eman ta zabal zazu

Universidad del País Vasco
Euskal Herriko Unibertsitatea

Doctorado en Matemáticas y Estadística

UPV/EHU

Departamento de Matemáticas

Tesis:

Grupos de automorfismos con acciones regulares y semirregulares en estructuras combinatorias

Para obtener el grado de Doctor en Matemáticas y Estadística
Presenta:

JUAN MANUEL MONTOYA CÁRDENAS

jmontoya006@ikasle.ehu.eus

Director: Luis Martínez

luis.martinez@ehu.eus

LEIOA, ESPAÑA. 2024

ÍNDICE GENERAL

AGRADECIMIENTOS

En primer lugar, quiero agradecer de manera especial a Liliana. Tu apoyo constante y comprensión durante esta etapa de mi vida han sido invaluables. Tus palabras de aliento y sacrificio han sido una fuente constante de motivación para superar los desafíos que encontré en el camino. Gracias por creer en mí y por estar a mi lado en cada paso del camino.

A mi querido hijo Santiago, agradezco todo lo que me has dado, a tu manera. Tus sonrisas y abrazos siempre fueron un recordatorio de la razón por la que estaba trabajando tan arduamente. Espero que este logro pueda servirte como un ejemplo de perseverancia y determinación en tu propia vida.

También deseo agradecer a mi director, el Dr. Luis Martínez. Tu guía experta, conocimientos y valiosos consejos fueron fundamentales para la culminación exitosa de esta investigación. Aprecio profundamente tu compromiso y dedicación al orientarme en la dirección correcta.

Asimismo, quiero expresar mi gratitud al profesor Luis Alberto Esteban de la Universidad de Pamplona (Colombia). Tus explicaciones en el ámbito computacional fueron de vital importancia en esta tesis.

Por último, pero no menos importante, deseo expresar mi gratitud a mis amigos y familiares que estuvieron ahí para escucharme, alentarme y brindarme palabras de ánimo cuando más las necesitaba. Su constante apoyo emocional ha sido un pilar fundamental en mi vida.

Capítulo 1

INTRODUCCIÓN

Los primeros trabajos sobre la generación de patrones combinatorios comenzaron cuando la civilización misma estaba tomando forma. La historia es bastante fascinante y abarca muchas culturas en muchas partes del mundo, con vínculos con la poesía y la música. Vamos a discutir en esta introducción solo los aspectos más destacados, los cuales servirán de motivación para profundizar en las raíces del tema.

Desde la antigüedad, los eruditos indios han mostrado interés en organizar cosas en orden regular, aplicando técnicas de ordenación a varios tipos de elementos y conceptos y teorizar sobre dichos arreglos matemáticamente. Este interés se manifestó en reglas para permutaciones, combinaciones y enumeración.

Muchos de los primeros textos sánscritos consideran varias posibilidades para seleccionar y ordenar elementos de un conjunto determinado de elementos. Ya en el período védico tardío en el primer milenio antes de Cristo, los textos conocidos como *pratisākhyās* prescribían formas sistemáticas de reordenar las sílabas de las invocaciones védicas. Dado que recitar perfectamente las palabras de los himnos sagrados se consideraba crucial para el éxito de la sacrificios que los acompañaban, los sacerdotes védicos los memorizaban, no solo en su forma adecuada, si no también con sus sílabas invertidas o reordenadas de otro modo para servir como control de una posible corrupción de la tradición oral.

En la literatura sánscrita se llevó mucho más tiempo incorporar plenamente en su propio campo el discurso matemático y las reglas relacionadas con combinaciones

y permutaciones. Inicialmente, parece que este crédito se manifestó simplemente mediante la adaptación de fórmulas combinatorias y ejemplos de otras disciplinas, fusionándolos con diversas reglas y temas. Un ejemