiciones previas nos permiten dar una condición necesaria para la existencia de un STS(v), fijándonos únicamente en el valor de v.

Teorema 1.4 *[13] Si un STS(v) existe, entonces v ≡ 1 o 3 mod(6).*

Por tanto, sabemos que sistemas triples de Steiner de órdenes 30 o 5 no existen. El recíproco de este teorema también es cierto. Es decir, un STS(v) existe si y solo si $v \equiv 1$ o 3 mod (6), pero previamente a demostrar la implicación que nos falta construiremos STS(v) para diversos valores de v, lo cual nos facilitará el camino de la demostración recíproca.
Nótese que utilizando las fórmulas (1.1) y (1.2) y sustituyendo con los correspondientes valores, vemos que las fórmulas se cumplen para los ejemplos 1 y 2. En el ejemplo 1 con $v = 3$ tenemos que $b = \frac{3\cdot 2}{6} = 1$ y $r = \frac{3-1}{2} = 1$. Más interesante es el ejemplo 2, donde vemos que el número de bloques, b, es igual al número de elementos, 7, y como cada punto aparece en 3 bloques distintos. El hecho de que un STS(v) tenga el mismo número de elementos que de bloques solo ocurre para $v = 7$, como podemos observar a continuación

$$v = b \Leftrightarrow v = \frac{v(v-1)}{6} \Leftrightarrow 6v = v(v-1) \Leftrightarrow 6 = v - 1.$$

1.2. Construcciones

En esta sección mostraremos construcciones para formar sistemas triples de Steiner. Puesto que algunas de ellas son recurrentes, podemos deducir que existen una infinidad de STS(v). Por otro lado, aunque formar un STS(v) con v pequeño puede ser relativamente fácil y se puede realizar a mano (como en los ejemplos 1 y 2), cuando v es mayor que, por ejemplo 15, es realmente complicado en la mayoría de los casos crear un STS(v). Por eso es necesario formar construcciones como las que exponemos a continuación. De aquí en adelante denotaremos por ($\mathbb{Z}_n$,+) el grupo de enteros $\{0, 1, ..., n-1\}$ con la suma módulo n y si q es primo o potencia de primo, es decir, $q = p^n$ con p primo, por $\mathbb{F}_q$ el cuerpo finito de orden q, el cual tiene característica p.

1. Tomamos X = $(\mathbb{F}_2)^n \setminus \{\bar{\mathbf{0}}\}$, $\bar{\mathbf{0}}$ = (0,0,...,0), con $n \in \mathbb{N} : n \geq 2$ y definimos el siguiente conjunto de ternas:

$$\Lambda = \{\{x, y, z\} : x, y, z \in \mathrm{X}, x + y + z = \bar{\mathbf{0}}\}$$

Veamos que el par (X,Λ) forma un STS($2^n - 1$). Para ello tenemos que seleccionar un par de elementos cualquiera, $\{x, y\}$ con $x, y \in$ X tal que $x \neq y$, y verificar que están en un único bloque de Λ. De hecho, basta verificar que el elemento restante del bloque, z (el cual queda unívocamente determinado por la igualdad $x + y + z = \bar{\mathbf{0}}$), es distinto de $\bar{\mathbf{0}}$ y de x e y (ver definición 1.1). Razonemos por reducción al absurdo. Supongamos que $z = \bar{\mathbf{0}}$. Entonces $x + y = \bar{\mathbf{0}}$. Luego $x = -y$, y como estamos en un cuerpo de característica 2, $x = y$, lo cual es absurdo por como habíamos tomado el par $\{x, y\}$. Supongamos ahora que $z = x$ (el razonamiento es totalmente análogo con $z = y$). Entonces tendríamos que $x + y + z = x + y + x = 2x + y = y = \bar{\mathbf{0}}$, lo cual es absurdo, pues $y \in$ X. Por lo tanto, tenemos un STS($2^n - 1$). Esta construcción nos proporciona infinitos STS(v). Para cada valor de $n \geq 2$ tenemos un STS(v) asociado, con $v = 2^n - 1$.

n	$\mathbf{v = 2^n - 1}$
2	3
3	7
4	15
5	31
6	63

2. Espacio afín sobre $\mathbb{F}_3$.
Sea $((\mathbb{F}_3)^n,+)$, con $n \in \mathbb{N}$, lo consideramos como espacio afín de dimensión n sobre $\mathbb{F}_3$. Vamos a tomar como conjunto de elementos $X = (\mathbb{F}_3)^n$ y como Λ el conjunto de ternas asociadas a las rectas de $(\mathbb{F}_3)^n$. Entonces, $\{x, y, z\} \subset (\mathbb{F}_3)^n$ es una terna si y solo si $x + y + z = \bar{\mathbf{0}}$; con esta condición vamos a comprobar que tenemos un STS(3^n) y, como en el caso anterior, basta comprobar que una vez que hemos seleccionado el par $\{x, y\}$ con $x, y \in X$ tal que $x \neq$ y, el elemento restante de la terna, el cual queda unívocamente determinado, no es ni x ni y. Para ello, vamos a volver a razonar por reducción al absurdo. Supongamos que $z = x$ (el razonamiento es totalmente análogo con $z = y$). Entonces tendríamos que $x + y + z = x + y + x = 2x + y = \bar{\mathbf{0}}$. Por lo tanto $y = -2x$, lo cual es equivalente a que $y = x$, y esto es absurdo, pues habíamos supuesto que $\{x, y\}$ era un par de elementos distintos. Obsérvese que en esta construcción los bloques son las rectas afines, que por dos puntos distintos pasa una única recta afín y que cada recta afín tiene tres puntos. Por último, veamos en la siguiente tabla como para cada valor de n tenemos asociado un STS(v).

n	$\mathbf{v = 3^n}$
1	3
2	9
3	27
4	81
5	243

Ejemplo 3 *Si n = 2, obtenemos un STS(9). Consideramos como conjunto de elementos* $X = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$*, y como conjunto de bloques:*

$$\Lambda = \{\{1,2,3\}, \{4,5,6\}, \{7,8,9\}, \{1,4,7\}, \{2,5,8\}, \{3,6,9\}, \{1,5,9\}, \{2,6,7\}, \{3,4,8\}, \{1,6,8\}, \{2,4,9\}, \{3,5,7\}\}.$$

Obsérvese cómo la suma de todos los elementos de cada terna es 0 módulo 3*. En rigor, los elementos de X deberían ser* $\{(0,0),(0,1),(0,2),...,(2,2)\}$*. Este cambio es por mera cuestión estética.*

3. *STS(7)*[16].
Veamos cómo se puede formar un STS(7), como el del ejemplo 2, mediante un método conocido como *método en diferencias*. Identificaremos como elementos de X los elementos de $\mathbb{Z}_7$ y como bloques las ternas $B_x = \{x, x + 1, x + 3\}$ con $x \in \mathbb{Z}_7$. Este par, (X,B_x) con $x \in \mathbb{Z}_7$, es un STS(7); para comprobarlo basta observar que los bloques que hemos formado contienen cualquier pareja de elementos que elijamos una única vez. Este hecho se basa en que las seis posibles diferencias entre los elementos $\{0, 1, 3\}$ son todos los elemento no nulos de $\mathbb{Z}_7$. Por ejemplo, si queremos encontrar un bloque que contenga al par $\{1, 6\}$, tenemos que 6-1=1-3=5 en $\mathbb{Z}_7$. Entonces, basta tomar $x = 5$, pues x+1 = 6, x+3 = 1 en $\mathbb{Z}_7$, y por tanto el par está en el bloque B_5. Los bloques son:

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

Ejemplo 4 *Sea el STS(7) siguiente:*

$$\{\{x_0,x_1,x_3\},\{x_1,x_2,x_4\},\{x_2,x_3,x_5\},\{x_3,x_4,x_6\},\{x_0,x_4,x_5\},\{x_1,x_5,x_6\},\{x_0,x_2,x_6\}\}$$

*Ahora vamos a construir un STS(*15*) a partir del STS(*7*) previo. El conjunto de elementos es* $X = \{0,...,6,\infty,x_0,...,x_6\}$ *y los bloques son las 35 ternas siguientes:*

$\{0,\infty,x_0\}$ $\{1,6,x_0\}$ $\{2,5,x_0\}$ $\{3,4,x_0\}$
$\{1,\infty,x_1\}$ $\{2,0,x_1\}$ $\{3,6,x_1\}$ $\{4,5,x_1\}$
$\{2,\infty,x_2\}$ $\{3,1,x_2\}$ $\{4,0,x_2\}$ $\{5,6,x_2\}$
$\{3,\infty,x_3\}$ $\{4,2,x_3\}$ $\{5,1,x_3\}$ $\{6,0,x_3\}$
$\{4,\infty,x_4\}$ $\{5,3,x_4\}$ $\{6,2,x_4\}$ $\{0,1,x_4\}$
$\{5,\infty,x_5\}$ $\{6,4,x_5\}$ $\{0,3,x_5\}$ $\{1,2,x_5\}$
$\{6,\infty,x_6\}$ $\{0,5,x_6\}$ $\{1,4,x_6\}$ $\{2,3,x_6\}$
$\{x_0,x_1,x_3\}\{x_1,x_2,x_4\}\{x_2,x_3,x_5\}\{x_3,x_4,x_6\}\{x_0,x_4,x_5\}\{x_1,x_5,x_6\}\{x_0,x_2,x_6\}$

Se puede comprobar como seleccionando cualquier par de elementos de X existe un único bloque en el que ese par está contenido. Veamos ahora la construcción que generaliza la anterior.

4. *Construcción de un STS(2v+1) a partir de un STS(v).*
Sea un STS(v), cuyos elementos los denotamos por X $= \{x_0,x_1,...,x_{v-1}\}$. Consideremos el nuevo conjunto de elementos X' = X$\cup\{0,1,...,v-1,\infty\}$ (en total $2v+1$ elementos). Ahora, para cada $i=0,1,...,v-1$, denotamos $F_i = \{\{x+i,-x+i\} : x \in \mathbb{Z}_v, x \neq 0\} \cup \{\{i,\infty\}\}$. Para cada $i=0,1,...,v-1$, formamos las ternas $\{a,b,x_i\}$ donde $\{a,b\} \in F_i$, es decir, el siguiente conjunto:

$$\left\{ \begin{array}{l} \{i,\ \infty,\ x_i\}, \\ \{x-i,\ x+i,\ x_i\} \end{array} \right\} \text{ con } i=0,...,v-1 \text{ y } x \in \mathbb{Z}_v.$$

El conjunto de todas las posibles ternas previas más las ternas del STS(v) original nos proporcionan un STS($2v$+1) cuyos elementos son los de X'; para comprobar que realmente hemos formado un STS($2v$+1) basta ver que para cada par de elementos distintos de X' existe una terna de los arriba descritas que contiene a ese par. Si uno de los elementos es ∞, es inmediato observar que el par está en un única terna. Si el par es de la forma $\{x_k,x_j\}$ con $k \neq j$, el par está en el STS(v) que habíamos tomado de partida. Si el par es de la forma $\{k,j\}$ con $k,j \in \mathbb{Z}_v$ y $k \neq j$ entonces tenemos que fijarnos en los pares de F_i y resolver el siguiente sistema compatible determinado:

$$\left\{ \begin{array}{l} i+x=k \\ i-x=j \end{array} \right. \text{ con } x,i \in \mathbb{Z}_v. \tag{1.3}$$

Entonces $i=j+x$, y por tanto, sustituyendo en (1.3), tenemos $2x=k-j$ en $\mathbb{Z}_v$. Esta operación tiene sentido, pues v es impar. De aquí calculamos tanto x como i, tras una sustitución en (1.3), y tenemos nuestro par $\{k,j\}$ en una terna, en la asociada a F_i. Por último, nos falta verificar que un par de la forma $\{k,x_j\}$ está en alguna terna. Basta observar que volvemos a tener un sistema de dos ecuaciones con dos incógnitas como en (1.3), donde ahora tenemos fijado el valor i y k, luego tenemos que calcular x y el otro elemento del par F_i. Este cálculo podemos hacerlo con el mismo procedimiento anterior.

Para los dos ejemplos siguientes hemos consultado [16, Capítulo 19].

5. *Construcción de un STS(w) a partir de un STS(v_1) y un STS(v_2), donde $w = v_1v_2$.*
Sean X_1 y X_2 conjuntos de elementos. Tenemos asociado a cada uno un STS(v_1) y un STS(v_2), respectivamente. Definimos como conjunto de elementos $\mathrm{X} = X_1 \times X_2$ y definimos como conjunto de bloques $\{(x_1, y_1), (x_2, y_2), (x_3, y_3)\}$ aquellos que cumplen una de las tres condiciones siguientes:

1) $x_1 = x_2 = x_3$ y $\{y_1, y_2, y_3\}$ es un bloque del STS(v_2).
2) $y_1 = y_2 = y_3$ y $\{x_1, x_2, x_3\}$ es un bloque del STS(v_1).
3) $\{x_1, x_2, x_3\}$ es un bloque de STS(v_1) y $\{y_1, y_2, y_3\}$ es un bloque del STS(v_2).

Es prácticamente obvio ver que así hemos definido un STS(v_1v_2). Aun así, vamos a comprobar que el número de bloques es el correcto, para ello hacemos uso de la fórmula (1.2). Si coinciden habríamos demostrado que es un STS(v_1v_2), pues el resto de condiciones de la definición 1.1 claramente se cumplen, pues hay v_1v_2 elementos y cada terna tiene tres elementos distintos; denotamos por b_i el número de ternas del STS(v_i) y por v_i el número de elementos de X_i, con $i = 1, 2$. Entonces, si cumplen la condición 1, fijamos un elemento de X_1, v_1 posibles, y tenemos todas las ternas del STS(v_2), b_2 en total. Luego son v_1b_2 bloques los que cumplen la condición 1. De forma totalmente análoga razonamos para la condición 2, tenemos así v_2b_1 posibles ternas. Por último, las ternas de la condición 3. Fijo 2 elementos del conjunto X_1 (esto es $\binom{v_1}{2}$) y multiplicamos por el número de bloques de STS(v_2), b_2, e igual pero al revés para X_2. Tenemos así $b_1\binom{v_2}{2} + b_2\binom{v_1}{2}$ ternas del tercer tipo. Utilizando la fórmula (1.2) para el STS(v_1v_2) vemos que $b_{v_1v_2} = \frac{v_1v_2(v_1v_2-1)}{6}$. Comprobamos que la suma de los bloques previamente calculados coincide con $b_{v_1v_2}$.

$$b_1\binom{v_2}{2} + b_2\binom{v_1}{2} + b_1v_2 + b_2v_1 =$$
$$\frac{v_1(v_1-1)}{6}\frac{v_2(v_2-1)}{2} + \frac{v_2(v_2-1)}{6}\frac{v_1(v_1-1)}{2} + \frac{v_2v_1(v_1-1)}{6} + \frac{v_1v_2(v_2-1)}{6} =$$
$$\frac{v_1v_2}{6}\left(\frac{(v_2-1)(v_1-1)}{2} + \frac{(v_1-1)(v_2-1)}{2} + v_1 - 1 + v_2 - 1\right) =$$
$$\frac{v_1v_2}{6}\left((v_2-1)(v_1-1) + (v_1-1) + (v_2-1)\right) =$$
$$\frac{v_1v_2}{6}\left(v_2v_1 - v_2 - v_1 + 1 + v_1 - 1 + v_2 - 1\right) = \frac{v_1v_2}{6}\left(v_1v_2 - 1\right)$$
$$= b_{v_1v_2}.$$

Luego el número de bloques es el correcto.

6. Construcción de un STS($uv - v + 1$) a partir de un STS(u) y un STS(v)[16, página 236].
Al STS(u) le asociamos el par (X, Λ) y al STS(v) el par (Y, Γ), donde vamos a considerar $X = \mathbb{Z}_{u-1} \cup \{p\}$. Nótese que STS($uv - v + 1$) = STS($(u-1)v + 1$). Por tanto, definimos como nuevo conjunto de elementos $(\mathrm{X} \setminus \{p\}) \times Y \cup \{p\} = \mathbb{Z}_{u-1} \times Y \cup \{p\}$ y como conjunto de bloques los siguientes:

   a) $\{(x_1, y), (x_2, y), (x_3, y)\}$ tal que $\{x_1, x_2, x_3\} \in \Lambda, p \notin \{x_1, x_2, x_3\}, y \in Y$.
   b) $\{p, (x_2, y), (x_3, y)\}$ tal que $\{p, x_2, x_3\} \in \Lambda, y \in Y$.
   c) $\{(x_1, y_1), (x_2, y_2), (x_3, y_3)\}$ tal que $x_1 + x_2 + x_3 \equiv 0 \bmod (u-1), x_1, x_2, x_3 \in \mathbb{Z}_{u-1}$ y $\{y_1, y_2, y_3\} \in \Gamma$.

Resulta claro que el conjunto de punto junto con el conjunto de bloques previamente definido forma un STS($uv - v + 1$).

Ejemplo 5 *Como caso concreto de esta construcción previa podemos formar un STS(2v+1) a partir de un STS(v) dado. Basta tomar* $X = \mathbb{Z}_2 \cup \{3\}$ *y asociar* Y *al conjunto de elementos del STS(v). Entonces el conjunto de elementos es* $(X \setminus \{3\}) \times Y \cup \{3\}$ *y el conjunto de bloques*

1. $\{3, (1, y), (2, y)\}$ *tal que* $y \in Y$.
2. $\{(1, y_1), (1, y_2), (2, y_3)\} \cup \{(2, y_1), (2, y_2), (2, y_3)\}$ *tal que* $\{y_1, y_2, y_3\} \in \Gamma$, *con* $1, 2 \in \mathbb{Z}_2$.

Las dos próximas construcciones nos van a permitir demostrar la implicación restante del teorema 1.4, es decir, un STS(v) existe **si y solo si** $v \equiv 1$ o 3 mod (6). Nos hemos basado en [13, capítulo 3] y en [19, capítulo 6]. Para la segunda construcción hemos hecho uso de algunos resultados de cuadros latinos y cuasigrupos, véase apéndice A. Puesto que $v \equiv 1$ o 3 mod (6), será suficiente probar la existencia de STS(v) para estos dos casos.

7. ***Caso v = 6t+3***.
   Sean el conjunto de elementos X = $\mathbb{Z}_{2t+1} \times \mathbb{Z}_3$ y el conjunto de bloques

   $\{(i, 0), (i, 1), (i, 2)\}$ para cada $i \in \mathbb{Z}_{2t+1}$,
   $\{(i, k), (j, k), (\frac{1}{2}(i + j), k + 1)\}$ para cada $i, j \in \mathbb{Z}_{2t+1}, i \neq j, k \in \mathbb{Z}_3$.

   Nótese que tiene sentido multiplicar por $\frac{1}{2}$, pues estamos operando en un grupo con un número impar de elementos, es decir, la multiplicación por $\frac{1}{2}$ es equivalente a multiplicar por $t + 1$ en $\mathbb{Z}_{2t+1}$; el número de bloques totales es $b = (2t + 1) + 3\binom{2t+1}{2} = \frac{v(v-1)}{6} = \frac{1}{3}\binom{v}{2}$. Vamos a comprobar que para todo par de elementos distintos, $x = (x_1, x_2)$, $y = (y_1, y_2) \in$ X, existe al menos una terna de las arriba descritas que los contiene. Los bloques contienen en total $3b = \binom{v}{2}$ subconjuntos de 2 elementos de X, luego todo par está en exactamente una terna. Entonces, si $x_1 = y_1$ el par $\{x, y\}$ está contenido en un bloque del primer tipo. Supongamos que $x_1 \neq y_1$. Si $x_2 = y_2$ es claro que el par está contenido en un bloque del segundo tipo. Por último, si $x_2 \neq y_2$, podemos suponer, sin pérdida de generalidad, que $x_2 = y_2 + 1$ (el caso $y_2 = x_2 + 1$ es totalmente análogo), recordemos que $x_2, y_2 \in \mathbb{Z}_3$. Por tanto el par $\{x, y\}$ está contenido en un bloque del segundo tipo con $j = 2x_1 - y_1$, pues $(t + 1)(y_1 + 2x_1 - y_1) = (2t + 2)x_1 = x_1$ en $\mathbb{Z}_{2t+1}$.

Con esta construcción hemos construido sistemas triples de Steiner para la mitad de valores posibles de v, y con la siguiente completaremos la otra mitad de valores que faltan.

8. ***Caso v = 6t+1*** [19, páginas 130-131].
   Sea $(\{0, 1, ..., 2t - 1\}, \circ)$ un cuasigrupo simétrico half-idempotente de orden $2t$ (consultar apéndice A). Definimos X=$(\{0, 1, ..., 2t - 1\} \times \mathbb{Z}_3) \cup \{\infty\}$ (este es el conjunto de elementos del STS(v)). Para $0 \leq x \leq t - 1$, definimos las ternas:

   $$A_x = \{(x, 0), (x, 1), (x, 2)\}.$$

   Para todo $x, y \in \{0, 1, ..., 2t - 1\}$, $x < y$, y para $i \in \mathbb{Z}_3$, definimos las ternas siguientes, donde la operación en la segunda componente es módulo 3:

   $$B_{x,y,i} = \{(x, i), (y, i), (x \circ y, i + 1)\}.$$

Y finalmente, para $0 \leq x \leq t-1$ y para $i \in \mathbb{Z}_3$, definimos las ternas siguientes, donde la operación en la segunda componente también es módulo 3:

$$C_{x,i} = \{\infty, (x+t, i), (x, i+1)\}.$$

Por tanto, el conjunto de ternas es

$$\{A_x : 0 \leq x \leq t-1\} \cup \{B_{x,y,i} : x, y \in \mathbb{Z}_{2t}, x < y, i \in \mathbb{Z}_3\} \cup \{C_{x,i} : 0 \leq x \leq t-1, i \in \mathbb{Z}_3\}$$

Vamos a ver que el par (X, Λ) es un STS(v). Claramente hay v elementos en X y cada terna de Λ contiene tres elementos, luego es suficiente comprobar que todo par de elementos está en exactamente una terna.
Consideremos el par de elementos $p_1 = (\alpha, j), \infty$. Si $\alpha \leq t-1$, entonces este par está en la terna $C_{\alpha,j-1}$, recordemos que la segunda coordenada es operada módulo 3. Si en cambio, $\alpha \geq t$, entonces el par está en la terna $C_{\alpha-t,j}$.
Ahora consideremos el par de elementos $p_1 = (\alpha, j)$ y $p_2 = (\beta, k)$. Si $\alpha = \beta \leq t-1$, el par está en la terna A_α. Supongamos que $\alpha = \beta \geq t$. Como $j \neq k$, sin pérdida de generalidad, podemos suponer que $k = (j+1) \bmod (3)$. La ecuación $\alpha \circ x = \alpha$ tiene una única solución, digamos $x = \gamma$. Por tanto, si $\gamma > \alpha$, el par está en la terna $B_{\alpha,\gamma,j}$. Si en cambio, $\alpha > \gamma$, como $\circ$ es una operación simétrica, tenemos que el par p_1 y p_2 pertenece a la terna $B_{\gamma,\alpha,j}$.
Por último, consideremos el caso en el que $\alpha \neq \beta$. Sin pérdida de generalidad podemos suponer que $\alpha < \beta$. Debemos distinguir tres casos:

a) Si $k = j$, el par está en la terna $B_{\alpha,\beta,j}$.

b) Si $k = (j+1) \bmod (3)$, entonces la ecuación $x \circ \alpha = \beta$ tiene una única solución, $x = \gamma$. Obsérvese que $\gamma \neq \alpha$, pues $\alpha < \beta$ y $\alpha \circ \alpha \leq \alpha$ para todo α. Si $\gamma < \alpha$, entonces el par $p_1,\ p_2$ está en la terna $B_{\gamma,\alpha,j}$. Si por el contrario, $\alpha < \gamma$, como $\circ$ es simétrica, el par $p_1,\ p_2$ está en la terna $B_{\alpha,\gamma,j}$.

c) Si $j = (k+1) \bmod (3)$, entonces la ecuación $x \circ \beta = \alpha$ tiene una única solución, digamos $x = \gamma$. Entonces tenemos que $\gamma = \beta$ si y solo si $\beta = \alpha + t$. Si esto ocurre, el par $p_1,\ p_2$ está en la terna $C_{\alpha,k}$. Por otro lado, si $\gamma < \beta$, el par $p_1,\ p_2$ está en la terna $B_{\gamma,\beta,k}$. Y por último, si $\beta < \gamma$, como $\circ$ es simétrica, el par $p_1,\ p_2$ está en la terna $B_{\beta,\gamma,k}$.

Para complementar esta demostración se pueden consultar unos diagramas en [12] que aclaran gráficamente como son las ternas.

Ejemplo 6 *Vamos a construir mediante este procedimiento un STS(19). Sea un cuasigrupo simétrico half-idempotente de orden 6, como el construido en el ejemplo 44 del apéndice A. Este cuasigrupo está definido sobre el conjunto* $\{0,1,2,3,4,5\}$*, por tanto, nuestro conjunto de elementos es* $X = (\{0,1,2,3,4,5\} \times \{0,1,2\}) \cup \{\infty\}$*. Representaremos los elementos de X como (0,0), (0,1), (0,2), (1,0), (1,1), (1,2),..., (5,0), (5,1), (5,2) y* ∞*. Haciendo uso de la fórmula (1.2) vemos que hay 57 bloques. En la siguiente tabla representamos primero los tres bloques del tipo* A_x *con* $0 \leq x \leq 2$*, seguidos de los 45 del tipo* $B_{x,y,i}$ *con* $0 \leq x < y \leq 5, 0 \leq i \leq 2$ *y los 9 bloques del tipo* $C_{x,i}$ *con* $0 \leq x \leq 2, 0 \leq i \leq 2$*. Añadimos al final la permutación* π *utilizada para construir el cuasigrupo.*

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

$$
\begin{array}{ccc}
\{(0,0),(5,0),(5,1)\} & \{(0,1),(5,1),(5,2)\} & \{(0,2),(5,2),(5,0)\} \\
\{(1,0),(2,0),(4,1)\} & \{(1,1),(2,1),(4,2)\} & \{(1,2),(2,2),(4,0)\} \\
\{(1,0),(3,0),(2,1)\} & \{(1,1),(3,1),(2,2)\} & \{(1,2),(3,2),(2,0)\} \\
\{(1,0),(4,0),(5,1)\} & \{(1,1),(4,1),(5,2)\} & \{(1,2),(4,2),(5,0)\} \\
\{(1,0),(5,0),(0,1)\} & \{(1,1),(5,1),(0,2)\} & \{(1,2),(5,2),(0,0)\} \\
\{(2,0),(3,0),(5,1)\} & \{(2,1),(3,1),(5,2)\} & \{(2,2),(3,2),(5,0)\} \\
\{(2,0),(4,0),(0,1)\} & \{(2,1),(4,1),(0,2)\} & \{(2,2),(4,2),(0,0)\} \\
\{(2,0),(5,0),(3,1)\} & \{(2,1),(5,1),(3,2)\} & \{(2,2),(5,2),(3,0)\} \\
\{(3,0),(4,0),(3,1)\} & \{(3,1),(4,1),(3,2)\} & \{(3,2),(4,2),(3,0)\} \\
\{(3,0),(5,0),(1,1)\} & \{(3,1),(5,1),(1,2)\} & \{(3,2),(5,2),(1,0)\} \\
\{(4,0),(5,0),(4,1)\} & \{(4,1),(5,1),(4,2)\} & \{(4,2),(5,2),(4,0)\} \\
\hline
\{\infty,(3,0),(0,1)\} & \{\infty,(3,1),(0,2)\} & \{\infty,(3,2),(0,0)\} \\
\{\infty,(4,0),(1,1)\} & \{\infty,(4,1),(1,2)\} & \{\infty,(4,2),(1,0)\} \\
\{\infty,(5,0),(2,1)\} & \{\infty,(5,1),(2,2)\} & \{\infty,(5,2),(2,0)\}
\end{array}
$$

La permutación π viene definida como $\pi(0)=0,\ \pi(1)=3,\ \pi(2)=1,\ \pi(3)=4,\ \pi(4)=2$ y $\pi(5)=5$, y la operación del cuasigrupo por:

$$x \circ y = \pi((x+y)\ \textit{mod}\ (n)).$$

Con esto se finaliza la prueba de la construcción para el caso $v = 6t+1$, juntándola con la construcción anterior, caso $v = 6t+3$, y con el teorema 1.4 concluimos esta sección con el siguiente resultado:

Teorema 1.5 *Un STS(v) existe si y solo si $v \equiv 1$ o 3 mod (6).*

1.3. Isomorfismos y Subsistemas

Definición 1.6 *[20] Dos sistemas triples de Steiner son* **isomorfos** *si existe una biyección entre los conjuntos de elementos, que asigna bloques a bloques. Dicha biyección es un isomorfismo. Un* **automorfismo** *de un sistema triple de Steiner es un isomorfismo de un STS(v) en sí mismo.*

Ejemplo 7 *[19] Sean dos STS(7), (X,Λ) y (Y,Δ):*

$$
\begin{array}{l}
X = \{1,2,3,4,5,6,7\}\ y \\
\Lambda = \{\{123\},\{145\},\{167\},\{246\},\{257\},\{347\},\{356\}\}. \\
Y = \{a,b,c,d,e,f,g\}\ y \\
\Lambda = \{\{abd\},\{bce\},\{cdf\},\{deg\},\{aef\},\{bfg\},\{acg\}\}.
\end{array}
$$

Definimos la biyección α como $\alpha(1)=a,\ \alpha(2)=b,\ \alpha(3)=d,\ \alpha(4)=c,\ \alpha(5)=g,\ \alpha(6)=e,\ \alpha(7)=f$. Entonces, cuando reescribimos los elementos de X bajo la acción de α, los bloques de Λ son los siguientes:

$$
\begin{array}{l}
123 \to abd \\
145 \to acg \\
167 \to aef \\
246 \to bce \\
257 \to bfg \\
347 \to cdf \\
356 \to deg.
\end{array}
$$

Por tanto, α es un isomorfismo. De hecho, es un automorfismo y ambos sistemas, (X,Λ) y (Y,Δ), son isomorfos.

El número de STS(v) no isomorfos se denota por $N(v)$. Los sistemas triples de Steiner de orden $v = 3, 7, 9$ son únicos, es decir, $N(3) = N(7) = N(9) = 1$. Para $v = 13$ hay dos sistemas no isomorfos, $N(13) = 2$. Ambos tienen en común los siguientes bloques (véase [8]):

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

Los bloques no comunes de uno de los sistemas son

$\{3,\ 6,\ 10\}$ $\{5,\ 6,\ 13\}$
$\{3,\ 9,\ 13\}$ $\{5,\ 9,\ 10\}$

Y los bloques del otro sistemas son

$\{3,\ 6,\ 13\}$ $\{5,\ 6,\ 10\}$
$\{3,\ 9,\ 10\}$ $\{5,\ 9,\ 13\}$

Para $v = 15$ hay 80 STS(15) no isomorfos, $N(15) = 80$. Estos pueden encontrarse en [9, parte I].
Para el último valor de v que hay datos conocidos es para $v = 19$. Se comprobó en [20] que hay 1108487429 sistemas triples de Steiner no isomorfos de orden 19. En la siguiente tabla puede observarse el crecimiento de tipo exponencial de $N(v)$.

v	3	7	9	13	15	19	21
N(v)	1	1	1	2	80	11084874829	?

La siguiente cota para $N(v)$ fue probada en [6]

$$(e^{-5}v)^{v^2/6} \leq N(v) \leq (e^{-1/2}v)^{v^2/6}.$$

Cualquier demostración de los resultados arriba mencionados excede las pretensiones de este trabajo.

Definición 1.7 *Sea (X,Λ) un STS(v). Decimos que el par (Y,Δ), donde Y es un subconjunto de w elementos de X y Δ es un subconjunto de Λ, es un* **subsistema** *de STS(v) si (Y,Δ) forma un STS(w).*

Ejemplo 8 *Dado un STS(7) como el del ejemplo previo, es inmediato observar que hay siete subsistemas isomorfos al STS(3).*

Ya hemos construido a lo largo de la sección 1.2 varios STS(v) con subsistemas, véase las construcciones 4, 5 y 6. Juntando el par de teoremas que exponemos a continuación y utilizando los conceptos de subsistemas y sistemas triples de Steiner isomorfos, en [8, páginas 280-283], podemos encontrar una demostración distinta del teorema 1.5. Esta se basa en ir haciendo construcciones iterativas y así construir cualquier STS(v) con $v = 6$t+1 o $v = 6$t+3.

Teorema 1.8 *[8] Dados dos sistemas triples de Steiner de órdenes v_1 y v_2, existe un STS(w) con $w = v_1 v_2$ que contiene subsistemas isomorfos a los dados de orden v_1 y v_2.*

Demostración: Este teorema ya ha sido demostrado en la construcción 5 de la sección 1.2. ■

Teorema 1.9 *[25] Sean A=STS(v_1) y B=STS(v_2), el cual contiene un subsistema C de v_3 elementos. Entonces existe un D=STS(v) donde $v = v_3 + v_1(v_2 - v_3)$ que contiene v_1 subsistemas de v_2 elementos, un subsistema de v_1 elementos y un subsistema de v_3 elementos.*

Esta última demostración puede encontrarse en [25, capítulo 12].

Por último, mencionar que en [28] se comprobó que el número de STS(21) no isomorfos que tienen un subsistema triple de Steiner de orden 9 es 12661527336 y que el número de STS(27) no isomorfos que tienen un subsistema triple de Steiner de orden 13 es 1356574942538935943268083236.

1.4. Familias de Diferencias

Definición 1.10 *[19] Sea $(G, +)$ un grupo finito de orden v, en el cual el elemento identidad es denotado por 0. Una $(v, 3, 1)$-***familia de diferencias** *en $(G, +)$ es una colección de subconjuntos de G, digamos $\{D_1, ..., D_L\}$, que cumple las siguientes propiedades:*

1. $|D_i| = 3$ *para todo* $i, 1 \leq i \leq L$.
2. *La unión*

$$\bigcup_{i=1}^{L} \{x - y : x, y \in D_i, x \neq y\}$$

contiene a cada elemento de $G \setminus \{0\}$ exactamente una vez.

Los conjuntos D_i son llamados **bloques base**.

Ejemplo 9 *[19] Una (13,3,1)-familia de diferencias en ($\mathbb{Z}_{13}, +$):*

$$\{\{0, 1, 4\}, \{0, 2, 8\}\}.$$

Las diferencias obtenidas módulo 13 de la primera terna son 1,3,4,9,10 y 12, y de la segunda terna son 2,5,6,7,8 y 11. Decimos que es una ($13, 3, 1$)-familia de diferencias porque hemos obtenido todos los elementos de $\mathbb{Z}_{13}$ no nulos una única vez a partir de ternas de 3 elementos.

A continuación damos la relación entre las familias de diferencias y el concepto básico sobre el que trabajamos en este capítulo: los sistemas triples de Steiner. Primeramente nótese que las $(v, 3, 1)$-familias de diferencias y los STS(v) tienen en común que los bloques son de tres elementos distintos. Nótese que en ambos conjuntos aparece la v para denotar el número de elementos de los conjuntos.
Dado un conjunto de bloques base, D_1, ..., D_L, llamamos el **desarrollo**, o el **trasladado**, de estos bloques al conjunto $D_i + g$ para cada $i = 1, ..., L$, donde $g \in G$.

Proposición 1.11 *[9] Si los bloques base $D_1, ...D_L$ forman una $(v, 3, 1)$-familia de diferencias sobre G, entonces el desarrollo de estos bloques constituyen un STS(v).*

Demostración: Bastará comprobar que dados dos elementos distintos del grupo G existe un único bloque del desarrollo que los contiene. Sean $x, y \in G, x \neq y$. Como tenemos una $(v, 3, 1)$-familia de diferencias, sabemos que existe únicamente un índice $j \in \{0, 1, ..., L\}$ de forma que

$$0 \neq x - y = \beta - \gamma, \text{ con } \beta, \gamma \in D_j.$$

Luego

$$x - \beta = y - \gamma = g, \text{ con } g \in G \setminus \{0\}.$$

Por tanto tenemos

$$\begin{cases} x = \beta + g \\ y = \gamma + g \end{cases} \Rightarrow x, y \in (D_j + g).$$

■

Definición 1.12 *Si el grupo G en el que está basada la $(v, 3, 1)$-familia de diferencias es cíclico, entonces decimos que la familia de diferencias es* **cíclica**.
Decimos que un bloque base D de una familia de diferencias sobre un grupo G es un **bloque de ciclo corto** *si su trasladado vuelve a ser el mismo para algún elemento no nulo de G, es decir, si $D + g = D$, con $g \in G \setminus \{0\}$.*
Decimos que la **longitud** *de un bloque base es igual al número de bloques distintos que podemos obtener a partir del bloque base trasladado.*

La longitud de un bloque es $|G|$, mientras que en los bloques de ciclo corto es estrictamente menor. De hecho, es un divisor del orden de G.

Ejemplo 10 *[8] Sea $G = \mathbb{Z}_{15}$. Consideramos una $(15, 3, 1)$-familia de diferencias, cuyos bloques base son:*

$$\{\{0, 1, 4\}, \{0, 7, 13\}, \{0, 5, 10\}\}$$

Haciendo el desarrollo de estos bloques obtenemos un STS(15).

$\{0, 1, 4\}$	$\{0, 7, 13\}$	$\{0, 5, 10\}$
$\{1, 2, 5\}$	$\{1, 8, 14\}$	$\{1, 6, 11\}$
$\{2, 3, 6\}$	$\{2, 9, 0\}$	$\{2, 7, 12\}$
$\{3, 4, 7\}$	$\{3, 10, 1\}$	$\{3, 8, 13\}$
$\{4, 5, 8\}$	$\{4, 11, 2\}$	$\{4, 9, 14\}$
$\{5, 6, 9\}$	$\{5, 12, 3\}$	
$\{6, 7, 10\}$	$\{6, 13, 4\}$	
$\{7, 8, 11\}$	$\{7, 14, 5\}$	
$\{8, 9, 12\}$	$\{8, 0, 6\}$	
$\{9, 10, 13\}$	$\{9, 1, 7\}$	
$\{10, 11, 14\}$	$\{10, 2, 8\}$	
$\{11, 12, 0\}$	$\{11, 3, 9\}$	
$\{12, 13, 1\}$	$\{12, 4, 10\}$	
$\{13, 14, 2\}$	$\{13, 5, 11\}$	
$\{14, 0, 3\}$	$\{14, 6, 12\}$	

El lector puede comprobar cómo cualquier pareja de elementos distintos de $\mathbb{Z}_{15}$ está en un único bloque. Obsérvese como el bloque $\{0, 5, 10\}$ es un bloque de ciclo corto, pues su longitud es 5, frente a la longitud 15 de los otros dos bloques base. Esto es causado porque las posibles diferencias de la terna $\{0, 5, 10\}$ son dos en vez de seis como en las otras. En este caso, como la familia de diferencias está basada en $\mathbb{Z}_{15}$, es una familia de diferencias cíclica. Por tanto, volvemos a obtener este mismo STS(15) si tomamos cualquiera de los bloques desplazados de un cierto bloque base y lo reemplazamos por su correspondiente bloque base.

En la tabla siguiente adjuntamos los bloques base de $(v, 3, 1)$-familias de diferencias cíclicas para $v \leq 21$, con las cuales podemos formar STS(v). Los bloques de ciclo corto son escritos en cursiva para diferenciarlos. Una colección más amplia de las $(v, 3, 1)$-familias de diferencias se puede encontrar en [9, página 271-272], con valores de v comprendidos entre 7 y 81.

v	**Bloques Base**
7	$\{0, 1, 3\}$
13	$\{0, 1, 4\}$;$\{0, 2, 7\}$
15	$\{0, 1, 4\}$;$\{0, 2, 9\}$;*{0,5,10}*
19	$\{0, 1, 4\}$;$\{0, 2, 9\}$;$\{0, 5, 11\}$
21	$\{0, 1, 3\}$;$\{0, 4, 12\}$;$\{0, 5, 11\}$;*{0,7,14}*

Concluimos esta sección con una construcción basada en el método de diferencias, véase [16].

Sea $q = 6t + 1$ una potencia de un número primo y α una raíz primitiva del cuerpo $\mathbb{F}_q$, es decir, $\mathbb{F}_q^*$ es un grupo cíclico generado por α, orden(α)=$6t$. El conjunto de elementos es X = $\mathbb{F}_q^*$. Denotamos $\alpha^{2t} - 1 = \alpha^s$. Definimos el siguiente bloque básico:

$$B_0 = \{\alpha^0 = 1, \alpha^{2t}, \alpha^{4t}\}.$$

Ahora calculamos las 6 posibles diferencias que hay entre los elementos de B_0 teniendo en cuenta el orden de α, la definición de α^s y que $\alpha^{3t} = -1$.

$$\begin{array}{ll} \alpha^{2t} - 1 = \alpha^s, & -(\alpha^{2t} - 1) = \alpha^{s+3t}, \\ \alpha^{4t} - \alpha^{2t} = \alpha^{s+2t}, & -(\alpha^{4t} - \alpha^{2t}) = \alpha^{s+5t}, \\ \alpha^{6t} - \alpha^{4t} = \alpha^{s+4t}, & -(1 - \alpha^{4t}) = \alpha^{s+t}. \end{array}$$

Estas 6 diferencias de B_0 las representamos en el siguiente conjunto:

$$\Delta B_0 = \{\alpha^s, \alpha^{t+s}, \alpha^{2t+s}, \alpha^{3t+s}, \alpha^{4t+s}, \alpha^{5t+s}\}.$$

Consideramos como bloques base los siguientes, donde $0 \leq i \leq t - 1$:

$$B_i = \alpha^i B_0 = \alpha^i\{\alpha^0, \alpha^{2t}, \alpha^{4t}\} = \{\alpha^i, \alpha^{2t+i}, \alpha^{4t+i}\}.$$

Ahora, fijado un i, volvemos a calcular las 6 posibles diferencias entre los elementos de B_i, que representamos en el siguiente conjunto:

$$\Delta B_i = \{\alpha^{s+i}, \alpha^{t+s+i}, \alpha^{2t+s+i}, \alpha^{3t+s+i}, \alpha^{4t+s+i}, \alpha^{5t+s+i}\} = \alpha^i \Delta B_0.$$

Puesto que $\mathbb{F}_q^*$ es un grupo cíclico generado por α sabemos que

$$\bigcup_{i=0}^{t-1} \Delta B_i = \{\alpha^0, \alpha^1, ..., \alpha^{6t-1}\} = \mathbb{F}_q^*$$

Concluimos esta construcción haciendo notar que los bloques base son los B_i y el conjunto $\{B_i\}_{i=0}^{t-1}$ es una $(q, 3, 1)$-familia de diferencias. En consecuencia, $\{a + B_i : i = 0, ..., t - 1, a \in \mathbb{F}_q\}$ es el conjunto de ternas de un STS(q).

1.5. Partición en Diferencias

Para esta sección hemos utilizado como referencia [25, capítulo 12], que trata este tema bajo el nombre de *sistemas triples cíclicos*. También se puede encontrar sobre este tema en [9, parte IV, capítulo 43], asociado al nombre de *primer y segundo problema de Heffter*. Recordemos que $(\mathbb{Z}_n, +)$ es el grupo de los enteros $\{0, 1, ..., n-1\}$ con la suma módulo n.

Definición 1.13 *Una* **terna de diferencia** *módulo v es un conjunto de tres enteros $\{x, y, z\}$ los cuales, o bien $x + y + z$ es congruente con cero módulo v, o bien alguno de los enteros x, y o z es congruente con la suma de los otros dos módulo v. Una* **partición en diferencias** *de un conjunto $S \subseteq \mathbb{Z}_n$ es una descomposición de S en ternas de diferencias.*

Obsérvese que si $\{x, y, z\}$ es una terna de diferencias, podemos suponer que $\pm(x+y) \equiv z \bmod (v)$. Decimos que un STS($v$), asociado al par (X,Λ), está basado en $\mathbb{Z}_v$ si a cada elemento de X lo asociamos un elemento de $\mathbb{Z}_v$.

Definición 1.14 *Un sistema triple de Steiner de orden v que está basado en $\mathbb{Z}_v$ es* **cíclico** *si al sumar 1 a cada elemento de cualquier terna módulo v obtenemos otra terna del sistema triple de Steiner.*

En particular, los desarrollos de los bloques base de las familias de diferencias proporcionan sistemas triples de Steiner cíclicos. En lo que sigue denotaremos S_v al subconjunto $\{1, 2, ..., \frac{v-1}{2}\} \subset \mathbb{Z}_v$ y por $S'_v = S_v \setminus \{\frac{v}{3}\} \subset \mathbb{Z}_v$.

Lema 1.15 *[25] Si $v \equiv 1 \bmod (6)$, y existe una partición en diferencias de S_v, entonces existe un STS(v) que es cíclico. De manera análoga, si $v \equiv 3 \bmod (6)$, y existe una partición en diferencias de S'_v, entonces existe un STS(v) que es cíclico.*

Demostración: Sea $v \equiv 1 \bmod (6)$ y P una partición en diferencias de S_v. Sea $\{x, y, z\} \in P$ una terna de diferencias módulo v. Podemos suponer, sin pérdida de generalidad, que todas las ternas cumplen

$$z = \pm(x + y) \bmod (v).$$

Ahora vamos a construir una $(v, 3, 1)$-familia de diferencias (véase sección 1.4) y desde esta obtendremos un STS(v) cíclico. A estas ternas $\{x, y, z\}$ las asociamos las ternas $\{0, x, x + y\}$, y definimos

$$B = \{\{0, x, x + y\} : \{x, y, z\} \in P\}.$$

Entonces es claro que las ternas $\{j, x + j, t + j\}$, donde la suma es módulo v, $j \in \mathbb{Z}_v$ y $\{0, x, t\} \in B$ (con $t = z$ o $t = -z$), forman un STS(v), pues B es el conjunto de bloques base de una $(v, 3, 1)$-familia de diferencias, véase la sección 1.4. Es una $(v, 3, 1)$-familia de diferencias, pues obtenemos los $v - 1$ elementos no nulos de $\mathbb{Z}_v$ como diferencias de los elementos de las ternas.
Para el caso $v \equiv 3 \bmod (6)$, escribimos $v = 3k$, y con P partición en diferencias de S'_v, haciendo la construcción previa, con los bloques $\{j, k + j, 2k + j\}$, donde $j \in \mathbb{Z}_v$, volvemos a obtener una $(v, 3, 1)$-familia de diferencias y, por tanto, un STS(v).
En ambos casos, por la propia construcción es claro que obtenemos un STS(v) cíclico. ■

A continuación vamos a ver que no existe una partición en diferencias para S'_9; el conjunto S'_9 es igual a $S_9 \setminus \{3\} = \{1, 2, 4\}$. Como este conjunto es de tres elementos, y no cumple ninguna de las condiciones de las ternas de diferencias (definición 1.13), no es una partición en diferencias. Esto nos permite intuir que el sistema triple de Steiner de orden 9 no es cíclico. En efecto, si fuera

cíclico existiría una $(9, 3, 1)$-familia de diferencias con la que podríamos obtener los ocho elementos no nulos de $\mathbb{Z}_9$. Esa familia de diferencias estaría compuesta por dos bloques base, de los cuales uno sería de ciclo corto. Se puede comprobar que el único candidato a bloque base de ciclo corto es el $\{0, 3, 6\}$. Luego faltaría encontrar un bloque base de longitud 9. Si suponemos que el 0 está en dicho bloque base, se pueden realizar todas las comprobaciones y verificar que no existe ninguna combinación posible en la que obtengamos las seis posibles diferencias restantes. Por tanto, el STS(9) no es cíclico.

Ejemplo 11 *[25] Vamos a construir una partición en diferencias para* $v = 15$. *Partimos del conjunto* $S'_{15} = \{1, 2, 3, 4, 6, 7\}$. *Podemos imponer que la partición tenga en una de sus ternas al 1, pues cualquier elemento de* S'_{15} *debe estar en alguna terna de diferencias. Estas ternas pueden ser de la siguiente forma (pues deben cumplir la definición de ternas de diferencias):*

$$\{1, x, x+1\} \text{ o } \{1, x, 15-(x+1)\} \text{ o } \{1, x, 15+1-x\} \text{ con } x \in S'_{15}.$$

Como los elementos de estas ternas no pueden ser mayores que 7, la única posibilidad es que las ternas de diferencias sean de la forma $\{1, x, x+1\}$ *con* $x + 1 \leq 7$ *y como el 5 no pertenece a* S'_{15}, x *solo puede ser igual a* 2, 3 *o* 6 *(*$x = 4$ *no puede ser, pues sería* $x + 1 = 5$*). Los candidatos entonces son:*

$$\{\{1, 2, 3\}, \{4, 6, 7\}\}, \ \{\{1, 3, 4\}, \{2, 6, 7\}\}, \ \{\{1, 6, 7\}, \{2, 3, 4\}\}.$$

Obsérvese que en cada par, la primera terna es el resultado de sustituir x *por uno de los tres valores arriba mencionados, y el segundo par son los elementos restantes de* S'_{15}. *Haciendo una rápida inspección vemos que no todo par de ternas son diferencias triples pues en el primer par el segundo bloque no cumple ninguna de las propiedades exigidas y en el tercer par el segundo bloque tampoco. Luego, la partición en diferencias de* S'_{15} *es el par:*

$$\{\{1, 3, 4\}, \{2, 6, 7\}\}.$$

Finalmente, concluimos esta sección con dos resultados que dan una visión muy relacionada con la que obteníamos con las familias de diferencias de los sistemas triples de Steiner, pues todos, excepto el de orden 9, son cíclicos y podemos obtenerlos a partir de un conjunto de ternas de partida (ver proposición 1.11). De hecho, a partir de una partición en diferencias podemos obtener un $(v, 3, 1)$-familia de diferencias, véase lema 1.15.

Teorema 1.16 *Existen particiones en diferencias de* S_v *para todo* $v \equiv 1 \mod (6)$ *y existen particiones en diferencias de* S'_v *para todo* $v \equiv 3 \mod (6)$, *excepto para* $v = 9$.

Demostración: La demostración de este teorema se basa en una tabla, donde se almacenan todas las particiones de forma reiterada. Esta tabla puede encontrarse en [25, página 194], la cual se ha extraído íntegramente de [2]. ■

En la siguiente tabla se adjuntan algunas particiones en diferencia para valores pequeños de v.

$\mathbf{v = 7}$	$\{1, 2, 3\}$
$\mathbf{v = 15}$	$\{1, 3, 4\}$;$\{2, 6, 7\}$
$\mathbf{v = 19}$	$\{1, 5, 6\}$;$\{2, 8, 9\}$;$\{3, 4, 7\}$
$\mathbf{v = 27}$	$\{1, 12, 13\}$;$\{2, 5, 7\}$;$\{3, 8, 11\}$;$\{4, 6, 10\}$
$\mathbf{v = 45}$	$\{1, 11, 12\}$;$\{2, 17, 19\}$;$\{3, 20, 22\}$;$\{4, 10, 14\}$;$\{5, 8, 13\}$;$\{6, 18, 21\}$;$\{7, 9, 16\}$

El siguiente corolario es trivial haciendo suma de los resultados previos.

Corolario 1.17 *Existe un sistema triple de Steiner cíclico de todos los órdenes posibles, excepto de orden* 9.

1.6. Notas

Los sistemas triples de Steiner fueron planteados por primera vez por W.S.B. Woolhouse en 1844 como una pregunta en la revista *The Lady's and Gentleman's Diary*, una revista de matemáticas recreativas. El problema fue resuelto por Thomas Kirkman en 1847. En 1850 Kirkman planteó un nuevo problema, conocido como *el problema de las estudiantes de Kirkman*. Este problema decía así:

Quince alumnas se colocan en filas de tres durante siete días seguidos. Se requiere colocarlas cada día de manera que al terminar la semana no haya habido dos de ellas que hayan caminado juntas (es decir, en la misma fila) más de una vez.

Este problema exige una condición extra a los sistemas triple de Steiner, que sean **clases paralelas** (véase [9, capítulo 6, parte IV]). Daremos una solución a este problema más adelante. Un ejemplo de sistemas triples de Steiner con clases paralelas es el ejemplo 3. Sin tener conocimiento de los trabajos de Kirkman sobre este tema, Jakob Steiner en 1853 volvió a introducir estos sistemas triples, y como este trabajo fue más conocido, los sistemas triples de Steiner fueron nombrados así en su honor.

Capítulo 2

2-Diseños

2.1. Definición y primeras propiedades

En este capítulo generalizamos los conceptos de los sistemas triples de Steiner. Los bloques pueden tener más de 3 elementos y 2 elementos diferentes pueden coincidir en más de un bloque. Esta generalización da paso al concepto de **2-diseño**, cuya definición es la siguiente:

Definición 2.1 *[19] Sean v, k y λ enteros positivos tales que $v > k \geq 2$. Un* $\mathbf{2-(v,k,\lambda)}$ **diseño** *es un par (X,Λ), donde X es un conjunto con v elementos, o puntos, y Λ es una colección de subconjuntos de X llamados bloques, que cumplen las siguientes propiedades:*

1. *Cada bloque contiene exactamente k elementos, o puntos, de X.*
2. *Todo par de elementos distintos de X está contenido en exactamente λ bloques.*

Siempre que no sean relevantes v, k o λ, nos referiremos al par (X,Λ) como un 2-diseño. Esto es causa de que nos fijamos en 2 elementos distintos de X cuando nos preguntamos en cuántos bloques está este par. En la literatura inglesa se hace referencia a los 2-diseños bajo el nombre de 'BIBD', *balanced incomplete block designs*. La relación con los STS(v) es clara, pues un STS(v) es un 2-$(v, 3, 1)$ diseño (véase la definición 1.1). En adelante solo trataremos con *bloques simples* (bloques que están una única vez en el 2-diseño), aunque a efectos teóricos se permiten 2-diseños con bloques repetidos. A continuación, exponemos algunos ejemplos de 2-diseños.

Ejemplo 12 *[9] Un 2-*$(10, 4, 2)$ *diseño.*

$X = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ *y*
$\Lambda = \{\{0123\}, \{0145\}, \{0246\}, \{0378\}, \{0579\}, \{0689\}, \{1278\}, \{1369\}, \{1479\}, \{1568\},$
$\{2359\}, \{2489\}, \{2567\}, \{3458\}, \{3467\}\}$.

Obsérvese como seleccionando cualquier par de elementos de X (por ejemplo, el 6 y el 8) existen únicamente $\lambda = 2$ bloques de Λ que contienen a este par (el sexto y el décimo).

Ejemplo 13 *[9] El único 2-*$(11, 5, 2)$ *diseño. El conjunto de elementos es* $X = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a\}$ *y el conjunto de bloques es:*
$\Lambda = \{\{0, 1, 2, 3, 7\}, \{0, 1, 4, 5, 6\}, \{0, 2, 5, 8, 9\}, \{0, 3, 6, 8, a\}, \{0, 4, 7, 9, a\},$
$\{1, 2, 4, 8, a\}, \{1, 3, 5, 9, a\}, \{1, 6, 7, 8, 9\}, \{2, 3, 4, 6, 9\}, \{2, 5, 6, 7, a\}, \{3, 4, 5, 7, 8\}\}$.

Ahora, al igual que hicimos con los sistemas triples de Steiner, vamos a mostrar un par de proposiciones que nos van a dar una fórmula para el cálculo del número de bloques que tiene un 2-diseño y el número de veces que aparece un elemento en los bloques del 2-diseño.

Proposición 2.2 *[19] En un 2-(v, k, λ) diseño todo elemento está contenido en exactamente*

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

bloques.

Demostración: Tomemos un 2-(v, k, λ) diseño. Denotemos por X al conjunto de elementos y por Λ al conjunto de bloques del 2-diseño. Tomemos un elemento x de X y denotemos por r_x el número de bloques en los que aparece x. Definimos el siguiente conjunto:

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

Calcularemos el cardinal de $\mathbf{I}$ de dos formas distintas. Por un lado, puesto que $y \in \mathrm{X}$, $y \neq x$, tenemos $v-1$ posibles elecciones para y. Además, como estamos en un 2-(v, k, λ) diseño tenemos λ elecciones de $\mathrm{A} \in \Lambda$ tal que $\{x, y\} \subseteq \mathrm{A}$ (ver definición 2.1). Luego, tenemos que $|\mathbf{I}| = \lambda(v-1)$. Por otro lado, tenemos r_x posibles bloques $\mathrm{A} \in \Lambda$ en los que aparece x. Además, para cada bloque tenemos $k-1$ posibles elecciones de y, distinto de x. Luego $|\mathbf{I}| = r_x(k-1)$. En consecuencia, $r_x = \frac{\lambda(v-1)}{k-1}$. Como el resultado obtenido no depende de la elección que hemos hecho del elemento x, concluimos:

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

■

Al r previamente calculado se le asigna el nombre de *número de replicación.*

Proposición 2.3 *[19] Un 2-(v, k, λ) diseño tiene exactamente*

$$b = \frac{vr}{k} = \frac{\lambda v(v-1)}{k(k-1)} \tag{2.2}$$

bloques.

Demostración: Tomemos un 2-(v, k, λ) diseño cualquiera. Sea $b = |\Lambda|$. Consideramos el conjunto:

$$\mathbf{I} = \{(x,\mathrm{A}) : x \in \mathrm{X},\ x \in \mathrm{A},\ \mathrm{A} \in \Lambda\}$$

Como en la demostración previa, calcularemos $|\mathbf{I}|$ de dos formas diferentes. Por un lado, como estamos en un 2-(v, k, λ) diseño tenemos v formas posibles de seleccionar x y por la proposición previa sabemos que cada x aparece en r bloques distintos. Por tanto, $|\mathbf{I}| = vr$. Por otro lado, como cada bloque tiene k elementos tenemos que $|\mathbf{I}| = kb$. Concluimos

$$vr = kb \ \Rightarrow\ b = \frac{vr}{k} = \frac{v(v-1)}{k(k-1)}$$

■

Equivalente a la notación que hemos usado hasta ahora, usaremos 2-(v, b, r, k, λ) diseño si queremos tener presente el valor de los cinco parámetros. De manera obvia deducimos que no todos los 2-diseños existen, pues tanto r como b deben ser enteros. Luego, por el par de proposiciones previas obtenemos este teorema, que nos muestra dos condiciones para la existencia de un 2-(v, b, r, k, λ) diseño.

Teorema 2.4 *Si un 2-(v, b, r, k, λ) diseño existe, entonces $\lambda(v-1) \equiv 0$ mod $(k-1)$ y $\lambda v(v-1) \equiv 0$ mod $(k(k-1))$.*

Este teorema nos muestra que un 2-diseño que tenga por parámetros 2-$(22, 4, 1)$ no puede existir, pues $\lambda v(v-1) = 462 \not\equiv 0$ mod (12). Un uso más general del teorema previo es determinar qué condiciones necesarias pasan a ser suficientes para los 2-diseños con los valores de λ y k fijos. Esto no siempre es posible, pero en algunos casos sí, como con los sistemas triples de Steiner, véase teorema 1.5. En la siguiente tabla se recogen algunos 2-diseños en los que esto sucede. De forma más amplia y detallada podemos encontrar esta tabla en [9, capítulo 2, parte I].

k	λ	**Posibles valores de** v	**Excepciones**
3	1	1,3 mod 6	Ninguna
3	2	0,1 mod 3	Ninguna
3	6	Todos	Ninguna
4	1	1,4 mod 12	Ninguna
4	2	1 mod 3	Ninguna
4	6	Todos	Ninguna
5	1	1,5 mod 20	Ninguna
5	2	1,5 mod 10	15
5	4	0,1 mod 5	Ninguna
5	5	1 mod 4	Ninguna
5	10	1 mod 2	Ninguna
5	20	Todos	Ninguna

Algunas veces es conveniente representar los 2-diseños en forma matricial, pues así disponemos de las herramientas del álgebra lineal para trabajar con ellas. Para ello se hace uso de la *matriz de incidencia*.

Definición 2.5 *[13] Dado un 2-(v, b, r, k, λ) diseño con un par (X,Λ) asociado, donde X=$\{x_1, ..., x_v\}$ y $\Lambda = \{B_1, ..., B_b\}$. La* **matriz de incidencia**, *$M = (m_{i,j})$, del 2-diseño es una matriz $v \times b$ de ceros y unos, la cual viene definida por la regla siguiente:*

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

Es inmediato notar que la matriz de incidencia de un 2-(v, b, r, k, λ) diseño cumple las siguientes propiedades:

1. Todas las columnas tienen exactamente k unos.

2. Todas las filas tienen exactamente r unos.

3. Dos filas distintas tienen unos en común en λ columnas.

Ejemplo 14 *Consideremos un 2-$(10, 15, 6, 4, 2)$ diseño, como el del ejemplo 12. La matriz de incidencia de este 2-diseño es la siguiente matriz 10×15:*

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

Un ejemplo de aplicación de la matriz de incidencia puede verse en la demostración del siguiente teorema, conocido como *"inecuación de Fisher"* o *"teorema de Fisher"*, del cual podemos encontrar una prueba en [13] o en [19, capítulo 1].

Teorema 2.6 *Si existe un 2-(v, b, r, k, λ) diseño, entonces $b \geq v$.*

Como resultados equivalentes a este teorema, podemos concluir que en un 2-(v, b, r, k, λ) diseño tiene que cumplirse que $r \geq k$ y que $\lambda(v-1) \geq k^2 - k$, dándose la igualdad en los 2-diseños simétricos, los cuales trataremos en el siguiente capítulo.

2.2. Isomorfismos y Subdiseños

Comencemos con la definición de 2-diseños isomorfos.

Definición 2.7 *[19] Sean (X,Λ) y (Y,Γ) los pares asociados a un 2-(v, k, λ) diseño y a un 2-(w, g, γ) diseño, respectivamente, con $v = w$. Decimos que dos 2-diseños son* **isomorfos** *si existe una biyección α : X$\to$Y tal que*

$$\{\{\alpha(x) : x \in A\} : A \in \Lambda\} = \Gamma.$$

Es decir, si renombramos a los elementos $x \in$ X por $\alpha(x)$, entonces la colección de bloques de Λ se transforma en la colección de bloques de Γ. La biyección α se llama **isomorfismo**.

Como ejemplo de un isomorfismo podemos recordar el ejemplo 7. Es evidente, por definición, que si tenemos dos 2-diseños y un isomorfismo entre ellos, digamos α, y en uno de ellos tenemos c copias de cierto bloque A, entonces en el diseño isomorfo tendremos c copias del bloque $\{\alpha(x) : x \in A\}$. Este caso no lo trataremos. A continuación, exponemos un par de resultados sin demostración (las demostraciones pueden encontrarse en [19, capítulo 1]) basados en la matriz de incidencia, que nos van a permitir identificar cuándo dos 2-diseños son isomorfos.

Teorema 2.8 *Sean $M = (m_{i,j})$ y $N = (n_{i,j})$, ambas matrices de incidencia $v \times b$. Dos 2-diseños son isomorfos si y solo si existe una permutación γ en $\{1, ..., v\}$ y una permutación β en $\{1, ..., b\}$ tal que*

$$m_{i,j} = n_{\gamma(i),\beta(j)}$$

para todo $i \in \{1, 2, ..., v\}$ y todo para todo $j \in \{1, 2, ..., b\}$

El siguiente corolario, proporciona una caracterización alternativa de 2-diseños isomorfos. Para esto necesitamos introducir el siguiente concepto: una **matriz de permutaciones** es una matriz no singular (invertible) de ceros y unos tal que cada fila y cada columna contiene exactamente un 1.

Corolario 2.9 *Sean M y N dos matrices de incidencia de dos 2-(v, b, r, k, λ) diseños. Entonces estos 2-diseños son isomorfos si y solamente si existe una matriz de permutaciones de $v \times v$, digamos P, y una matriz de permutaciones de $b \times b$, digamos Q, tal que $M = PNQ$.*

En general, determinar si dos 2-diseños son no isomorfos es un problema computacional difícil (recuérdese que hay 1108487429 sistemas triples de Steiner no isomorfos de orden 19). Existen $v!$ posibles biyecciones que pueden ser isomorfismos entre dos conjuntos de cardinal v. Aún así, existen otro tipo de técnicas (tanto teóricas como computacionales) para determinar si dos 2-diseños son o no isomorfos. Para completar información sobre este tema puede consultarse [9, capítulo 9, parte VI], [11] o [19].

En la siguiente tabla mostramos el número de 2-diseños no isomorfos para un cierto conjunto de parámetros, [9, parte I].

$(\mathbf{v}, \mathbf{k}, \lambda)$	**No isomorfos**
$(6, 3, 2)$	1
$(7, 3, 2)$	4
$(7, 3, 3)$	10
$(8, 4, 3)$	4
$(9, 3, 2)$	36
$(9, 4, 3)$	11
$(10, 4, 2)$	3
$(16, 4, 1)$	1
$(19, 9, 4)$	6
$(25, 4, 1)$	16
$(10, 3, 2)$	960
$(13, 4, 2)$	2461

Concluimos esta sección definiendo los subdiseños y damos una propiedad relativa a estos. En la sección 1.3 se trataba este mismo tema para el caso específico de los sistemas triples de Steiner.

Definición 2.10 *[9] Decimos que el par (X,Λ) es un* **subdiseño** *de otro 2-diseño, (Y,Γ), si X$\subseteq$Y y $\Lambda \subseteq \Gamma$. Se dice que es* **propio** *si X$\subset$Y.*

Proposición 2.11 *[9] Si un 2-(v, k, λ) diseño tiene un subdiseño que es un 2-(w, k, λ) diseño propio, entonces $w \leqslant (v-1)/(k-1)$.*

2.3. Conjunto de Diferencias y Familia de Diferencias

En esta sección introducimos una generalización de la sección 1.4 del capítulo de los sistemas triples de Steiner. Empezaremos por el concepto más básico, el de *conjunto de diferencias* sobre grupos abelianos, y a partir de él introduciremos los conceptos de *conjuntos de diferencias consistentes en residuos cuadráticos* y *familias de diferencias*. Aunque en esta sección expongamos diversos ejemplos para mostrar la forma de trabajo del *método de diferencias*, en la siguiente sección añadiremos una mayor variedad de ejemplos de este tipo. A pesar de que en algunos casos los conjuntos y familias de diferencias responden a fórmulas y ecuaciones, pudiéndose construir a raíz de estas, muchos casos han sido encontrados a mano (véase [3], [4]).
La construcción con la que vamos a empezar ahora proporciona 2-diseños simétricos, los cuales abordaremos más detalladamente en el siguiente capítulo. Para esta primera parte nos hemos basado en [19, capítulo 3].

Definición 2.12 *Un 2-diseño con el mismo número de bloques que de elementos es un* **2-diseño simétrico**.

Si un 2-diseño es simétrico resulta claro lo siguiente:

$$v = b \Leftrightarrow k = r \Leftrightarrow vk(k-1) = \lambda v(v-1) \Leftrightarrow k(k-1) = \lambda(v-1) \tag{2.3}$$

Si un bloque no es simple (se repite más de una vez en el 2-diseño) utilizaremos esta notación para remarcarlo: [ ]. Los "conjuntos"que tienen varios elementos iguales los denominaremos **multiconjuntos**.

Definición 2.13 *Sea $(G,+)$ un grupo finito abeliano de orden v, en el cual el elemento identidad es denotado por 0. Dados k y λ enteros positivos tales que $2 \leq k < v$, un (v,k,λ)-***conjunto de diferencias** *en $(G,+)$ es un subconjunto de G, digamos $D \subset G$, que cumple las siguientes propiedades:*

1. $|D| = k$.
2. *El multiconjunto*

$$[x - y : x, y \in D, x \neq y]$$

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

El conjunto D es llamado **bloque base**.
*El (v,k,λ)-***conjunto de diferencias** *sobre $(G,+)$ se dice que es cíclico si el grupo G es cíclico.*

Ejemplo 15 *Un $(21,5,1)$-conjunto de diferencias sobre $(\mathbb{Z}_{21},+)$:*

$$D = \{0, 1, 6, 8, 18\}$$

Calculando las 20 posibles diferencias entre los pares de D (módulo 21) obtenemos todos los elementos no nulos de $\mathbb{Z}_{21}$.

$$\begin{array}{ll} 1-0=1 & 0-1=20 \\ 6-0=6 & 0-6=15 \\ 8-0=8 & 0-8=13 \\ 18-0=18 & 0-18=3 \\ 6-1=5 & 1-6=16 \\ 8-1=7 & 1-8=14 \\ 18-1=17 & 1-18=4 \\ 8-6=2 & 6-8=19 \\ 18-6=12 & 6-18=9 \\ 18-8=10 & 8-18=11. \end{array}$$

Ejemplo 16 *El conjunto $D = \{1, 3, 4, 5, 9\}$ es un $(11,5,2)$-conjunto de diferencias sobre $\mathbb{Z}_{11}$.*

Como sucedía con los sistemas triples de Steiner, con cada conjunto de diferencias podemos formar un 2-diseño. Para ello necesitamos la siguiente definición:

Definición 2.14 *Sea D el bloque base de un (v,k,λ)-conjunto de diferencias sobre un grupo abeliano $(G,+)$. Decimos que un bloque, B, es el* **trasladado** *del bloque base si $B = D + g$, con $g \in G$. Es decir*

$$B = \{b_1, b_2, ..., b_k\} = \{d_1 + g, d_2 + g, ..., d_k + g\} = D + g, \text{ donde } g \in G.$$

El conjunto de todos los bloques trasladados de D se denomina **desarrollo** *de D.*

Teorema 2.15 *Sea D un (v, k, λ)-conjunto de diferencias sobre un grupo abeliano $(G, +)$. Entonces, si $X = G$ y Λ es el desarrollo de D, el par (X,Λ) forma un 2-(v, v, k, k, λ) diseño simétrico.*

Demostración: Sean $x, y \in G$, $x \neq y$. Primero, probaremos que existen λ elementos $g \in G$ de forma que el par $\{x, y\} \subseteq D + g$. Denotemos $x - y = d$. Hay exactamente λ pares ordenados (x_i, y_i), donde $x_i, y_i \in D$ y donde $1 \leq i \leq \lambda$, tales que $x_i - y_i = d$. Recordemos que D es el bloque base de un (v, k, λ)-conjunto de diferencias. Entonces, para $1 \leq i \leq \lambda$ definimos $g_i = -x_i + x$. Luego $g_i = -y_i + y$, y por tanto $\{x, y\} \subseteq D + g_i$. Es decir,

$$\left\{ \begin{array}{l} x - y = d \\ x_i - y_i = d \end{array} \right\} \Rightarrow \left\{ \begin{array}{l} -x_i + x = g_i \\ -y_i + y = g_i \end{array} \right\} \Rightarrow \left\{ \begin{array}{l} x = x_i + g_i \\ y = y_i + g_i \end{array} \right\}$$

donde $\{x_i, y_i\} \subseteq D$ y $g_i \in G$ para $1 \leq i \leq \lambda$.
Puesto que los elementos x_i son distintos, tenemos que los elementos g_i son distintos, por lo tanto, tenemos exactamente λ valores de g tal que $\{x, y\} \subseteq D + g$. Como todos los bloques de Λ (el desarrollo de D) tienen k elementos y como $|G| = v$, tenemos que el par (X,Λ) forma un 2-(v, v, k, k, λ) diseño. ■

Por tanto, este teorema nos garantiza que a partir del desarrollo de los bloques base de los ejemplos 15 y 16, obtenemos un 2-$(21, 5, 1)$ diseño y un 2-$(11, 5, 2)$ diseño, respectivamente. Este par de 2-diseños son simétricos. En la sección siguiente mostramos un mayor número de ejemplos, mientras que en [9, capítulo 12, parte IV] encontramos una tabla con (v, k, λ)-conjuntos de diferencias para $k - \lambda \leq 30$.

Obsérvese que hasta ahora siempre hemos supuesto que el grupo sobre el que operábamos, $(G, +)$, es abeliano. En [9, capítulo 13, parte IV], en [16, capítulos 27 y 28] y en [8, capítulo 11] amplían esta teoría a grupos no abelianos.

Una forma de construir conjuntos de diferencias es mediante *conjuntos de diferencias consistentes en residuos cuadráticos*. Estos los consideramos en un cuerpo finito $\mathbb{F}_q$, donde $q = 4n - 1$ es una potencia de un primo. Consideramos el conjunto de los cuadrados no nulos de $\mathbb{F}_q$, denominado **conjunto de residuos cuadráticos**.

$$D = \{z^2 : z \in \mathbb{F}_q,\ z \neq 0\} \subset \mathbb{F}_q.$$

Mostramos a continuación un resultado que es necesario para nuestro propósito con los conjuntos de residuos cuadráticos.

Teorema 2.16 *Sea $\mathbb{F}_q$ un cuerpo finito, donde q es una potencia de un primo y es de la forma $q = 4n - 1$. Entonces, el elemento -1 no es un cuadrado en $\mathbb{F}_q$.*

Demostración: Razonemos por reducción al absurdo. Supongamos que existe un elemento α de $\mathbb{F}_q$ tal que $\alpha^2 = -1$. Es claro que $\alpha^4 = 1$ y por tanto el orden de α en $\mathbb{F}_q$ sería 4. Pero entonces, 4 tendría que ser un divisor de $q - 1 = 4n - 2$, lo cual es absurdo. ■

Ahora sí estamos en condiciones de enunciar el siguiente teorema, con el cual relacionamos los conjuntos residuales cuadráticos con los conjuntos de diferencias y, por tanto, con los 2-diseños.

Teorema 2.17 *[16] Sea $q = 4n - 1$ una potencia de un primo. El conjunto de residuos cuadráticos $D = \{z^2 : z \in \mathbb{F}_q,\ z \neq 0\}$ en $\mathbb{F}_q$ es un $(4n - 1, 2n - 1, n - 1)$-conjunto de diferencias sobre el grupo aditivo $\mathbb{F}_q$.*

Demostración: Claramente $|D| = \frac{q-1}{2} = \frac{4n-2}{2} = 2n-1$, pues si $a \in \mathbb{F}_q \backslash \{0\}$ entonces $a^2 = (-a)^2$. Luego el número de elementos por bloque es $2n-1$. Lo único que queda por comprobar es que cada elemento no nulo de $\mathbb{F}_q$ aparece $n-1$ veces como diferencia de dos elementos de D. Para ello calculamos todos los pares de diferencias del conjunto D,

$$\Delta D = [a^2 - b^2 : a^2, b^2 \in D,\ a^2 \neq b^2].$$

Supongamos que h es un elemento que aparece λ veces en ΔD, $h = a^2 - b^2$. Concluimos si comprobamos que λ es igual a $n-1$ para cualquier elemento no nulo de $\mathbb{F}_q$. Tomamos el elemento $\alpha^2 h$, basta darse cuenta que $\alpha^2 h = (\alpha a)^2 - (\alpha b)^2$, luego aparece el mismo número de veces que h, es decir, λ. Por lo tanto, los elementos que son cuadrados de $\mathbb{F}_q$ aparecen λ veces. Si h es un cuadrado, $-h$ no lo es (ver teorema previo). Obsérvese que entonces $-h$ es igual a $b^2 - a^2$, luego aparecen λ veces los elementos que no son cuadrados. Así tenemos un $(4n-1, 2n-1, \lambda)$-conjunto de diferencias. Se concluye con el valor de λ utilizando la fórmula (2.3), $\lambda = \frac{k(k-1)}{v-1} = n-1$. ■

Veamos un ejemplo de conjunto de residuos cuadráticos .

Ejemplo 17 *Consideramos el cuerpo $\mathbb{F}_q$, con $q = 11$, que es de la forma $4n-1$. Calculamos el conjunto de los residuos cuadráticos.*

$\mathbf{z}$	$\rightarrow$	$\mathbf{z^2\ mod(11)}$
1	$\rightarrow$	1
2	$\rightarrow$	4
3	$\rightarrow$	9
4	$\rightarrow$	5
5	$\rightarrow$	3
6	$\rightarrow$	4
7	$\rightarrow$	5
8	$\rightarrow$	9
9	$\rightarrow$	4
10	$\rightarrow$	1

Luego, $D = \{1, 3, 4, 5, 9\}$. Este conjunto, como acabamos de ver, forma un $(11, 5, 2)$-conjunto de diferencias y con el desarrollo de D, el cual podemos identificar como bloque base, obtenemos un 2-$(11, 11, 5, 5, 2)$ diseño.

Con esta construcción podemos obtener los siguientes 2-diseños:

q=4n-1	**(4n-1,2n-1,n-1)**
7	2-$(7, 3, 1)$ diseño
11	2-$(11, 5, 2)$ diseño
19	2-$(19, 9, 4)$ diseño
23	2-$(23, 11, 5)$ diseño
27	2-$(27, 13, 6)$ diseño
31	2-$(31, 15, 7)$ diseño

Con esta misma idea que acabamos de presentar, podemos formar otros tipos de conjuntos de diferencias. Estos los podemos encontrar más detalladamente en [8, capítulo 11] o en [9, capítulo 12, parte IV]. Recordemos que $\mathbb{F}_q$ representa el cuerpo finito, con q potencia de un primo.

1. $D_4 = \{z^4 : z \in \mathbb{F}_q \backslash \{0\}\}$, donde $q = 4n^2+1$, q primo y n impar. Obtenemos 2-$\left(q, n^2, \frac{n^2-1}{4}\right)$ diseño sobre el grupo aditivo $\mathbb{F}_q$.

2. $D_4 \cup \{0\}$, con $q = 4n^2+9$ y n impar. Obtenemos 2-$\left(q, n^2+3, \frac{n^2+3}{4}\right)$ diseño sobre el grupo aditivo $\mathbb{F}_q$.

Para terminar esta sección vamos a dar un concepto más amplio que el de conjunto de diferencias, *familia de diferencias*. Una vez más, las familias de diferencias de los sistemas triples de Steiner vuelven a ser un caso concreto de lo que a continuación exponemos.

Definición 2.18 *[19] Sea $(G,+)$ un grupo finito de orden v, en el cual el elemento identidad es denotado por 0. Sean k y λ enteros tal que $2 \leq k < v$. Una (v,k,λ)-***familia de diferencias** *en $(G,+)$ es una colección de subconjuntos de G, digamos $\{D_1, ..., D_L\}$, que cumple las siguientes propiedades:*

1. $|D_i| = k$ *para todo* i, $1 \leq i \leq L$.
2. *El multiconjunto unión*

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

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

Los conjuntos D_i son llamados **bloques base**.

Ejemplo 18 *Una (13,5,5)-familia de diferencias en $(\mathbb{Z}_{13}, +)$, con bloques base:*

$$\{\{0,1,2,4,8\}, \{0,1,3,6,12\}, \{0,2,5,6,10\}\}.$$

Las diferencias obtenidas en el primer bloque base son 1, 2, 4, 8, 12, 11, 9, 5, 1, 3, 7, 12, 10, 6, 2, 6, 11, 7, 4 y 9, del segundo bloque base 1, 3, 6, 12, 12, 10, 7, 1, 2, 5, 11, 11, 8, 2, 3, 9, 10, 4, 6 y 7 y del último bloque base son 2, 5, 6, 10, 11, 8, 7, 3, 3, 4, 8, 10, 9, 5, 1, 5, 12, 8, 4 y 9. Es una (13,5,5)-familia de diferencias porque hemos obtenido todos los elementos de $\mathbb{Z}_{13}$ no nulos cinco veces partiendo de bloques base de cinco elementos.

La relación entre las familias de diferencias y los 2-diseños resulta obvia después de haber tratado los conjuntos de diferencias y la familia de diferencias de los sistemas triples de Steiner. Hagamos notar que para relacionar los STS(v) con (v,k,λ)-familias de diferencias tenemos que hacer $k = 3$ y $\lambda = 1$, pues las ternas están compuestas por tres elementos y un elemento cualquiera aparece una única vez como diferencia de los elementos de los bloques base, véase definición 1.1.

Definición 2.19 *[9] Dado una (v,k,λ)-familia de diferencias sobre G, con bloques base $D_1, ...D_L$, se denomina el* **trasladado** *del bloque i a $D_i + g = \{b_1 + g, b_2 + g, ..., b_k + g\}$ donde $b_1, b_2, ..., b_k \in D_i$ y $g \in G$. El conjunto de todos los bloques trasladados se denomina* **desarrollo** *de la (v,k,λ)-familia de diferencias.*
Decimos que un bloques base D de una familia de diferencias sobre un grupo G es un **bloque de ciclo corto** *si su trasladado vuelve a ser el mismo para algún elemento no nulo de G, es decir, si $D + g = D$, con $g \in G \setminus \{0\}$.*
Decimos que la **longitud** *de un bloque base es igual al número de bloques distintos que podemos obtener del bloque base trasladado.*

La longitud de un bloque base es $|G|$, mientras que en los bloques de ciclo corto es estrictamente menor. De hecho, es un divisor del orden de G. La siguiente proposición es la generalización de la proposición 2.15.

Proposición 2.20 *[9] Si los bloques base $D_1, ...D_L$ forman una (v, k, λ)-familia de diferencias sobre G, entonces el desarrollo de la (v, k, λ)-familia de diferencias forman un 2-(v, k, λ) diseño.*

Demostración: Resulta claro por las definiciones previas que cualquier bloque trasladado tiene k elementos y como estamos operando dentro del grupo G, tendremos v elementos. Luego solo nos falta comprobar que para cualquier pareja de elementos distintos que seleccionemos de G, existen λ bloques del desarrollo en los que está la pareja. Sean $x \neq y \in G$. Como los bloques base $D_1, ...D_L$ forman una (v, k, λ)-familia de diferencias, $x - y \in G$ está en λ diferencias de los bloques base. Es decir, $x - y = h_i - h'_i$, con h_i y h'_i en λ bloques base. Entonces

$$\left\{ \begin{array}{l} x - y = d \\ h_i - h'_i = d \end{array} \right\} \Rightarrow \left\{ \begin{array}{l} -h_i + x = g_i \\ -h'_i + y = g_i \end{array} \right\} \Rightarrow \left\{ \begin{array}{l} x = h_i + g_i \\ y = h'_i + g_i \end{array} \right\}$$

donde $\{h_i, h'_i\}$ son elementos de algún bloque base y $g_i \in G$ para $1 \leq i \leq \lambda$.
■

Definición 2.21 *[9] Si el grupo G en el que está basada la (v, k, λ)-familia de diferencias es cíclico, entonces decimos que la familia de diferencias es* **cíclica** *y, por tanto, también es cíclico el 2-diseño.*

Ejemplo 19 *[9] Sea $G = \mathbb{Z}_{13}$. Asociado a este grupo una $(13, 4, 1)$-familia de diferencias, cuyo bloque base es:*

$$\{0, 1, 3, 9\}$$

Veamos como haciendo el trasladado de este bloque base obtenemos un 2-$(13, 4, 1)$ diseño.

$$\begin{array}{c} \{0, 1, 3, 9\} \\ \{1, 2, 4, 10\} \\ \{2, 3, 5, 11\} \\ \{3, 4, 6, 12\} \\ \{4, 5, 7, 0\} \\ \{5, 6, 8, 1\} \\ \{6, 7, 9, 2\} \\ \{7, 8, 10, 3\} \\ \{8, 9, 11, 4\} \\ \{9, 10, 12, 5\} \\ \{10, 11, 0, 6\} \\ \{11, 12, 1, 7\} \\ \{12, 0, 2, 8\} \end{array}$$

El lector puede comprobar como cualquier pareja de elementos distintos de $\mathbb{Z}_{13}$ están en un único bloque. En este caso, como la familia de diferencias está basada en $\mathbb{Z}_{13}$, es una familia de diferencias cíclica, luego podríamos reemplazar el bloque base por cualquiera de sus trasladados. Puesto que solo hay un bloque base, este ejemplo también nos muestra un $(13, 4, 1)$-conjunto de diferencias. Luego cualquier (v, k, λ)-conjunto de diferencias es una (v, k, λ)-familia de diferencias, pero no al revés, como muestra el siguiente ejemplo.

Ejemplo 20 *Sea $G = \mathbb{Z}_{13}$. Asociado a este una $(13, 5, 5)$-familia de diferencias, cuyos bloques base son:*

$$\{0, 1, 2, 4, 8\},\ \{0, 1, 3, 6, 12\},\ \{0, 2, 5, 6, 10\}$$

Ya comprobamos en el ejemplo 18 como todas las posibles diferencias de los bloques base nos proporcionaban cinco veces todos los elementos no nulos de $\mathbb{Z}_{13}$. *Veamos ahora como con sus trasladados obtenemos un 2-(*$13, 5, 5$*) diseño.*

$\{0,1,2,4,8\}$	$\{0,1,3,6,12\}$	$\{0,2,5,6,10\}$
$\{1,2,3,5,9\}$	$\{1,2,4,7,0\}$	$\{1,3,6,7,11\}$
$\{2,3,4,6,10\}$	$\{2,3,5,8,1\}$	$\{2,4,7,8,12\}$
$\{3,4,5,7,11\}$	$\{3,4,6,9,2\}$	$\{3,5,8,9,0\}$
$\{4,5,6,8,12\}$	$\{4,5,7,10,3\}$	$\{4,6,9,10,1\}$
$\{5,6,7,9,0\}$	$\{5,6,8,11,4\}$	$\{5,7,10,11,2\}$
$\{6,7,8,10,1\}$	$\{6,7,9,12,5\}$	$\{6,8,11,12,3\}$
$\{7,8,9,11,2\}$	$\{7,8,10,0,6\}$	$\{7,9,12,0,4\}$
$\{8,9,10,12,3\}$	$\{8,9,1,1,7\}$	$\{8,10,0,1,5\}$
$\{9,10,11,0,4\}$	$\{9,10,12,2,8\}$	$\{9,11,1,2,6\}$
$\{10,11,12,1,5\}$	$\{10,0,12,3,9\}$	$\{10,12,2,3,7\}$
$\{11,12,0,2,6\}$	$\{11,12,1,4,10\}$	$\{11,0,3,4,8\}$
$\{12,0,1,3,7\}$	$\{12,0,2,5,11\}$	$\{12,1,4,5,9\}$
$\{0,1,2,4,8\}$	$\{0,1,3,6,12\}$	$\{0,2,5,6,10\}$

El [9, capítulo 10, parte IV] es un capítulo entero dedicado a las familias de diferencias, en este capítulo se puede encontrar una amplia colección de (v, k, λ)-familia de diferencias con sus respectivos bloques base.

Por último, exponemos unos teoremas basados en familias de diferencias para construir 2-(v, k, λ) diseños. Ya hemos expuesto alguna construcción con estos métodos, véase sección 1.2 del capítulo de los sistemas triples de Steiner, construcción 3. Para estos teoremas hemos tomado como referencia [8, capítulo 15].

Teorema 2.22 *Sea* $v = 6t + 1 = p^n$*, con* p *primo. Sea* x *una raíz primitiva del cuerpo* $\mathbb{F}_v$*. Entonces los bloques*

$$\{x^0, x^{2t}, x^{4t}\}, \quad ..., \quad \{x^i, x^{2t+i}, x^{4t+i}\}, \quad ..., \quad \{x^{t-1}, x^{3t-1}, x^{5t-1}\}$$

forman una $(v, 3, 1)$*-familia de diferencias. Estos bloques base sobre el grupo* $\mathbb{Z}_v$ *y su desarrollo forman un 2-(*$6t + 1, 6t^2 + 1, 3t, 3, 1$*) diseño.*

La demostración de este primer teorema fue dada en la sección 1.4 del capítulo de los sistemas triples de Steiner.

Teorema 2.23 *Sea* $v = 12t + 1 = p^n$*, con* p *primo. Sea* x *una raíz primitiva del cuerpo* $\mathbb{F}_v$ *tal que* $x^{4t} - 1 = x^q$ *con* q *impar. Entonces los bloques*

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

forman una $(v, 4, 1)$*-familia de diferencias. Estos bloques base sobre el grupo* $\mathbb{Z}_v$ *y su desarrollo forman un 2-(*$12t + 1, t(12t + 1), 4t, 4, 1$*) diseño.*

El teorema previo puede aplicarse a números primos como $73, 97, 109, ...$ Pero no es válido para $37, 49, 61, ...$

2.4. Ejemplos

En esta sección mostramos algunos ejemplos concretos de 2-diseños que se pueden forman por el método de diferencias, expuesto en la sección anterior.

Ejemplo 21 *[19] Veamos un 2-*$(16, 6, 2)$ *diseño formado a partir de un* $(16, 6, 2)$*-conjunto de diferencias en* $(\mathbb{Z}_4 \times \mathbb{Z}_4, +)$*:*

$$D = \{(0,1), (0,2), (0,3), (1,0), (2,0), (3,0)\}$$

Tenemos 30 *posibles diferencias, más las* 2 *veces que aparece el* $(0,0)$ *hacen un total de* 32 *elementos, justamente son los* 16 *elementos que aparecen* $2 = \lambda$ *veces cada uno. Calculemos sus diferencias.*

$(0,1)$	$(0,3)$	$(0,1)$	$(0,3)$	$(1,1)$	$(3,3)$	$(1,0)$	$(3,0)$	$(1,0)$	$(3,0)$
$(0,2)$	$(0,2)$	$(1,2)$	$(3,2)$	$(2,1)$	$(2,3)$	$(2,0)$	$(2,0)$		
$(1,3)$	$(3,1)$	$(2,2)$	$(2,2)$	$(3,1)$	$(1,3)$				
$(2,3)$	$(2,1)$	$(3,2)$	$(1,3)$						
$(3,3)$	$(1,1)$								

Este ejemplo es particularmente interesante, pues no existe un $(16, 6, 2)$*-conjunto de diferencias sobre* $\mathbb{Z}_{16}$*.*

Ejemplo 22 *[14] Veamos un 2-*$(9, 4, 3)$ *diseño formado a partir de una* $(9, 4, 3)$*-familia de diferencias sobre el grupo* $\mathbb{Z}_9$*. En este caso los bloques bases son:*

$$B_1 = \{0, 1, 2, 4\} \qquad B_2 = \{0, 3, 4, 7\}$$

Como en el caso anterior las posibles diferencias son $9 \cdot 3 - 3 = 24$*. Estas las almacenamos a continuación:*

1	8	1	8	2	7	3	6	1	8	3	6
2	7	3	6			4	5	4	5		
4	5					7	2				

Otro par de ejemplos especialmente ilustrativos son los siguientes, los cuales son familias de diferencias y sus bloques bases son múltiplos entre sí. Esto quiere decir que, si tomamos todos los elementos de un bloque base y los multiplicamos por un elemento del grupo, obtenemos otro bloque base.

Ejemplo 23 *[14] Consideramos como grupo sobre el que se realizan las operaciones pertinentes* $G = \mathbb{Z}_5 \times \mathbb{Z}_5$*. Escribimos los elementos de dicho grupo así* xy*, en vez de así* (x, y)*, donde* $x, y \in \mathbb{Z}_5$*. Consideramos como bloques base:*

$$A = \{00, 01, 10, 22\},$$
$$B = \{00, 02, 20, 44\}.$$

Puede comprobarse que claramente se cumple que $2A = B$*. Estos bloques base junto con su desarrollo forman un 2-*$(25, 4, 1)$ *diseño. Escribimos a continuación las* 24 *diferencias.*

01	04	14	41	12	43	02	03	23	32	24	34
10	40	21	34			20	30	42	13		
22	33					44	11				

Ejemplo 24 *[14] Sean los bloques base* $B_1 = \{0, 1, 8\}$, $B_2 = \{0, 4, 13\}$ *y* $B_3 = \{0, 14, 16\}$. *Forman una* $(19, 3, 1)$*-familia de diferencias sobre* $\mathbb{Z}_{19}$. *Es decir, podemos formar un 2-*$(19, 3, 1)$ *diseño. Obsérvese que* $B_2 = 4B_1$ *y que* $B_3 = 4B_2$ *módulo* 19.

En la siguiente tabla quedan reflejados algunos de los 2-diseños que podemos formar con este método de diferencias basados en grupos cíclicos. En cada caso dicho grupo es $\mathbb{Z}_v$.

v	**b**	**r**	**k**	λ	**Bloques Base**
9	18	8	4	3	$\{1, 2, 3, 5\}; \{1, 2, 5, 7\}$
41	82	10	5	1	$\{1, 10, 16, 18, 37\}; \{5, 8, 9, 21, 39\}$
13	26	12	6	5	$\{1, 2, 4, 7, 8, 12\}; \{1, 2, 3, 4, 8, 12\}$
16	80	15	3	2	$\{1, 2, 4\}; \{1, 2, 8\}; \{1, 3, 13\}; \{1, 4, 9\}; \{1, 5, 10\}$
22	44	14	7	4	$\{1, 7, 12, 16, 19, 21, 22\}; \{1, 6, 8, 9, 10, 14, 20\}$

Por último, mostramos un ejemplo en el que se introduce el símbolo ∞. En esta última parte que sigue, tomamos como grupo G un grupo abeliano con $v-1$ elementos. Añadimos a G un nuevo elemento, ∞. Llamamos a este nuevo conjunto G'. La suma en G' se construye como la suma en G, añadiendo la regla adicional

$$\infty + \mathbf{g} = \infty \text{ para cada } \mathbf{g} \in G'.$$

Entonces, si B es un subconjunto de k elementos de G', el desarrollo generado por B consiste en los bloques

$$B + x : x \in G$$

Obsérvese que hemos escrito G y no G', pues $B + \infty$ sería un bloque con k copias de ∞. Por ejemplo, si G es $\mathbb{Z}_3$, el desarrollo del bloque $\{\infty, 0, 1\}$ es $\{\infty, 0, 1\}$, $\{\infty, 1, 2\}$ y $\{\infty, 2, 0\}$. Ahora bien, si queremos obtener un 2-diseño como desarrollo de un bloque base que tenga al ∞ debemos tener en cuenta lo siguiente: el ∞ aparece en los $v-1$ bloques del desarrollo del bloque en el que esté y no aparece nunca en el desarrollo de un bloque en el que no esté. Por otro lado, los otros elementos de G' aparecen en $v-1$ bloques o en v bloques, dependiendo si está el ∞ en el mismo bloque o no.

Ejemplo 25 *[25] Consideramos como bloques base los siguientes:*

$$\{\infty, 0, 1, 3, 7\},\ \{0, 1, 2, 4, 5\}$$

Como conjunto donde realizar las respectivas diferencias consideramos $G' = \mathbb{Z}_9 \cup \infty$. *Vamos a calcular todas las diferencias posibles.*

$\infty - 0 = \infty$ $0 - 1 = 8$ $1 - 0 = 1$ $1 - 3 = 7$ $3 - 1 = 2$ $3 - 7 = 5$ $7 - 3 = 4$
$\infty - 1 = \infty$ $0 - 3 = 6$ $3 - 0 = 3$ $1 - 7 = 3$ $7 - 1 = 6$
$\infty - 3 = \infty$ $0 - 7 = 2$ $7 - 0 = 7$
$\infty - 7 = \infty$

Obsérvese que solo hemos calculado las diferencias del infinito con este a la izquierda.

$0 - 1 = 8$ $1 - 0 = 1$ $1 - 2 = 8$ $2 - 1 = 1$ $2 - 4 = 7$ $4 - 2 = 2$ $4 - 5 = 8$ $5 - 4 = 1$
$0 - 2 = 7$ $2 - 0 = 2$ $1 - 4 = 6$ $4 - 1 = 3$ $2 - 5 = 6$ $5 - 2 = 3$
$0 - 4 = 5$ $4 - 0 = 4$ $1 - 5 = 5$ $5 - 1 = 4$
$0 - 5 = 4$ $5 - 0 = 5$

Ahora resulta claro, viendo todas las diferencias, que tenemos un 2-($10, 18, 9, 5, 4$) diseño, que procede de un concepto ligeramente más amplio que el de familia de diferencias. Simplemente hemos ampliado para poder operar con el símbolo ∞. Hemos construido un 2-($10, 18, 9, 5, 4$) diseño.

Terminamos esta sección mostrando una tabla con bloques base en los que aparece el ∞, véase [25]. Recordemos que el grupo sobre el que se basan es $G' = \mathbb{Z}_{v-1} \cup \{\infty\}$, es decir, las operaciones son módulo $v - 1$.

v	**b**	**r**	**k**	λ	**Bloques Base**
10	30	9	3	2	$\{\infty, 0, 5\}; \{0, 1, 4\}; \{0, 2, 3\}; \{0, 2, 7\}$
12	44	11	3	2	$\{\infty, 0, 3\}; \{0, 1, 3\}; \{0, 1, 5\}; \{0, 4, 6\}$
15	42	14	5	4	$\{\infty, 0, 1, 2, 7\}; \{0, 1, 4, 9, 11\}; \{0, 1, 4, 10, 12\}$

2.5. 2-Diseños Resolubles

Al igual que en la definición de 2-diseño simétrico se exigía una condición adicional sobre los 2-diseños, en esta sección nos centramos en los **2-diseños resolubles**.

Definición 2.24 *[9] Una* **clase paralela** *en un 2-diseño es un conjunto de bloques del 2-diseño que son una partición del conjunto de elementos.*
Un **2-diseño resoluble** *es un 2-(v, b, λ) diseño cuya familia de bloques admite una partición en clases paralelas. También lo escribiremos como 2-(v, b, λ) diseño resoluble.*

Ejemplo 26 *[9] Veamos el conjunto de bloques de un 2-($9, 3, 1$) diseño resoluble.*

$$\begin{array}{cccc} \{1,2,3\} & \{1,4,7\} & \{1,5,9\} & \{1,6,8\} \\ \{4,5,6\} & \{2,5,8\} & \{2,6,7\} & \{2,4,9\} \\ \{7,8,9\} & \{3,6,9\} & \{3,4,8\} & \{3,5,7\} \end{array}$$

Cada columna forma una clase paralela.

El siguiente teorema es similar al teorema 2.6, ahora específico a los 2-diseños resolubles, obteniendo así una condición necesaria para la existencia de 2-diseños resolubles.

Teorema 2.25 *[29] Si un 2-(v, k, λ) diseño resoluble existe, entonces $b \geq v + r - 1$.*

Esta demostración puede encontrarse en [19, capítulo 5]. Además, el teorema previo se cumple si y solo si $r \geq k + \lambda$. Obsérvese que el ejemplo anterior es un STS(9). De hecho, el origen de estos 2-diseños procede de la definición subsiguiente. Nótese que $k = 3$ y $\lambda = 1$.

Definición 2.26 *[29] Un* **sistema triple de Kirkman** *de orden v es un 2-($v, 3, 1$) diseño resoluble junto con sus bloques distribuidos en clases paralelas.*

Ejemplo 27 *[9] En 1850 Kirkman planteo la cuestión siguiente (véase sección 1.6):*

Quince alumnas se colocan en filas de tres durante siete días seguidos. Se requiere colocarlas cada día de manera que al terminar la semana no haya habido dos de ellas que hayan caminado juntas (es decir, en la misma fila) más de una vez.

Claramente, este problema es equivalente a encontrar un 2-($15, 3, 1$) diseño resoluble y dar la configuración de esa colocación. Es decir, es equivalente a dar un sistema triple de Steiner de orden 15 con sus bloques en clases paralelas. Ya sabemos que hay 80 STS(15) no isomorfos (sección 1.3) de los cuales hay solo cuatro que son resolubles. Mostramos un ejemplo de los cuatro posibles. Nótese que $b = 35 = 5 \cdot 7 = \frac{15 \cdot 14}{6}$. Consideramos como conjunto de elementos (las 15 alumnas) $\{a, b, c, ..., n, o\}$ y como bloques las filas de tres elementos.

Día 1	Día 2	Día 3	Día 4	Día 5	Día 6	Día 7
abc	*ahi*	*ajk*	*ade*	*afg*	*alm*	*ano*
djn	*beg*	*bmo*	*bln*	*bhj*	*bik*	*bdf*
ehm	*cmn*	*cef*	*cij*	*clo*	*cdg*	*chk*
fio	*dko*	*dhk*	*fkm*	*dim*	*ejo*	*eil*
gkl	*fjl*	*gin*	*gho*	*ekn*	*fhn*	*gjm*

Con el siguiente teorema finalizamos esta sección. Puede encontrarse la demostración del siguiente resultado en [25, capítulo 13].

Teorema 2.27 *Un sistema triple de Kirkman de orden v existe si y solo si $v \equiv 3$ mod(6).*

2.6. Construcciones

En esta sección vamos a dar algunos tipos de construcciones para la creación de 2-diseños. Aunque la creación de los 2-diseños puede basarse en multitud de ideas y áreas de las matemáticas, nosotros vamos a mostrar algunas de las más clásicas. Recordemos que $\mathbb{F}_q$, con q potencias de primo, es el cuerpo finito de q elementos y que $(\mathbb{Z}_p,+)$, con p primo, es el grupo finito módulo p.

2.6.1. Nuevos 2-diseños a partir de viejos

En esta parte vamos a mostrar como a partir de 2-diseños ya obtenidos previamente, o de los cuales conocemos su existencia, se pueden obtener nuevos 2-diseños. Empezamos con un método que se llama *método de la suma*, pues se basa en sumar (juntar) los bloques de dos 2-diseños dados previamente, con el mismo número de elementos y de bloques, en un nuevo 2-diseño. Obsérvese que los bloques del nuevo 2-diseño pueden repetirse.

Teorema 2.28 *[19] Si existe un 2-(v, k, λ_1) diseño y un 2-(v, k, λ_2) diseño, entonces existe un 2-$(v, k, \lambda_1 + \lambda_2)$ diseño.*

El número de elementos sigue siendo v, la longitud de cada bloque sigue siendo k y cada par de puntos distintos aparecen en $\lambda_1 + \lambda_2$ bloques. Claramente, si permitimos que los bloques se repitan, es decir, que no sean bloques simples, en el momento que tengamos un 2-(v, k, λ) diseño, podemos construir todos los 2-$(v, k, s\lambda)$ diseños, con $s \geq 1$.

Corolario 2.29 *Si existe un 2-(v, k, λ) diseño, entonces existe un 2-$(v, k, s\lambda)$ diseño, con $s \geq 1$.*

Ejemplo 28 *Para ilustrar un poco la aplicación de la construcción suma, vamos a considerar los 2-$(16, 6, \lambda)$ diseños. Como una consecuencia directa del teorema de Fisher (teorema 2.6), un 2-$(16, 6, 1)$ diseño no puede existir, pues sería $r = 3$ y en este caso no se cumpliría que r tiene que ser mayor o igual que $k = 6$. Por otro lado, sabemos que existe un 2-$(16, 6, 2)$ diseño y un 2-$(16, 6, 3)$ diseño, lo veremos más adelante. Por tanto, podemos concluir que los 2-$(16, 6, \lambda)$ diseños existen si y solo si $\lambda > 1$.*

La siguiente construcción se llama *2-diseño complementario* y, como anuncia su nombre, se basa en tomar el complementario de cada bloque respecto el conjunto total de elementos, es decir, si dado el conjunto (X,Λ), el cual es un 2-diseño, se reemplaza cada bloque $A \in \Lambda$ por X $\setminus A$, volvemos a obtener un 2-diseño, con distintos parámetros que el inicial.

Teorema 2.30 *[19] Si existe un 2-(v, b, r, k, λ) diseño, donde $k \leq v - 2$, entonces existe un 2-$(v, b, b - r, v - k, b - 2r + \lambda)$ diseño.*

Demostración: Supongamos que tenemos un par (X,Λ) que es un 2-(v, b, r, k, λ) diseño. Vamos a comprobar que el par

$$(\mathrm{X},\{\mathrm{X} \setminus A : A \in \Lambda\})$$

es un 2-$(v, b, b-r, v-k, b-2r+\lambda)$ diseño. Resulta obvio que este 2-diseño tiene v elementos y b bloques. Además, cada bloque contiene $v-k$ elementos (obsérvese que $v-k \geq 2$) y que el número de replicación es $b-r$. Por tanto, solo nos falta comprobar que cualquier par de elementos está en exactamente $b-2r+\lambda$ bloques. Sean $x, y \in X, x \neq y$. Definimos

$$\begin{aligned} a_1 &= \mid \{A \in \Lambda : x, y \in A\} \mid, \\ a_2 &= \mid \{A \in \Lambda : x \in A, y \notin A\} \mid, \\ a_3 &= \mid \{A \in \Lambda : x \notin A, y \in A\} \mid, \\ a_4 &= \mid \{A \in \Lambda : x, y \notin A\} \mid . \end{aligned}$$

Se comprueba fácilmente que

$$\begin{aligned} a_1 &= \lambda, \\ a_1 + a_2 &= r, \\ a_1 + a_3 &= r, \\ a_1 + a_2 + a_3 + a_4 &= b. \end{aligned}$$

Tenemos así lo siguiente:

$$a_1 = \lambda,\ a_2 = a_3 = r - \lambda,\ a_4 = b - 2r + \lambda.$$

Resulta obvio que dos elementos distintos que estaban en λ bloques de Λ ahora están en a_4 bloques. ■

El complementario de un 2-$(7, 3, 1)$ diseño es un 2-$(7, 4, 2)$ diseño, el de un 2-$(9, 3, 1)$ diseño es un 2-$(9, 6, 5)$ diseño y el de un 2-$(16, 6, 2)$ diseño es un 2-$(16, 10, 6)$ diseño.

Ejemplo 29 *[25] Dado un 2-($9, 12, 4, 3, 1$) diseño, a cuyo conjunto de bloques lo llamamos Λ, vamos a formar el diseño complementario, que es un 2-($9, 12, 8, 6, 5$) diseño, a cuyo conjunto de bloques lo llamamos Γ. En ambos casos, el conjunto de elementos es X $=\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$. La primera columna son los bloques del primer diseño y la segunda son los complementarios de dichos bloques.*

Bloques de Λ	**Bloques de Γ**
123	*456789*
456	*123789*
789	*123456*
147	*235689*
258	*134679*
369	*124578*
168	*234579*
249	*135678*
357	*124689*
159	*234678*
267	*134589*
348	*125679*

Definición 2.31 *[19] Dado un (X,Λ), un 2-(v, b, r, k, λ) diseño, llamamos 2-diseño dual del dado a un 2-diseño (Y,Γ) que cumple lo siguiente:*

$$|X| = |\Gamma| = v, \quad |Y| = |\Lambda| = b.$$

donde los puntos del 2-diseño (X,Λ) hacen las veces de bloques del 2-diseño (Y,Γ) y viceversa.

Obsérvese que no siempre el 2-diseño dual existe. Por ejemplo, dado un 2-$(3, 1, 1)$ diseño (ver ejemplo 1), su 2-diseño dual sería un 2-$(1, 3, 1)$ diseño, el cual resulta claro que no existe. De hecho, el 2-diseño dual solo existe cuando $b = v$, como mera consecuencia del teorema de Fisher (teorema 2.6). Si $b = v$ el 2-(v, b, r, k, λ) diseño es simétrico. Trataremos sobre ellos en el próximo capítulo. Sí existe el 2-diseño dual cumplirá las condiciones recogidas en el siguiente teorema.

Teorema 2.32 *Sea el par (X,Λ) un 2-(v, b, r, k, λ) diseño, y sea (Y,Γ) su 2-diseño dual. Entonces se cumple lo siguiente:*

1. *Todo bloque de Γ tiene longitud r.*
2. *Todo punto de Y está en exactamente k bloques de Γ.*
3. *Dos bloques distintos $B_i, B_j \in \Gamma$ tienen en común λ puntos.*

2.6.2. Construcciones basadas en la geometría afín

Tanto en esta parte como en la siguiente vamos a considerar geometrías finitas. Recordemos que por $\mathbb{F}_q$ entendemos el cuerpo finito de q elementos, con q potencia de primo. Las construcciones que vamos a exponer a continuación generalizan la construcción 2 del capítulo de los sistemas triples de Steiner. Estas construcciones se apoyan en los axiomas y en los resultados de las distintas geometrías finitas. Denotaremos el espacio afín de dimensión 2 (el plano afín) sobre el cuerpo finito $\mathbb{F}_q$ por $\mathbb{A}^2(\mathbb{F}_q)$ o por $AG(2, q)$. Análogamente, denotaremos el espacio afín de dimensión n sobre el cuerpo finito $\mathbb{F}_q$ por $\mathbb{A}^n(\mathbb{F}_q) = AG(n, q)$. Empezamos por el plano afín, donde consideramos los bloques como las rectas. A continuación, consideramos el espacio afín de dimensión 3 donde los bloques pueden ser rectas o planos. Generalizamos estas ideas para espacios de dimensión n y mostramos una construcción adicional también basada en la geometría afín finita.

Espacio afín de dimensión 2 sobre $\mathbb{F}_q$.

Teorema 2.33 *[25] Dado un plano afín $AG(2, q)$, con q potencia de primo, entonces existe un 2-($q^2, q^2 + q, q + 1, q, 1$) diseño.*

Demostración: Basta considerar como bloques las rectas de $\mathbb{F}_q^2$ y como conjunto de puntos los elementos de $AG(2, q)$, pues cada recta pasa por q puntos. Las rectas son de la siguiente forma:

$$\begin{cases} Y = aX + b \\ X = c \end{cases} \quad \text{con } a, b, c \in \mathbb{F}_q.$$

Luego, de la primera forma podemos formar q^2 rectas distintas y de la segunda q. El número de rectas es $q^2 + q$. Por último, notar que por dos puntos distintos únicamente pasa una recta y que por cada punto pasan $q + 1$ rectas, lo cual resulta evidente si nos fijamos en la forma de las rectas. Por tanto, tenemos un 2-$(q^2, q^2 + q, q + 1, q, 1)$ diseño. ■

Ejemplo 30 *Consideramos $\mathbb{A}^2(\mathbb{F}_2)$. Consideramos todas las posibles rectas como bloques:*

1. *x=0, con los puntos (0,0), (0,1).*
2. *x=1, con los puntos (1,0), (1,1).*
3. *x+y=0, con los puntos (0,0), (1,1).*
4. *x+y+1=0, con los puntos (1,0), (0,1).*
5. *y=0, con los puntos (0,0), (1,0).*
6. *y=1, con los puntos (0,1), (1,1).*

Luego, dado $AG(2,2)$*, podemos construir un 2-*$(4,6,3,2,1)$ *diseño, cuyos bloques son los siguientes:*

$$\{(0,0),(0,1)\},\quad \{(1,0),(1,1)\},\quad \{(0,0),(1,1)\},$$
$$\{(1,0),(0,1)\},\quad \{(0,0),(1,0)\},\quad \{(0,1),(1,1)\}.$$

En la siguiente tabla se muestran algunos de los 2-diseños que podemos crear a partir de $AG(2,q)$, con q potencia de primo.

$\mathbf{q}$	$\mathbf{2-(q^2, q^2+q, q+1, q, 1)}$ **diseño**
2	2-$(4,6,3,2,1)$ diseño
3	2-$(9,12,4,3,1)$ diseño
4	2-$(16,20,5,4,1)$ diseño
5	2-$(25,30,6,5,1)$ diseño
7	2-$(49,56,8,7,1)$ diseño
8	2-$(64,72,9,8,1)$ diseño
9	2-$(81,90,10,9,1)$ diseño
11	2-$(121,132,12,11,1)$ diseño

Obsérvese que en un 2-$(q^2, q^2+q, q+1, q, 1)$ diseño se cumple:

1. Tiene q^2 elementos.
2. Tiene q^2+q bloques de q elementos.
3. Un elemento está en $q+1$ bloques.
4. Dos bloques distintos coinciden en un único elemento.

Si identificamos los bloques como rectas y los elementos como puntos de $\mathbb{A}^2(\mathbb{F}_q)$, resulta claro el porque a los 2-diseños de esta forma se los llama **planos afines**.

Definición 2.34 *Un 2-*$(q^2, q^2+q, q+1, q, 1)$ *diseño se denomina* **plano afín** *de orden* q*.*

Espacio afín de dimensión 3 sobre $\mathbb{F}_q$.

Primero consideramos los bloques como rectas en $\mathbb{F}_q^3$, luego consideraremos los bloques como planos en $\mathbb{F}_q^3$. Obsérvese que podemos dividir $\mathbb{F}_q^3$ en q planos paralelos de q^2 puntos, entendiendo por planos los subespacios de dimensión 2 en $\mathbb{F}_q^2$ en $\mathbb{F}_q^3$. Es obvio que obtenemos 2-diseños distintos a partir de las distintas consideraciones.

Teorema 2.35 *Dado un espacio afín* $\mathbb{A}^3(\mathbb{F}_q)$*, con* q *potencia de primo, existe un 2-*$(q^3, q^2(q^2+q+1), q^2+q+1, q, 1)$ *diseño.*

Demostración: Razonemos como antes, considerando como bloques las rectas de $\mathbb{F}_q^3$. En esta ocasión el conjunto de puntos es $AG(3,q)$, luego tenemos $v = q^3$ elementos. Cada recta pasa por $k = q$ puntos y dos puntos distintos están en una única recta, luego $\lambda = 1$. Para calcular el número de rectas basta observar que estas vienen determinadas por 2 puntos. Fijémonos en un plano y en un punto que pertenezca al plano, tenemos q^2 elecciones de este punto. Para determinar el número de rectas vamos a hacer dos distinciones: si la recta está en el plano fijado o si no lo está. Basándonos en la parte previa, sabemos que hay $q^2 + q$ rectas en el mismo plano y como hay q planos paralelos en $\mathbb{F}_q^3$ tenemos $q(q^2+q)$. Por otro lado, un plano tiene q^2 puntos. Si la recta no está contenida en el plano seleccionado tiene con cada uno de los planos paralelos un punto en común y como viene determinada por dos puntos basta con fijar un punto de otro plano. Tenemos q^2q^2 rectas. En total $q(q^2+q)+q^2q^2 = q^2(q^2+q+1)$. Por último, para determinar el número de rectas que pasan por un punto solo tenemos que añadir las que no están en el mismo plano que hayamos fijado ($q+1$, ver teorema previo) y pasan por dicho punto, que son q^2. Por tanto, $r = q^2+q+1$. Hemos obtenido así un 2-$(q^3, q^2(q^2+q+1), q^2+q+1, q, 1)$ diseño. ■

Ahora consideramos como bloques los planos de $\mathbb{F}_q^3$.

Teorema 2.36 *Dado un espacio afín $\mathbb{A}^3(\mathbb{F}_q)$, con q potencia de primo, entonces existe un 2-$(q^3, q(q^2+q+1), q^2+q+1, q^2, q+1)$ diseño.*

Demostración: En este caso calculamos únicamente v, k y λ, el resto de parámetros podemos calcularlos utilizando las fórmulas (2.1) y (2.2). Como conjunto de puntos consideramos $\mathbb{A}^3(\mathbb{F}_q)$, luego $v = q^3$. Es claro que si consideramos los bloques como los planos de $\mathbb{F}_q^3$, cada bloque tiene $q^2 = k$ puntos. Por último, fijados dos puntos, veamos cuántos planos los contienen. Este problema es equivalente a calcular cuántos planos contienen a una cierta recta, pues esta viene determinada por el par de puntos previamente seleccionados. Ahora bien, obsérvese que un plano viene determinado por dos rectas distintas con un punto en común. Luego, el problema se reduce a calcular cuantas rectas de un plano pasan por un punto, el común entre las dos rectas. Esta cuestión la resolvimos en el teorema 2.33, $q+1$. Por tanto, hemos obtenido así un 2-$(q^3, q^2, q+1)$ diseño. ■

Espacio afín de dimensión n sobre $\mathbb{F}_q$.

De manera análoga podemos extender los resultados previos a espacios afines de dimensión mayor, considerando como bloques los subespacios de $\mathbb{F}_q^n$ de dimensión h, con $1 \leq h < n$ y obteniendo así una amplia diversidad de 2-diseños.

Teorema 2.37 *[25] Considerando como conjunto de puntos $AG(n,q)$ y como conjunto de bloques los subespacios de dimensión h, con $1 \leq h < n$, obtenemos el siguiente 2-diseño:*

$$2\text{-}\left(q^n, \frac{\lambda q^{n-h}(q^n-1)}{q^h-1}, \frac{\lambda(q^n-1)}{q^h-1}, q^h, \lambda\right) \text{diseño.}$$

donde

$$\lambda = \frac{q^{n-1}-1}{q-1}\frac{q^{n-2}-1}{q^2-1}\cdots\frac{q^{n-h+1}-1}{q^{h-1}-1}.$$

Obsérvese que como caso particular, si identificamos como elementos los puntos de $\mathbb{A}^n(\mathbb{F}_q)$ y como bloques las rectas de $\mathbb{F}_q^n$ ($h = 1$) obtenemos el siguiente 2-diseño:

$$2\text{-}\left(q^n, \frac{q^{n-1}(q^n-1)}{q-1}, \frac{q^n-1}{q-1}, q, 1\right) \text{ diseño.}$$

Otra construcción sobre $\mathbb{A}^2(\mathbb{F}_q)$.

Vamos a ver una construcción que está basada en el plano afín $\mathbb{A}^2(\mathbb{F}_q)$ debida a [24], un 2-$(q^2, 2q, 2q-1)$ diseño. En esta ocasión $q > 4$. Vamos a tomar como bloques las parejas de rectas paralelas distintas. Por tanto, el número elementos por bloque es $q + q = 2q$. Para el cálculo de λ vamos a fijarnos en dos puntos distintos. Solo tenemos una recta que pasa por los dos puntos y tenemos $q - 1$ elecciones de paralelas a esta recta. Recordemos que la forma de las rectas en el plano afín son así

$$\begin{cases} Y = aX + b \\ X = c \end{cases} \quad \text{con } a, b, c \in \mathbb{F}_q.$$

Por último, basta darse cuenta que si un punto está en una recta y el otro punto está en la otra recta, tenemos q posibles elecciones de estas rectas (direcciones de las rectas). En total $q-1+q = 2q-1$. Este 2-diseño nos permite construir 2-diseños como los siguientes. Recordemos que q tiene que ser mayor o igual que 5 y potencia de primo.

$\mathbf{q}$	$\mathbf{2-(q^2, 2q, 2q-1)}$ **diseño**
5	2-$(25, 10, 9)$ diseño
7	2-$(49, 14, 13)$ diseño
9	2-$(81, 18, 17)$ diseño
11	2-$(121, 22, 21)$ diseño

2.6.3. Construcciones basadas en la geometría proyectiva

Recordemos que por $\mathbb{F}_q$ entendemos el cuerpo finito de q elementos, con q potencia de primo. Estas construcciones se apoyan en los axiomas y en los resultados de la geometría finita proyectiva, los cuales pueden encontrarse en [8, capítulo 12]. Denotaremos el espacio proyectivo de dimensión 2 (el plano proyectivo) sobre el cuerpo finito $\mathbb{F}_q$ por $\mathbb{P}^2(\mathbb{F}_q)$ o por $PG(2, q)$. Análogamente, denotaremos el espacio proyectivo de dimensión n sobre el cuerpo finito $\mathbb{F}_q$ por $\mathbb{P}^n(\mathbb{F}_q) = PG(n, q)$. Empezaremos mostrando la relación de los 2-diseños con el plano proyectivo y a raíz de este, como en la sección anterior, vamos a generalizar estas ideas.

Definición 2.38 *[29] Un* **plano finito proyectivo** *es un conjunto finito de puntos y rectas los cuales cumplen:*

1. *Todo par de puntos está en una única recta.*
2. *Dos rectas cualquieras tienen en común un único punto.*
3. *Para cualquier conjunto de cuatro puntos, existen tres que pertenecen a la misma recta.*

Si cada recta tiene $m + 1$ puntos, se dice que el plano finito proyectivo es de orden m.

Un ejemplo de plano proyectivo conocido es el plano de Fano, el cual es un plano finito proyectivo de orden 2, véase el ejemplo 2.

Teorema 2.39 *[29] En cualquier plano proyectivo finito, el número de rectas que pasan por un punto es igual al número de puntos que hay en cada recta.*

Demostración: Sea un plano proyectivo finito. Tomamos cualquier recta, digamos L. Por la tercera condición de la definición de plano proyectivo, sabemos que existe un punto, x, que no se encuentran en L. Por la primera condición, para cada punto y en la recta L sabemos que existe

una recta que pasa por x y que contiene a y, digamos L_y. Supongamos que existe una recta L' que contiene a x y que no corta a ningún punto de L. Esto es una contradicción por la segunda condición de plano proyectivo. Por lo tanto, L' es una recta del tipo L_y. Entonces, L y las rectas que contienen a x forman una correspondencia uno a uno con los puntos de cualquier recta L. En otras palabras, el número de rectas a través de cada punto en un plano proyectivo finito es igual al número de puntos en cada recta. ■

Como consecuencia inmediata obtenemos este corolario.

Corolario 2.40 *[29] Un plano finito proyectivo con $m+1$ puntos en cada recta, tiene m^2+m+1 puntos y m^2+m+1 rectas.*

Demostración: Por el teorema previo, un plano proyectivo finito con $m+1$ puntos en cada recta tiene $m+1$ rectas a través de cada punto. Ahora, tomemos cualquier punto x. Existen $m+1$ rectas a través de x de forma que cada una de estas rectas tienen m puntos en ellas distintos de x. Contemos el número total de puntos. Multiplicando el número de rectas que contienen a x por el número de puntos en cada una de estas rectas sin contar a x y sumando a x una única vez obtenemos el total:

$$m(m+1)+1 = m^2+m+1$$

Este mismo argumento se puede hacer para contar el número total de rectas en un plano proyectivo finito. ■

Este último corolario es el que hace que los 2-diseños asociados a los planos proyectivos sean 2-diseños simétricos. De forma natural surge la siguiente definición que usaremos a lo largo del trabajo.

Definición 2.41 *Un 2-$(q^2+q+1, q+1, 1)$ diseño, con $q \geq 2$, se denomina* **plano proyectivo** *de orden q.*

Teorema 2.42 *[19] Para todo $q \geq 2$ potencia de primo, existe un 2-$(q^2+q+1, q+1, 1)$ diseño simétrico.*

La cuestión de la existencia de planos proyectivos de orden q, con q no potencia de primo, es uno de los problemas abiertos más importantes en la teoría de diseños combinatorios. Actualmente, se sabe que no existen planos proyectivos de órdenes 6 o 10, pero es un problema abierto la existencia de un plano proyectivo de orden 12. Este problema se puede resolver comprobando un número finito de configuraciones, pero este número de posibles configuraciones es más grande de lo que puede procesar la computación contemporánea. Un resultado relacionado con esta conjetura es el teorema de Bruck-Ryser.

Teorema 2.43 *[29] Si $q = 1$ o 2 mod (4) y q no es suma de dos cuadrados, entonces no existen planos proyectivos de orden q.*

Este teorema nos soluciona los casos cuando $q = 6, 14, 21, 22, ...$ Aun así queda una infinidad de valores, el primero de ellos el 12. Por último, damos una generalización a las ideas de construcciones de 2-diseños, como hicimos con la geometría afín, que consiste en tomar como bloques los hiperplanos (espacios de una dimensión menor que el espacio total) del espacio proyectivo $\mathbb{P}^d(\mathbb{F}_q)$.

Teorema 2.44 *[8] Sea $q \geq 2$ una potencia de un primo y sea $d \geq 2$ la dimensión del espacio total. Entonces existe un 2-diseño simétrico con los siguientes parámetros:*

$$2\text{-}\left(\frac{q^{d+1}-1}{q-1}, \frac{q^d-1}{q-1}, \frac{q^{d-1}-1}{q-1}\right) \text{ diseño.}$$

Esto es, todos los hiperplanos (dimensión $d-1$) del espacio proyectivo $\mathbb{P}^d(\mathbb{F}_q)$.

De manera similar podemos identificar como bloques los subespacios de dimensión menor. Es decir, si dado un espacio proyectivo de dimensión n, sobre un cuerpo $\mathbb{F}_q$, con q potencia de primo, identificamos como bloques los subespacios de dimensión s, con $s < n$, obtenemos un 2-diseño cuyos parámetros son los siguiente:

$$\begin{aligned}
v &= \frac{q^{n+1}-1}{q-1}, \\
b &= \frac{(q^{n+1}-1)(q^{n+1}-q)\cdots(q^{n+1}-q^s)}{(q^{s+1}-1)(q^{s+1}-q)\cdots(q^{s+1}-q^s)}, \\
r &= \frac{(q^{n+1}-q)(q^{n+1}-q^2)\cdots(q^{n+1}-q^s)}{(q^{s+1}-q)(q^{s+1}-q^2)\cdots(q^{s+1}-q^s)}, \\
k &= \frac{q^{s+1}-1}{q-1}, \\
\lambda &= \frac{(q^{n+1}-q^2)\cdots(q^{n+1}-q^s)}{(q^{s+1}-q^2)\cdots(q^{s+1}-q^s)}.
\end{aligned}$$

La demostración de los resultados previos se puede encontrar en [8].

2.6.4. Construcciones particulares

En esta parte mostramos ejemplos de las diversas formas que existen de construir 2-diseños. El primero de ellos hace uso de los denominados *cuadrados de Room*, que deben su nombre al matemático Thomas Gerald Room.

Definición 2.45 *[9] Sea S un conjunto de $n+1$ elementos (símbolos). Un* **cuadrado de Room** *de longitud n es una matriz $n \times n$, M, que cumple lo siguiente:*

1. *Todas las entradas de la matriz, o bien están vacías o bien contienen dos elementos distintos de S.*

2. *Cada símbolo de S está en cada fila y en cada columna de M una única vez.*

3. *Todo par de símbolos está en una única entrada de M.*

Definición 2.46 *[9] Si consideramos que $\infty \in S$, donde S es el conjunto de símbolos, un cuadrado de Room es* **estándar** *si en la entrada (i,i) está el par $\{\infty, i\}$.*
Un cuadrado de Room es **sesgado** *si de las entradas (i,j) y (j,i), con $i \neq j$, está una y solo una con un par de elementos de S.*

Teorema 2.47 *[9] Un cuadrado de Room sesgado de longitud n existe si y solo si n es impar mayor o igual que 7.*

Ejemplo 31 *[25] Consideremos $S = \{0,1,2,3,4,5,6,\infty\}$. Un cuadrado de Room estándar sesgado de longitud 7 puede ser el siguiente:*

$\infty, 0$			*1,5*		*4,6*	*2,3*
3,4	$\infty, 1$			*2,6*		*5,0*
6,1	*4,5*	$\infty, 2$			*3,0*	
	0,2	*5,6*	$\infty, 3$			*4,1*
5,2		*1,3*	*6,0*	$\infty, 4$		
	6,3		*2,4*	*0,1*	$\infty, 5$	
		0,4		*3,5*	*1,2*	$\infty, 6$

Obsérvese que si consideramos como bloques de longitud 2 cada entrada de dos símbolos de la matriz de este cuadrado de Room estándar sesgado y como conjunto de elementos S, obtenemos un 2-$(8, 2, 1)$ diseño.

Un posible método de construcción de este cuadrado de Room puede basarse en lo siguiente: a partir de la entrada (i, j), sumando 1 a cada miembro de dicha entrada módulo 7 y considerando que $\infty + 1 = \infty$ (por convenio) obtenemos la entrada $(i+1, j+1)$. Basta tomar como fila inicial la primera fila del cuadrado. Este método de construcción puede generalizarse bajo ciertas hipótesis. Para encontrar más información sobre este tema véase [25, capítulo 15]. Otro posible ejemplo de un cuadrado de Room estándar de longitud 7, y por tanto de un 2-$(8, 2, 1)$ diseño, es el que nos proporciona [22]:

$\infty, 0$		3,4	5,6			1,2
4,6	$\infty, 1$				0,2	3,5
	4,5	$\infty, 2$	0,1		3,6	
2,5	2,6		$\infty, 3$	1,5		0,4
1,3	0,3	1,6		$\infty, 4$		
			2,4	0,6	$\infty, 5$	
		0,5		2,3	1,4	$\infty, 6$

Con la misma idea que aquí se ha recogido para construir 2-diseños, podemos fijarnos en el teorema A.11 de cuadros latinos (véase apéndice A), y seleccionando correctamente ciertas casillas podremos obtener también 2-diseños.
Por último, mostramos un STS(15) que se ha obtenido por *orden lexicográfico*. Este consiste (como indica su nombre) en ir ordenando los elementos de cada terna en el orden natural. Basta con fijar el primer elemento del bloque, siendo este lo más pequeño posible, y poner el elemento siguiente lo más pequeño posible, siempre cumpliendo la definición de sistema triple de Steiner, es decir, que no coincidan dos elementos distintos más de una vez. Esto pone de manifiesto que, a pesar de que existen muchos métodos de construcción de 2-diseños que pueden resultar artificiales o laboriosos, también existen construcciones que son relativamente naturales y sencillas.

Ejemplo 32 *[30] Sea $X = \{1, 2, 3, ..., 15\}$. Consideramos el conjunto de ternas siguientes, formadas por orden lexicográfico, que forman un STS(15), o lo que es lo mismo, un 2-$(15, 3, 1)$ diseño.*

$1,2,3$	$2,13,15$	$5,9,12$
$1,4,5$	$3,4,7$	$5,10,15$
$1,6,7$	$3,5,6$	$5,11,14$
$1,8,9$	$3,8,11$	$6,8,14$
$1,10,11$	$3,9,10$	$6,9,15$
$1,12,13$	$3,12,15$	$6,10,12$
$1,14,15$	$3,13,14$	$6,11,13$
$2,4,6$	$4,8,12$	$7,8,15$
$2,5,7$	$4,9,13$	$7,9,14$
$2,8,10$	$4,10,14$	$7,10,13$
$2,9,11$	$4,11,15$	$7,11,12$
$2,12,14$	$5,8,13$	

Cerramos esta sección con un resultado relativo a la construcción por orden lexicográfico.

Proposición 2.48 *Dado un STS(v) construido por orden lexicográfico, se puede formar un STS($2v+1$) construido por orden lexicográfico.*

Puesto que el primer sistema triple de Steiner que se puede formar por orden lexicográfico es el de orden 3, podemos construir por este método el de orden $7, 15, 31, 63, ...$

Previo a la demostración mostramos un ejemplo concreto: pasamos del STS(7) al STS($2 \cdot 7 + 1$)=STS(15).

Ejemplo 33 *Sea el STS(7), donde $X = \{1,2,3,4,5,6,7\}$ y como conjunto de ternas*

$$\Lambda = \begin{array}{l} \{1,2,3\},\{1,4,5\},\{1,6,7\}, \\ \{2,4,6\},\{2,5,7\}, \\ \{3,4,7\},\{3,5,6\}. \end{array}$$

Obsérvese que sus ternas están formadas por orden lexicográfico. Ahora tenemos que añadir todas las posibles ternas que empiezan por 1. Como ya hemos usado los siete primeros elementos, nos falta por usar $15-7=8$, es decir, nos faltan cuatro ternas con el 1. Son las siguientes:

$$\{1,8,9\},\{1,10,11\},\{1,12,13\},\{1,14,15\}$$

Ahora tenemos todas las ternas en las que aparece el 1. Para las del 2 el razonamiento es igual, tenemos las dos ternas del STS(7) más la terna que sale con el 1, y como el número de replicación es siete (basta aplicar la fórmula (2.1)) tenemos que añadir $7-3=4$ bloques por orden lexicográfico. En cada bloque tenemos dos elementos distintos de los ocho que hemos añadido al conjunto de elementos. Las ternas son las siguientes:

$$\{2,8,10\},\{2,9,11\},\{2,12,14\},\{2,13,15\}$$

El razonamiento es totalmente análogo con el resto de elementos. Obsérvese que en ambos casos hemos añadido cuatro bloques con el mismo elemento de partida. En la siguiente tabla está el STS(15) que hemos construido, donde la primera columna son los bloques del STS(7) y los de la segunda son los bloques que hemos añadido.

$\{1,2,3\};\{1,4,5\};\{1,6,7\}$	$\{1,8,9\};\{1,10,11\};\{1,12,13\};\{1,14,15\}$
$\{2,4,6\};\{2,5,7\}$	$\{2,8,10\};\{2,9,11\};\{2,12,14\};\{2,13,15\}$
$\{3,4,7\};\{3,5,6\}$	$\{3,8,11\};\{3,9,10\};\{3,12,15\};\{3,13,14\}$
	$\{4,8,12\};\{4,9,13\};\{4,10,14\};\{4,11,15\}$
	$\{5,8,13\};\{5,9,12\};\{5,10,15\};\{5,11,14\}$
	$\{6,8,14\};\{6,9,15\};\{6,10,12\};\{6,11,13\}$
	$\{7,8,15\};\{7,9,14\};\{7,10,13\};\{7,11,12\}$

Demostración: Dado un STS(v) construido por orden lexicográfico vamos a construir un STS($2v+1$) (que sabemos que existe) también por orden lexicográfico. Haciendo uso de la fórmula (2.2) sabemos que el STS(v) tiene $\frac{v(v-1)}{6}$ bloques y que el STS($2v+1$) tiene $\frac{(2v+1)2v}{6} = \frac{v(2v+1)}{3}$. Es decir, tenemos que añadir

$$\frac{v(2v+1)}{3} - \frac{v(v-1)}{6} = \frac{v}{3}\left(2v+1-\frac{v-1}{2}\right) = \frac{v(v+1)}{2}$$

bloques nuevos. Ahora, añadimos $\frac{v+1}{2}$ bloques que empiezan por 1 a los que teníamos del STS(v), pues el número de replicación del STS($2v+1$) es (usando la fórmula (2.1)) $\frac{2v+1-1}{2} = v$ y como hemos usado los bloques del STS(v), la diferencia es

$$v - \frac{v-1}{2} = \frac{2v-v+1}{2} = \frac{v+1}{2}.$$

Añadimos $\frac{v+1}{2}$ bloques que empiezan por 2 por la misma razón que antes, pues el 2 está en un bloque con el 1 por construcción. Añadimos $\frac{v+1}{2}$ bloques que empiezan por 3 y así hasta añadir $\frac{v+1}{2}$ bloques que empiezan por v. Obsérvese que hemos añadido $\frac{v+1}{2}$ bloques v veces. En total, hemos añadido $\frac{v(v+1)}{2}$, justo el número de bloques necesarios para formar el STS($2v+1$). Estos nuevos bloques pueden ser construidos por orden lexicográfico porque son todas las posibles combinaciones de $v+1$ elementos en pares, es decir, $\binom{v+1}{2} = \frac{v(v+1)}{2}$. ■

Capítulo 3

2-Diseños Simétricos

3.1. Definición y propiedades

En este capítulo nos centramos en los 2-diseños simétricos. Ya hemos introducido este término previamente (ver definición 2.12) y ahora profundizamos más en él, mostrando propiedades y construcciones relativas a 2-diseños simétricos.

Definición 3.1 *Un 2-diseño con el mismo número de bloques que de elementos es un* **2-diseño simétrico**.

Ahora vamos a mostrar algunos enunciados equivalentes a la definición previa.

Proposición 3.2 *[19] Sea el par (X,Λ), el cual es un 2-(v, b, r, k, λ) diseño. Son equivalentes los siguientes enunciados:*

1. *El 2-(v, b, r, k, λ) diseño es simétrico, es decir, $b = v$.*
2. $\lambda(v-1) = k^2 - k$.
3. $r = k$.

Omitimos la demostración de esta proposición, pues basta ir sustituyendo los valores correspondientes (v, b y r) en las ecuaciones (2.2) y (2.1) para ir obteniendo la igualdad esperada. A partir de ahora, también nos referiremos a un 2-diseño simétrico por un 2-(v, v, k, k, λ) diseño.

Ejemplo 34 *[19] Consideremos el par (X,Λ), donde $|X| = v$ y Λ es el conjunto de todos los subconjuntos de k elementos de X. Hemos obtenido así un 2-$\left(v, k, \binom{v-2}{k-2}\right)$ diseño. Utilizando las fórmulas (2.2) y (2.1) obtenemos*

$$b = \frac{\frac{(v-2)!}{(k-2)!(v-k)!}v(v-1)}{k(k-1)} = \binom{v}{k},$$

$$r = \frac{\frac{(v-2)!}{(v-2-k+2)!(k-2)!}(v-1)}{k-1} = \frac{(v-1)!}{(k-1)!(v-k)!} = \binom{v-1}{k-1}.$$

Es decir, un 2-$\left(v, \binom{v}{k}, \binom{v-1}{k-1}, k, \binom{v-2}{k-2}\right)$ diseño. Si ahora tomamos $v = k+1$, formamos un 2-$(v, v, v-1, v-1, v-2)$ diseño, que proporciona una familia infinita de 2-diseños simétricos. Por ejemplo, el 2-$(4, 4, 3, 3, 2)$ diseño es de la siguiente forma:

$$X = \{1, 2, 3, 4\},$$
$$\Lambda = \{123, 124, 134, 234\}.$$

Obsérvese que el par previo tiene el mismo número de elementos que de bloques.

El siguiente teorema nos va a permitir realizar algunas construcciones de 2-diseños a partir de 2-diseños simétricos obtenidos previamente.

Teorema 3.3 *[19] Sea (X,Λ) un 2-(v, k, λ) diseño simétrico, donde $\Lambda = \{A_1, ..., A_v\}$. Entonces $\mid A_i \cap A_j \mid = \lambda$, para $1 \leq i < j \leq v$.*

La demostración de este teorema se puede encontrar en [19, capítulo 2]. Como consecuencia de este teorema podemos obtener el siguiente corolario. Recordemos previamente la definición de 2-diseño dual a un 2-diseño dado y la matriz de incidencia de un 2-diseño, conceptos en los que nos apoyamos para demostrar el recíproco del teorema previo.

Definición 3.4 *[19] Dado un (X,Λ), un 2-(v, b, r, k, λ) diseño, llamamos 2-diseño dual del dado a un 2-diseño (Y,Γ) que cumple lo siguiente:*

$$|X| = |\Gamma| = v, \quad |Y| = |\Lambda| = b.$$

donde los puntos del 2-diseño (X,Λ) hacen las veces de bloques del 2-diseño (Y,Γ) y viceversa.

Definición 3.5 *[13] Dado un 2-(v, b, r, k, λ) diseño con el par (X,Λ) asociado, donde X=$\{x_1, ..., x_v\}$ y $\Lambda = \{B_1, ..., B_b\}$. La* **matriz de incidencia**, *$M = (m_{i,j})$, del 2-diseño es una matriz $v \times b$ de ceros y unos, la cual viene definida por la siguiente regla:*

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

Corolario 3.6 *[19] Sean un 2-diseño y su correspondiente matriz de incidencia M. Entonces, si existe el 2-diseño dual del dado, su matriz de incidencia es M^T.*

Este corolario muestra que el dual de un 2-diseño simétrico vuelve a ser un 2-diseño simétrico. La demostración es obvia a partir de las propiedades del 2-diseño dual (teorema 2.32) y de las de la matriz de incidencia.

Corolario 3.7 *[19] Sean μ un entero positivo y (X,Λ) un 2-(v, b, r, k, λ) diseño tal que $\mid A \cap A' \mid = \mu$ para todo $A, A' \in \Lambda$. Entonces el par (X,Λ) es un 2-diseño simétrico y $\mu = \lambda$.*

Demostración: Vimos en el teorema 2.32 las propiedades del 2-diseño dual, el cual nos asegura que el dual del 2-(v, b, r, k, λ) diseño (si existe) es un 2-(b, v, k, r, μ) diseño. Aplicando el teorema de Fisher (teorema 2.6) al par (X,Λ) y al 2-(b, v, k, r, μ) diseño obtenemos que $b \geq v$ y que $v \geq b$. Luego $v = b$ y por tanto, aplicando el teorema 3.3 obtenemos que $\mu = \lambda$. ■

Juntando este corolario previo con el teorema 3.3 obtenemos la siguiente propiedad, exclusiva de los 2-diseños simétricos.

Teorema 3.8 *Sea (X,Λ) un 2-(v, b, r, k, λ) diseño. Entonces, el 2-diseño es simétrico si y solo si para todo par de bloques distintos $A, A' \in \Lambda$ se cumple $\mid A \cap A' \mid = \mu$, donde μ es un entero positivo.*

Nótese que entonces $\mu = \lambda$.

Ejemplo 35 *Sea el 2-$(7, 7, 3, 3, 1)$ diseño. Tenemos lo siguiente:*

$$X = \{1, 2, 3, 4, 5, 6, 7\},$$
$$\Lambda = \{125, 136, 147, 237, 246, 345, 567\}$$

Obsérvese como dos bloques cualesquiera tienen $1 = \lambda$ *elemento en común.*

En la siguiente tabla (que puede encontrarse con un mayor número de valores en [9]) recogemos algunos 2-diseños simétricos.

$(\mathbf{v}, \mathbf{b}, \mathbf{r}, \mathbf{k}, \lambda)$
$(16, 16, 6, 6, 3)$
$(25, 25, 9, 9, 3)$
$(31, 31, 10, 10, 3)$
$(71, 71, 15, 15, 3)$
$(49, 49, 16, 16, 5)$
$(41, 41, 16, 16, 6)$

Existe una conjetura sobre los 2-(v, b, r, k, λ) diseños simétricos. Dice lo siguiente:

Fijado $\lambda > 1$*, existe solo un número finito de 2-diseños simétricos con dicho* λ*.*

Obsérvese que la conjetura es para $\lambda > 1$, pues 2-diseños simétricos con $\lambda = 1$ ya hemos visto que existen infinitos, los planos proyectivos son 2-$(q^2+q+1, q+1, 1)$ diseños con q potencia de primo. Valores conocidos de k para $\lambda = 2$ son $2, 3, 4, 5, 6, 9, 11$ y 13. Estos 2-diseños son conocidos como *biplanos*. Trataremos sobre ellos más adelante. Valores conocidos de k para $\lambda = 3$ son $4, 6, 9, 10, 12$ y 15.

3.2. Construcciones

Para los dos siguientes métodos de construcción se necesita que el 2-(v, k, λ) diseño del que partimos sea un 2-diseño simétrico (ver definición 3.1), esto es equivalente a que dos bloques cualesquiera del 2-diseño tengan λ puntos en común (teorema 3.3). Los 2-diseños creados a partir de estas construcciones se denominan *2-diseño derivado* y *2-diseño residual*. En el primero fijamos un bloque como conjunto de elementos, siendo la intersección de este con los demás bloques el nuevo conjunto de bloques. Para formar el 2-diseño residual fijamos un bloque. Los elementos del nuevo conjunto son todos los elementos que no estén en el bloque seleccionado. Para formar el conjunto de bloques basta hacer lo mismo con cada bloque.

Definición 3.9 *[19] Sean* (X,Λ) *un 2-*(v, k, λ) *diseño simétrico y* $A_0 \in \Lambda$*. Definimos*

$$Der(X, \Lambda, A_0) = (A_0, \{A \cap A_0 : A \in \Lambda, A \neq A_0\})$$

y definimos

$$Res(X, \Lambda, A_0) = (X \setminus A_0, \{A \setminus A_0 : A \in \Lambda, A \neq A_0\}).$$

A $Der(X, \Lambda, A_0)$ *lo llamamos* **2-diseño derivado** *y a* $Res(X, \Lambda, A_0)$ *lo llamamos* **2-diseño residual**.

Puesto que todos los bloques tienen un mismo número de elementos en común, ningún bloque se comporta de forma distinta respecto al resto. Esto es lo que permite enunciar el siguiente teorema.

Teorema 3.10 *[16] Sean el par* (X,Λ) *un 2-*(v, v, k, k, λ) *diseño simétrico y un bloque* $B \in \Lambda$*, entonces el 2-diseño derivado,* $Der(X, \Lambda, B)$*, es un 2-*$(k, v-1, k-1, \lambda, \lambda-1)$ *diseño, si* $\lambda \geq 2$*. El 2-diseño residual,* $Res(X, \Lambda, B)$*, es un 2-*$(v-k, v-1, k, k-\lambda, \lambda)$ *diseño, si* $k \geq \lambda + 2$*.*

Demostración: Claramente, por definición, el 2-diseño derivado y el 2-diseño residual son 2-diseños con los parámetros previamente descritos. Lo único que hay que comprobar para el caso del 2-diseño derivado es que $k > \lambda$ (ver definición 2.1). En cualquier 2-diseño simétrico se cumple que $\lambda(v-1) = k(k-1)$ (proposición 3.2) y como $v > k$ tenemos la desigualdad buscada. Para el caso del 2-diseño residual, tenemos que probar que $v - k > k - \lambda$ (ver definición 2.1). Probaremos que esta desigualdad es cierta en los 2-diseños simétricos. Razonemos por reducción al absurdo. Supongamos que $v \leq 2k - \lambda$. Tendríamos entonces que $k(k-1) = \lambda(v-1) \leq \lambda(2k - \lambda - 1)$. Esto equivaldría a $(k-\lambda)(k-\lambda-1) \leq 0$. Pero esto es absurdo, pues k y λ son enteros positivos y para que se cumpla esta desigualdad tendría que darse que, o bien $k \leq \lambda$ o bien $k \leq \lambda + 1$, pero habíamos supuesto que en el 2-diseño residual se cumplía $k \geq \lambda + 2$. Por tanto, se verifica $v - k > k - \lambda$. ■

Ejemplo 36 *[25] En la siguiente tabla se muestra un 2-*$(11, 11, 6, 6, 3)$*) diseño simétrico. La primera columna corresponde a los bloques del 2-*$(11, 6, 3)$*) diseño, la segunda muestra los bloques del 2-diseño residual, con parámetros 2-(5,10,6,3,3), y la tercera columna muestra los bloques del 2-diseño derivado, con parámetros 2-(6,10,5,3,2). Tomamos como bloque de partida el* $\{1, 2, 3, 4, 5, 6\}$.

2-(11,11,6,6,3) diseño	**2-(5,10,6,3,3) diseño**	**2-(6,10,5,3,2) diseño**
1,2,3,4,5,6	*Diseño Residual*	*Diseño Derivado*
2,5,6,7,10,11	*7,10,11*	*2,5,6*
1,4,6,7,8,10	*7,8,10*	*1,4,6*
2,4,5,7,8,9	*7,8,9*	*2,4,5*
3,5,6,8,9,10	*8,9,10*	*3,5,6*
3,4,6,7,9,11	*7,9,11*	*3,4,6*
1,3,5,7,8,11	*7,8,11*	*1,3,5*
1,2,6,8,9,11	*8,9,11*	*1,2,6*
1,2,3,7,9,10	*7,9,10*	*1,2,3*
2,3,4,8,10,11	*8,10,11*	*2,3,4*
1,4,5,9,10,11	*9,10,11*	*1,4,5*

Como consecuencia directa del teorema 2.42, que nos justifica la existencia del plano proyectivo finito para toda potencia de primo $q \geq 2$, si tomamos el 2-diseño residual de un plano proyectivo, el correspondiente 2-diseño es un plano afín, ver definiciones 2.34 y 2.41.

Teorema 3.11 *Para toda potencia de primo* $q \geq 2$*, existe un 2-*$(q^2, q, 1)$*) diseño (es decir, un plano afín de orden* q*).*

Plano Proyectivo **Plano Afín**

$\mathbf{q}$	$\mathbf{q^2+q+1}$	$\mathbf{q+1}$
2	7	3
3	13	4
4	21	5
5	31	6
7	57	8

$\longrightarrow$

$\mathbf{q}$	$\mathbf{q^2}$	$\mathbf{q}$
2	4	2
3	9	3
4	16	4
5	25	5
7	49	7

Es decir, si tenemos un plano proyectivo de orden q, tenemos un 2-$(q^2+q+1, q+1, 1)$ diseño, y al calcular el 2-diseño residual de este obtenemos un 2-$(q^2, q, 1)$ diseño, un plano afín de orden q. Por ejemplo, si $q = 4$ tenemos un 2-$(21, 5, 1)$ diseño y al hacer el 2-diseño residual obtenemos un 2-$(16, 4, 1)$ diseño. Obviamente, un plano proyectivo menos una recta (la recta del infinito) es un

plano afín, que es lo que hacemos al pasar de un 2-diseño simétrico a su 2-diseño residual.

De forma totalmente análoga, escribimos los siguientes 2-diseños basados en la geometría finita proyectiva (sección 2.6.3) y sus correspondientes 2-diseños residuales, basados en la geometría finita afín (sección 2.6.2). Recordemos que $q \geq 2$ y $d \geq 2$. El 2-diseño basado en la geometría finita proyectiva consiste en identificar los bloques como los hiperplanos (subespacios de una dimensión menor que el espacio total) del espacio proyectivo, de dimensión d. Obsérvese que se puede hacer el 2-diseño residual porque partimos de un 2-diseño simétrico.

Proyectivo		**Afín**	
$2-\left(\frac{q^{d+1}-1}{q-1}, \frac{q^d-1}{q-1}, \frac{q^{d-1}-1}{q-1}\right)$	$\longrightarrow$	$2-\left(q^d, q^{d-1}, \frac{q^{d-1}-1}{q-1}\right)$	con $d \geq 2$.

Como acabamos de ver, hay una infinidad de 2-diseños simétricos con $\lambda = 1$. A continuación mostramos algunos ejemplos en los que λ es mayor que uno. Recordemos que actualmente se cree que solo existe un número finito de 2-(v, k, λ) diseños simétricos, con $\lambda > 1$ fijado.

Ejemplo 37 *[16] Consideramos un cuadro latino L de orden 6 (véase apéndice A). Para nombrar al elemento que está en la posición (i, j) del cuadro latino L lo denotamos por $L(i, j)$. Definimos $C = \{1, 2, 3, 4, 5, 6\}$. Consideramos como conjunto de puntos $X = C \times C$ y como conjunto de bloques*

$$B_{i,j} = \{(x, y) \in X : x = i\} \cup \{(x, y) \in X : y = j\} \cup \{(x, y) \in X : L(x, y) = L(i, j)\} \setminus \{(i, j)\}.$$

Por ejemplo, utilizando el cuadro latino de abajo, el bloque $B_{3,4}$ es el siguiente:

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

Obsérvese que los cinco primero elementos del bloque previo tienen por primera coordenada 3, los cinco siguientes tienen por segunda coordenada 4, los cinco últimos tienen el mismo valor en el cuadro latino que el elemento $L(3, 4)$, es decir 6, y que el elemento $(3, 4)$ no está en el bloque $B_{3,4}$.

Acabamos de construir un 2-$(36, 36, 15, 15, 6)$ diseño. Claramente hay 36 bloques y 36 elementos, pues $|X| = 36$ y tenemos un bloque definido por cada elemento. El resto de comprobaciones las dejamos al lector.

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

La idea de este ejemplo podemos aplicarla con $v = 4$, en este caso obtenemos el 2-$(4, 4, 3, 3, 2)$ diseño, como el del ejemplo 34.

3.2.1. Biplanos

A modo de una primera aproximación, un biplano podemos interpretarlo como un conjunto de rectas (bloques) que tienen dos puntos en común con cualquier otra recta, pero son distintas entre sí. Los bloques son como rectas 'curvas'. Se explica formalmente en la siguiente definición:

Definición 3.12 *[8] Un* **biplano** *es un 2-(v, k, λ) diseño simétrico con $\lambda = 2$.*

Esta definición implica que dos bloques distintos cualesquiera tienen en común $\lambda = 2$ elementos.

Los valores de k (número de elementos en cada bloque) para los cuales se conoce la existencia de biplanos son: $2, 3, 4, 5, 6, 9, 11$ y 13. Veamos algunos ejemplos. En lo que sigue, nos hemos basado en [8].

2-$(2, 2, 2, 2, 2)$ diseño.

Este biplano es el único que no es simple, pues tiene su único bloque repetido. El 2-diseño asociado es el siguiente:

$$\begin{aligned} \mathrm{X} &= \{1, 2\}, \\ \Lambda &= [12, 12]. \end{aligned}$$

2-$(4, 4, 3, 3, 2)$ diseño.

El 2-diseño asociado a este biplano es el siguiente:

$$\begin{aligned} \mathrm{X} &= \{1, 2, 3, 4\}, \\ \Lambda &= \{123, 124, 134, 234\}. \end{aligned}$$

Los bloques de este 2-diseño los podemos obtener de varias formas distintas. La primera de ellas es como el desarrollo del bloque base $\{0, 1, 2\}$ sobre el grupo $\mathbb{Z}_4$. Otra forma posible es basándose en la siguiente figura:

1	$\bigoplus$	2	$\bigoplus$
$\bigoplus$	3	$\bigoplus$	4

Para construir un bloque nos fijamos en los cuadros que no tienen un elemento de X (en los cuales está situado el símbolo $\bigoplus$) y tomamos los elementos de X que están en la misma fila y en la misma columna. La comprobación de que esto proporciona el 2-$(4, 3, 2)$ diseño es clara.

2-$(7, 7, 4, 4, 2)$ diseño.

El 2-diseño asociado a este biplano es el siguiente:

$$\begin{aligned} \mathrm{X} &= \{1, 2, 3, 4, 5, 6, 7\}, \\ \Lambda &= \{3567, 4671, 5712, 6123, 7234, 1345, 2456\}. \end{aligned}$$

Si tomamos como bloque base el $\{0, 2, 3, 4\}$ sobre $\mathbb{Z}_7$ obtenemos el $(7, 4, 2)$-conjunto de diferencias y, por tanto, el biplano correspondiente al 2-$(7, 4, 2)$ diseño.

2-$(11, 11, 5, 5, 2)$ diseño.

El 2-diseño asociado a este biplano es el siguiente:

$$\begin{aligned} \mathrm{X} &= \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}, \\ \Lambda &= \{\{0, 2, 3, 4, 8\}, \{1, 3, 4, 5, 9\}, \{2, 4, 5, 6, 10\}, \{0, 3, 5, 6, 7\}, \{1, 4, 6, 7, 8\}, \{2, 5, 7, 8, 9\}, \\ &\quad \{3, 6, 8, 9, 10\}, \{0, 4, 7, 9, 10\}, \{0, 1, 5, 8, 10\}, \{0, 1, 2, 6, 9\}, \{1, 2, 3, 7, 10\}\}. \end{aligned}$$

Como en el caso anterior, este biplano podemos obtenerlo como desarrollo del $(11, 5, 2)$-conjunto de diferencias. En este caso, el bloque base puede ser $\{0, 2, 3, 4, 8\}$ sobre el grupo $\mathbb{Z}_{11}$. Estos biplanos que hemos mostrado previamente son únicos salvo isomorfismo.

2-$(16, 16, 6, 6, 2)$ diseño.

Un 2-diseño asociado a este biplano es el siguiente:

$X = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15\}$,
$\Lambda = \{\{1, 2, 3, 4, 8, 12\}, \{0, 2, 3, 5, 9, 13\}, \{0, 1, 3, 6, 10, 14\}, \{0, 1, 2, 7, 11, 15\}, \{0, 5, 6, 7, 8, 12\}, \{1, 4, 6, 7, 9, 13\}, \{2, 4, 5, 7, 10, 14\}, \{3, 4, 5, 6, 11, 15\}, \{0, 4, 9, 10, 11, 12\}, \{1, 5, 8, 10, 11, 13\}, \{2, 6, 8, 9, 11, 14\}, \{3, 7, 8, 9, 10, 15\}, \{0, 4, 8, 13, 14, 15\}, \{1, 5, 9, 12, 14, 15\}, \{2, 6, 10, 12, 13, 15\}$
$\{3, 7, 11, 12, 13, 14\}\}$.

Una posible construcción de este biplano se basa en la siguiente figura:

0	1	2	3
4	5	6	7
8	9	10	11
12	13	14	15

Para formar un bloque nos fijamos en una casilla de las 16 posibles (tenemos los 16 elementos de X, uno por casilla, y 16 bloques, uno por casilla). Los elementos de dicho bloque son los elementos que están en la misma fila y en la misma columna menos el correspondiente elemento de la casilla en la que nos fijamos. Por ejemplo, si nos fijamos en la casilla correspondiente al elemento 6, el bloque asociado es $\{2, 4, 5, 7, 10, 14\}$. Es fácil comprobar que el conjunto de todos los bloques genera un biplano con $k = 6$.

Los biplanos que nos faltan por mostrar son tres, de los cuales recogemos sus parámetros en la siguiente tabla. Si se desea consultar más sobre este tema véase [8, capítulo 15]. Para más información sobre un método de construcción de biplanos véase [7].

$\mathbf{k}$	$\mathbf{2} - (\mathbf{v}, \mathbf{k}, \lambda)$
6	2-$(16, 6, 2)$
9	2-$(37, 9, 2)$
11	2-$(56, 11, 2)$
13	2-$(79, 13, 2)$
16	?
18	?

Por último, cabe destacar que los biplanos con $k > 13$ no se sabe si existen o no, se sospecha que solo existen los arriba mencionados, cumpliéndose así la conjetura para el primer valor de $\lambda > 1$. Obsérvese que se desconoce la existencia del 2-$(121, 16, 2)$ diseño, o la del 2-$(154, 18, 2)$ diseño, biplanos con parámetros relativamente pequeños.

Capítulo 4

Aplicaciones

La teoría de diseños combinatorios, marco teórico donde se encaja este trabajo, tuvo sus orígenes en distintas ramas de las matemáticas. Por un lado, como ya hemos visto anteriormente (sección 1.6), en la matemática recreativa, ofreciendo soluciones y problemas de combinaciones y posibles configuraciones con cierta regularidad. Puede asociarse a la teoría de diseños combinatorios problemas conocidos como son los sudokus, los cuadrados mágicos (véase versiones nuevas de [9]) y también se pueden encontrar problemas de ajedrez (entre otros muchos) que pueden ser resueltos (teóricamente por lo menos) mediante los 2-diseños. Por ejemplo, ¿cuántas torres pueden introducirse en un tablero de ajedrez sin que ninguna amenace a otra de forma esencialmente distinta?, ¿y de forma que dos cualesquiera se amenacen?, ¿y si consideramos las preguntas previas pero con los cuadros que pueden recorrer al desplazarse?, ¿o con otras piezas distintas de la torre?, véase [27].
Como en otras ramas de las matemáticas, aunque quizás en combinatoria se cumpla más notablemente, la teoría de diseños combinatorios está relacionada con casi cualquier otro tema en combinatoria. Es sencillo establecer una relación con los grafos, con la teoría de números, con los códigos correctores (véase [9], [17]) o, como hemos ido viendo a lo largo del trabajo, con las geometrías finitas (véase [10]) y ver como según se va desarrollando una teoría se va desarrollando la otra. También hemos observado la relación que guardan los sistemas triples de Steiner con los cuadros latinos, los cuales, en principio, parecían temas sin relación alguna.
El origen seguramente más importante de la teoría de diseños combinatorios provenga de la estadística y de la creación de diseños de experimentos estadísticos. Artículos de estadística como [5] se consideran el origen de esta teoría. Esto queda reflejado en otra multitud de artículos que hacen uso de los 2-diseños para crear diversos experimentos. Algunos de esos artículos son [1], [21], [26] y más claramente en [15].
A continuación, mostramos algunos ejemplos concretos de diversos casos en los que se pueden utilizar 2-diseños para resolver problemas que pueden darse en la realidad.

Ejemplo 38 *Supongamos que en una facultad se van a examinar 26 trabajos de fin de grado. Se han seleccionado 13 profesores para que constituyan los tribunales de cada trabajo. Cada tribunal debe estar constituido por tres profesores. Cada profesor debe estar en 6 tribunales exactamente. Y dos profesores distintos deben coincidir exactamente en un tribunal. La solución es claramente un STS(*13*), es decir, un 2-(*$13, 26, 6, 3, 1$*) diseño; obsérvese que los bloques, de 3 elementos, representan el jurado que evalúa cada uno de los 26 trabajos. Cada profesor corresponde a un elemento del STS(*13*), y cada uno de ellos está en 6 tribunales, número de replicación. Además, dos profesores distintos solo coinciden en la evaluación de un trabajo,* $\lambda = 1$.

Pueden concretarse los ejemplos siguientes pensando que los productos son cremas, vinos, medicamentos, móviles o cualquier otra cosa que necesite un período de pruebas antes de su

exposición al público.

Ejemplo 39 *Supongamos que tenemos una serie de productos y queremos comprobar cual es el que mejor se adapta a nuestras necesidades antes de su comercialización. Para compararlos hacemos que los productos los prueben un conjunto de personas. Supongamos que tenemos 105 productos y 21 personas. Como es lógico, cada persona no puede probar todos los productos, por cuestiones físicas, temporales o por el mero hecho de que no disponemos de 21 muestras de cada uno de los 105 productos. Es aquí donde se puede aplicar la teoría de diseños combinatorios. Por ejemplo, si utilizamos un 2-(*$21, 105, 20, 4, 3$*) diseño tenemos lo siguiente: 21 personas que prueban los 105 productos, cada producto lo prueban 4 personas, cada persona prueba 20 productos y dos personas distintas coinciden en probar 3 productos. De forma totalmente análoga podemos utilizar el 2-(*$21, 105, 40, 8, 14$*) diseño, este 2-diseño hace que 21 personas prueben los 105 productos, que cada producto lo prueben 8 personas, cada persona pruebe 40 productos y dos personas distintas coinciden en probar 14 productos. Ahora tendríamos que elegir el 2-diseño que mejor se adapte a nuestras necesidades. Este tipo de experimentos vienen propuestos en [15].*

Una vez que se ha realizado el experimento pertinente y se dispone de las distintas valoraciones de cada persona, es cuando la estadística utiliza sus herramientas y resultados para determinar cual es el producto más adecuado. Una posible referencia para saber por donde se puede continuar una vez que se ha concluido el experimento puede ser [18, capítulo 4].
También es habitual encontrarse el uso de 2-diseños para la formación de *secretos compartidos*. Para ciertas acciones importantes (lanzamiento de misiles, grandes transacciones económicas...) es normal que tengan que ponerse de acuerdo varias personas, y así no dependa de una sola persona la ejecución de dicha acción. Lo vemos en el siguiente ejemplo.

Ejemplo 40 *Supongamos que existen 28 personas encargadas de las grandes transacciones de una entidad financiera. Para la realización de una transacción por encima de un cierto umbral establecido se requiere la confirmación de 4 personas simultáneamente. Si vemos todas las posibles combinaciones,* $\binom{28}{4}$*, nos damos cuenta de que es un número excesivamente grande para una acción que no suele ser común. Por lo tanto, parece lógico restringir a cada persona en un número determinado de posibles confirmaciones, por ejemplo 9. Es decir, una persona cualquiera está en 9 grupos de cuatro personas con derecho a confirmar la transacción. Puede intentarse a mano las posibles combinaciones. La solución a este problema es un 2-(*$28, 63, 9, 4, 1$*) diseño. Compárese con los datos dados en el enunciado. Obsérvese que dos personas cualesquiera se pueden poner de acuerdo y entonces tienen que convencer a otras dos personas que ya están determinadas por el acuerdo de estas dos, pues* $\lambda = 1$.

Una vez que se han establecido los bloques capaces de realizar la acción pertinente, a cada persona se le puede asignar una parte del secreto total y cuando se completa el secreto es cuando se puede realizar la acción. Podemos pensar que es un segmento de código, un trozo de un mapa...
También podemos encontrar una forma un poco distinta de trabajar con los secretos compartidos aplicando los cuadrados de Room, como puede consultarse en [22].
Por último, de igual forma que la teoría de diseños combinatorios puede utilizarse para solucionar este tipo de problemas previos, también puede utilizarse para crear organizaciones en torneos donde el número de participantes no es una potencia de dos.

Todos los 2-diseños posibles que solucionen los problemas propuestos previamente vienen recogidos, junto con una forma de construcción, en [9].

Apéndice A

Cuadros Latinos y Cuasigrupos

En este apéndice mostramos resultados asociados a los cuadros latinos y a los cuasigrupos, de los cuales hacemos uso a lo largo del trabajo. Hemos seguido [19, capítulo 6] para la mayoría de los resultados y [9, parte II].

Definición A.1 *Un* **cuadro latino** *de orden n es una matriz de $n \times n$ elementos en la que cada casilla está ocupada por uno de los n elementos de un conjunto de cardinal n, de tal forma que cualquiera de ellos aparece una única vez en cada fila y en cada columna.*

Es fácil construir un cuadro latino de orden n. Por ejemplo, podemos tomar la primera fila de la siguiente forma:

1	2	...	n

y hacer rotaciones cíclicas hacia la derecha (o hacia la izquierda) de esta fila $1, 2, ..., n-1$ veces y así construir las $n-1$ filas restantes. En lo que sigue, dado un cuadro latino L, cuando hagamos referencia al elemento que ocupa la posición (i, j), escribiremos $L(i, j)$.

Ejemplo 41 *Un cuadro latino de orden 4.*

1	*2*	*3*	*4*
4	*1*	*2*	*3*
3	*4*	*1*	*2*
2	*3*	*4*	*1*

Por ejemplo, $L(3, 3) = 1$.

Relacionados con los cuadros latinos están los cuasigrupos, los cuales definimos a continuación.

Definición A.2 *Sean X un conjunto de n elementos, y $\circ$ una operación binaria definida en X (es decir, $\circ : X \times X \longrightarrow X$). Decimos que el par $(X, \circ)$ es un* **cuasigrupo** *de orden n siempre que se cumplan las dos propiedades siguientes:*

1. *Para todo $x, y \in X$, la ecuación $x \circ z = y$ tiene una única solución para $z \in X$.*

2. *Para todo $x, y \in X$, la ecuación $z \circ x = y$ tiene una única solución para $z \in X$.*

La *tabla de la operación* de una operación binaria $\circ$ definida en X es la matriz $A = (a_{x,y})$, donde A es de dimensión | X | $\times$ | X | y $a_{x,y} = x \circ y$. El siguiente teorema establece la relación entre los cuasigrupos y los cuadros latinos.

Teorema A.3 *Sea una operación binaria $\circ$ definida sobre X, de cardinal n. Entonces $(X, \circ)$ es un cuasigrupo si y solo si la tabla de la operación es un cuadro latino de orden n.*

Vamos a trabajar con las cuasigrupos (o cuadros latinos) que satisfacen el par de propiedades que definimos a continuación.

Definición A.4 *Sea $(X, \circ)$ un cuasigrupo. Decimos que $(X, \circ)$ es un* **cuasigrupo idempotente** *si $x \circ x = x$ para todo $x \in X$, y decimos que es un* **cuasigrupo simétrico** *si $x \circ y = y \circ x$ para todo $x, y \in X$.*

Estos conceptos también pueden ser definidos para cuadros latinos de manera obvia.

Definición A.5 *Un cuadro latino simétrico $L = (l_{x,y})$ con elementos en X es aquel en el cual se cumple que $l_{x,y} = l_{y,x}$ para todo $x, y \in X$, y es idempotente si $l_{x,x} = x$ para todo $x \in X$.*

Ejemplo 42 *Sea $X = \{1, 2, 3\}$. Tenemos 12 cuadros latinos definidos con los elementos de X.*

$$L_1 = \begin{array}{|c|c|c|}\hline 1&2&3\\\hline 2&3&1\\\hline 3&1&2\\\hline\end{array} \quad L_2 = \begin{array}{|c|c|c|}\hline 1&2&3\\\hline 3&1&2\\\hline 2&3&1\\\hline\end{array} \quad L_3 = \begin{array}{|c|c|c|}\hline 1&3&2\\\hline 2&1&3\\\hline 3&2&1\\\hline\end{array} \quad L_4 = \begin{array}{|c|c|c|}\hline 1&3&2\\\hline 3&2&1\\\hline 2&1&3\\\hline\end{array}$$

$$L_5 = \begin{array}{|c|c|c|}\hline 2&1&3\\\hline 1&3&2\\\hline 3&2&1\\\hline\end{array} \quad L_6 = \begin{array}{|c|c|c|}\hline 2&1&3\\\hline 3&2&1\\\hline 1&2&3\\\hline\end{array} \quad L_7 = \begin{array}{|c|c|c|}\hline 2&3&1\\\hline 1&2&3\\\hline 3&1&2\\\hline\end{array} \quad L_8 = \begin{array}{|c|c|c|}\hline 2&3&1\\\hline 3&1&2\\\hline 1&2&3\\\hline\end{array}$$

$$L_9 = \begin{array}{|c|c|c|}\hline 3&1&2\\\hline 1&2&3\\\hline 2&3&1\\\hline\end{array} \quad L_{10} = \begin{array}{|c|c|c|}\hline 3&1&2\\\hline 2&3&1\\\hline 1&2&3\\\hline\end{array} \quad L_{11} = \begin{array}{|c|c|c|}\hline 3&2&1\\\hline 1&3&2\\\hline 2&1&3\\\hline\end{array} \quad L_{12} = \begin{array}{|c|c|c|}\hline 3&2&1\\\hline 2&1&3\\\hline 1&3&2\\\hline\end{array}$$

El único idempotente es el L_4. Los cuadrados L_1, L_4, L_5, L_8, L_9 y L_{12} son simétricos.

A continuación, vamos a construir cuasigrupos idempotentes y simétricos. Comenzaremos estableciendo una condición para la existencia de cuasigrupos que sean a la par idempotentes y simétricos de orden n.

Lema A.6 *Si existe un cuasigrupo simétrico e idempotente de orden n, entonces n es impar.*

Demostración: Supongamos que X con la operación $\circ : X \times X \longrightarrow X$ es un cuasigrupo simétrico idempotente. Sean $z \in X$, y $S = \{(x, y) : x \circ y = z\}$. Como X es idempotente se sigue que $(x, x) \in S$ si y solo si $x = z$. Además, como X es simétrico se tiene que $(x, y) \in S$ si y solo si $(y, x) \in S$. Entonces $\{\{x, y\} : x \neq y,\ x \circ y = z\}$ es una partición de $X \setminus \{z\}$ en conjuntos de cardial 2. Puesto que $|X| - 1$ es par, $|X|$ es impar. ■

Ahora construiremos un cuasigrupo idempotente y simétrico para cualquier orden impar. Sea n impar y consideremos el grupo $(\mathbb{Z}_n, +)$. Puesto que es un grupo, es claro que también es un cuasigrupo, ver definición A.2. Además, también es simétrico porque la suma módulo n es conmutativa. Como este cuasigrupo no es idempotente (basta tomar el elemento $2 \in \mathbb{Z}_3$) vamos a realizar unas modificaciones para que lo sea. Cuando n es impar, la lista de valores de la diagonal de la *tabla de la operación* de $(\mathbb{Z}_n, +)$ son (en orden):

$$(2x \text{ mod (n)} : x \in \mathbb{Z}_n) = (0, 2, 4, ..., n-1, 1, 3, ..., n-3)$$

Obsérvese como la *tabla de la operación* de $(\mathbb{Z}_n, +)$ tiene todos los elementos de $\mathbb{Z}_n$ en la diagonal, pero en un orden distinto del que buscamos. Vamos a modificar esto mediante una permutación de tal forma que los elementos aparezcan en la diagonal en el orden $0, 1, ...n-1$. Para ello, definimos la permutación π tal que $\pi(0) = 0,\ \pi(2) = 1, ...,\ \pi(n-1) = \frac{n-1}{2},\ \pi(1) = \frac{n+1}{2},\ \pi(3) = \frac{n+3}{2}, ...,\ \pi(n-3) = n-1$. De hecho, la permutación π la podemos escribir como sigue

$$\pi(x) = 2^{-1}x \bmod (n) = \left(\frac{n+1}{2}\right) x \bmod (n)$$

donde $2^{-1} \bmod (n) = \frac{n+1}{2}$ siempre que n sea impar. Entonces, una operación binaria $\circ$, definida sobre $\{0, ..., n-1\}$, que proporciona la estructura de cuasigrupo simétrico idempotente es la siguiente:

$$x \circ y = \left(\frac{n+1}{2}\right)(x+y) \bmod (n).$$

Por tanto, la construcción previa junto con el lema A.6 nos permiten dar el siguiente resultado.

Teorema A.7 *Existe un cuasigrupo simétrico idempotente de orden n si y solo si n es impar.*

Ejemplo 43 *Sea $n = 5$. La operación binaria*

$$x \circ y = 3(x+y) \ \textit{mod}\ (5)$$

define un cuasigrupo simétrico idempotente sobre el conjunto $\{0, 1, 2, 3, 4\}$. El correspondiente cuadro latino (tabla de la operación $\circ$) es como sigue

0	*3*	*1*	*4*	*2*
3	*1*	*4*	*2*	*0*
1	*4*	*2*	*0*	*3*
4	*2*	*0*	*3*	*1*
2	*0*	*3*	*1*	*4*

La siguiente estructura algebraica es la que necesitamos para nuestros propósitos. Fijémonos en que antes, cuando construimos un cuasigrupo simétrico idempotente de orden n, este orden era impar.

Definición A.8 *Sea $X = \{0, 1, ..., n-1\}$, donde n es par. Un cuasigrupo $(X, \circ)$ se dice que es* **cuasigrupo half-idempotente** *si cumple*

$$x \circ x = \begin{cases} x & \textit{si}\ 0 \leq x < \dfrac{n}{2} \\ x - \frac{n}{2} & \textit{si}\ \dfrac{n}{2} \leq x < n \end{cases}$$

Ahora en la diagonal de la *tabla de la operación* veremos las siguientes entradas

$$0, 1, ..., \frac{n}{2} - 1, 0, 1, ..., \frac{n}{2} - 1.$$

Construimos a continuación un cuasigrupo half-idempotente para todos los órdenes n pares. Consideremos el grupo $(\mathbb{Z}_n, +)$. Como en el caso en el que n era impar, el cuasigrupo asociado, con la correspondiente operación, es simétrico e idempotente. Realicemos modificaciones para que $(\mathbb{Z}_n, +)$, con n par, sea un cuasigrupo half-idempotente. Basta darnos cuenta que la lista de valores de

$$(2x \bmod (n) : x \in \mathbb{Z}_n)$$

contiene todos los elementos pares de $\mathbb{Z}_n$ dos veces si n es par. Es decir, los valores que aparecen en la diagonal de la *tabla de la operación* son (en orden):

$$0, 2, ..., n-2, 0, 2, ..., n-2.$$

Por lo tanto, es suficiente renombrar los elementos para que aparezcan en el orden que sigue

$$0, 1, ..., \frac{n}{2} - 1, 0, 1, ..., \frac{n}{2} - 1.$$

Para obtener la estructura de un cuasigrupo half-idempotente, una permutación que cumpla esto puede ser la siguiente:

$$\pi(x) = \left\{ \begin{array}{ll} \frac{x}{2} & \text{si x es par} \\ \frac{x+n-1}{2} & \text{si x es impar} \end{array} \right\}$$

Por tanto la operación del cuasigrupo la podemos definir como

$$x \circ y = \pi((x + y) \bmod (n)).$$

Ejemplo 44 *Sea $n = 6$. La permutación π viene definida como $\pi(0) = 0$, $\pi(1) = 3$, $\pi(2) = 1$, $\pi(3) = 4$, $\pi(4) = 2$ y $\pi(5) = 5$. El resultado es el siguiente cuasigrupo simétrico half-idempotente con la tabla de la operación*

0	*3*	*1*	*4*	*2*	*5*
3	*1*	*4*	*2*	*5*	*0*
1	*4*	*2*	*5*	*0*	*3*
4	*2*	*5*	*0*	*3*	*1*
2	*5*	*0*	*3*	*1*	*4*
5	*0*	*3*	*1*	*4*	*2*

Con la construcción previa podemos concluir con el siguiente teorema:

Teorema A.9 *Existe un cuasigrupo simétrico half-idempotente de orden n si y solo si n es par.*

Finalizamos este apéndice con otras nociones básicas de cuadros latinos. Empezamos con el concepto de cuadros latinos ortogonales y concluimos con las definiciones de cuadros latinos isomorfos y cuadros latinos reducidos.

Definición A.10 *[13] Dos cuadros latinos, $A = (a_{ij})$ y $B = (b_{ij})$, de orden n son* **ortogonales** *si para todo par $(c, d) \in \{(1, 1), (1, 2), ..., (n, n)\}$ existe un único par de índices i, j de forma que $(a_{ij}, b_{ij}) = (c, d)$. Un conjunto de cuadros latinos son* **mutuamente ortogonales** *si dos cualesquiera de ellos son ortogonales.*

Ejemplo 45 *Estos dos cuadros latinos son ortogonales*

1	*2*	*3*	*4*
3	*4*	*1*	*2*
4	*3*	*2*	*1*
2	*1*	*4*	*3*

1	*2*	*3*	*4*
4	*3*	*2*	*1*
2	*1*	*4*	*3*
3	*4*	*1*	*2*

Obsérvese que si ponemos uno encima de otro, obtenemos todos los pares posibles en las 16 casillas, como queda reflejado en el siguiente cuadro. Nótese que sí importa el orden de los elementos.

1 1	2 2	3 3	4 4
3 4	4 3	1 2	2 1
4 2	3 1	2 4	1 3
2 3	1 4	4 1	3 2

Es decir, si nos fijamos en un par de los 16 posibles, existe una única casilla de este cuadro que contiene a ese par. Por ejemplo, si nos fijamos en el par $(4,3)$*, la casilla que contiene a ese par es la* $(2,2)$*.*

El siguiente teorema nos proporciona una forma de construir cuadros latinos ortogonales.

Teorema A.11 *[19] Existen cuadros latinos ortogonales de orden* n *si* $n > 1$ *es impar.*

Demostración: Vamos a construir dos cuadros latinos de orden n cuyos elementos son los elementos de $\mathbb{Z}_n$. Dichos cuadros son:

$$L_1(i,j) = (i+j) \bmod (n)$$
$$L_2(i,j) = (i-j) \bmod (n)$$

Claramente L_1 y L_2 son cuadros latinos de orden n, ver definición A.1. Veamos ahora que son ortogonales cuando n es impar. Supongamos que $(x,y) \in \mathbb{Z}_n \times \mathbb{Z}_n$. Queremos encontrar la única casilla (i,j) de L_1 y de L_2 tal que $L_1(i,j) = x$ y $L_2(i,j) = y$. Resolviendo el siguiente sistema

$$\left\{ \begin{array}{l} i+j \equiv x \bmod (n) \\ i-j \equiv y \bmod (n) \end{array} \right\}$$

cuya solución es

$$i = \left(\frac{x+y}{2}\right) \bmod (n), \qquad j = \left(\frac{x-y}{2}\right) \bmod (n)$$

obtenemos lo buscado. Observamos que esta solución es única. Debido a que n es impar, tiene sentido dividir por 2 en $\mathbb{Z}_n$. ■

Ejemplo 46 *Usando el teorema previo, hemos construido los siguientes cuadros latinos ortogonales de orden 5, cuyos elementos son los elementos de* $\mathbb{Z}_5$*.*

$L_1 =$

0	1	2	3	4
1	2	3	4	0
2	3	4	0	1
3	4	0	1	2
4	0	1	2	3

$L_2 =$

0	4	3	2	1
1	0	4	3	2
2	1	0	4	3
3	2	1	0	4
4	3	2	1	0

Como en el caso previo, basta poner los cuadros uno encima de otro para darse cuenta que están los 25 posibles pares.

0 0	1 4	2 3	3 2	4 1
1 1	2 0	3 4	4 3	0 2
2 2	3 1	4 0	0 4	1 3
3 3	4 2	0 1	1 0	2 4
4 4	0 3	1 2	2 1	3 0

Definición A.12 *[9] Un cuadro latino de orden n, cuyos elementos sean los de $\mathbb{Z}_n$, es* **reducido** *si en la primera fila y en la primera columna aparecen los elementos en orden natural.*
Dos cuadros latinos L y L' de orden n son **isomorfos** *si existe una biyección $\phi : S \to S$ tal que $\phi L(i,j) = L'(\phi(i), \phi(j))$ para cada $i, j \in S$, donde S es el conjunto de elementos y el conjunto de índices de las fila y las columna.*

La siguiente tabla pone de manifiesto la cantidad de posibilidades que hay de formar cuadros latinos, véase [9].

n	**Cuadros latinos de orden n**	**Reducidos de orden n**	**Clases de Isomorfía**
1	1	1	1
2	2	1	1
3	12	1	5
4	576	4	35
5	161280	56	1411
6	812851200	9408	1130531
7	61479419904000	16942080	12198455835
8	108776032459082956800	535281401856	2697818331680661

Apéndice B

Tabla de 2-Diseños

En esta tabla mostramos todos los 2-diseños construidos o mencionados a lo largo del trabajo. Se cita la sección o el ejemplo donde puede encontrarse dicho 2-diseño. Los 2-diseños han sido ordenados por el valor de r, de más pequeño a más grande, después en función del valor de k, en función de λ y, por último, en función de v, como se hace en [9].

Número	**v**	**b**	**r**	**k**	λ	**Lugar**
1	3	1	1	1	1	Ejemplo 1
2	2	2	2	2	2	Sección 3.2.1
3	4	6	3	2	1	Ejemplo 30
4	7	7	3	3	1	Ejemplo 2
5	4	4	3	3	2	Ejemplo 34
6	9	12	4	3	1	Ejemplo 3
7	13	13	4	4	1	Ejemplo 19
8	7	7	4	4	2	Sección 3.2.1
9	6	10	5	3	2	Ejemplo 36
10	16	20	5	4	1	Sección 3.2
11	21	21	5	5	1	Sección 3.2
12	11	11	5	5	2	Ejemplo 17
13	13	26	6	3	1	Sección 1.3
14	7	14	6	3	2	Sección 2.3
15	5	10	6	3	3	Sección 3.2
16	10	15	6	4	2	Sección 12
17	21	30	6	5	1	Ejemplo 15
18	25	30	6	5	1	Sección 3.2
19	31	31	6	6	1	Sección 3.2
20	16	16	6	6	2	Sección 3.2.1
21	11	11	6	6	3	Sección 3.2
22	8	28	7	2	1	Ejemplo 31
23	15	35	7	3	1	Ejemplo 4
24	8	14	7	4	3	Sección 2.3
25	9	24	8	3	2	Sección 2.3
26	25	50	8	4	1	Ejemplo 23
27	13	26	8	4	2	Sección 2.3
28	9	18	8	4	3	Ejemplo 22
29	9	12	8	6	5	Sección 2.6

Número	**v**	**b**	**r**	**k**	λ	**Lugar**
30	49	56	8	7	1	Sección 3.2
31	57	57	8	8	1	Sección 3.2
32	19	57	9	3	1	Ejemplo 6
33	10	30	9	3	2	Sección 2.4
34	7	21	9	3	3	Sección 2.3
35	28	63	9	4	3	Sección 4
36	10	18	9	5	4	Ejemplo 25
37	64	72	9	8	1	Sección 2.6
38	19	19	9	9	4	Sección 2.3
39	21	70	10	3	1	Sección 1.4
40	41	82	10	5	1	Sección 2.4
41	81	90	10	9	1	Sección 2.6
42	16	16	10	10	6	Sección 2.6
43	12	44	11	3	2	Sección 2.4
44	23	23	11	11	5	Sección 2.3
45	13	26	12	6	5	Sección 2.4
46	121	132	12	11	1	Sección 2.6
47	27	117	13	3	1	Sección 1.2
48	27	27	13	13	6	Sección 2.3
49	31	155	15	3	1	Sección 1.2
50	16	80	15	3	2	Sección 2.4
51	13	39	15	5	5	Ejemplo 20
52	36	36	15	15	6	Ejemplo 37
53	31	31	15	15	7	Sección 2.3
54	21	105	20	4	3	Sección 4
55	45	330	22	3	1	Sección 1.5
56	25	60	24	10	9	Sección 2.6
57	63	651	31	3	1	Sección 1.2
58	81	1080	40	3	1	Sección 1.2

Número	**v**	**b**	**r**	**k**	λ	**Lugar**
59	21	105	40	8	14	Sección 4
60	49	168	48	14	13	Sección 2.6
61	81	360	80	18	17	Sección 2.6
62	121	660	120	22	21	Sección 2.6
63	243	9801	121	3	1	Sección 1.2

Bibliografía

[1] F. Yates, M.A. *Incomplete Randomized Blocks*. Preprint. 1936.

[2] R. Peltesohn. *Eine Lösung der Beiden Heffterschen Differenzenprobleme*, Compositio Math. **6** (1939), 251-267.

[3] R. C. Bose. *On the construction of balanced incomplete block designs*, Ann. Eugenics **9** (1939), 353-399.

[4] K. Takeuchi. *A Table of Difference Sets Generating Balanced Incomplete Block Designs*, Review of the International Statistical Institute, **30, No.3** (1962), 361-366.

[5] R. A. Fisher and F. Yates. *Statistical Tables for Biological, Agricultural and Medical Research, Sixth Edition*. Hafner Press, (1963).

[6] R. M. Wilson. *Nonisomorphic Steiner triple systems*, Math. Z. **135** (1974), 303-313. MR **49:**4803

[7] Chester J. Salwach and Joseph A. Mezzaroba. *The Four Biplanes with k=9*, J. Combin. Theory Ser. A, **24** (1978), 141-145.

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

[9] Charles J. Colbourn and Jeffrey H. Dinitz. *The CRC handbook of combinatorial designs*. The CRC series. 1996.

[10] Dieter Jungnickel. *Designs and Finite Geometries*. Des. Codes Cryptogr. Volume 8, **No. 1/2**, (1996).

[11] W. D. Wallis. *Computational and Constructive Design Theory*. Springer Science+Business Media Dordrecht. 1996.

[12] C. C. Lindner and C. A. Rodger. *Design Theory*. CRC Press. 1997

[13] Ian Anderson and Iiro Honkala. *A Short Course in Combinatorial Designs*. Internet Edition, Spring. 1997.
`http://www.utu.fi/~honkala/designs.ps`

[14] Thomas Beth, Dieter Jungnickel and Hanfriend Lenz. *Design Theory*. Cambridge University Press. 1999.

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

[16] J. H. van Lint and R. M. Wilson. *A course in Combinatorics, Second Edition*. Cambridge University Press. 2001.

[17] W. Cary Huffman and Vera Pless. *Fundamentals of Error-Correcting Codes*. Cambridge University Press, 2003.

[18] Douglas C. Montgomery. *Diseño y Análisis de Experimentos, Segunda Edición*. Limusa Wiley, 2004.

[19] Douglas R. Stinson. *Combinatorial Designs: Constructions and Analiysis*. Springer. 2004.

[20] Petteri Kaski and Patric R. J. Östergård. *The Steiner triple systems of order 19*, Math. Comp. **73, No.248** (2004), 2075-2092.

[21] Christos A. Bentis, Anastasioss Zotos and Dimitrios Petridis. *Production of fish-protein products (surimi) from small pelagic fish (Sardinops pilchardusts), underutilized by the industry*. Journal of Food Engineering, **68**, (2005), 303–308.

[22] Justie Su-Tzu Juan and Chia-Li Huang. *Efficient Secret Sharing Schemes from Room Square*. Proceedings of the Third International Conference on Information Technology and Applications, (2005).

[23] A. D. Forbes, M. J. Grannell and T. S. Griggs. *Distance and fractional isomorphism in Steiner triple systems*, Rend. Circ. Mat. Palermo. **56** (2006), 17-32.

[24] A. Caggegi. *$2-(n^2, 2n, 2n-1)$ Designs Obtained from Affine Planes*, Acta Univ. Palacki. Olomuc., Fac. rer. nat., Mathematica **45** (2006), 31-34.

[25] W. D. Wallis. *Introduction to Combinatorial Design, Second Edition*. Chapman & Hall CRC. 2007.

[26] Simone Mueller, Patricia Osidacz, I. Leigh Francis and Larry Lockshin. *Combining discrete choice and informed sensory testing in a two-stage process: Can it predict wine market share?* Food Quality and Preference, **21**, (2010), 741–754.

[27] Ye. Yá. Guik. *Matemática en el tablero de ajedrez: T.1: El tablero y las piezas*. Krasand. 2012.

[28] Petteri Kaski, Patric R. J. Östergård and Alexandru M. Popa. *Enumeration of Steiner triple systems with subsystems*, Math. Comp. **84, No.296** (2015), 3051-3067.

[29] Ian T.W. Neill. *Balanced Incomplete Block Designs and Other Combinatorial Objects*. Preprint.

[30] *https://www.ccrwest.org/cover/steiner.html*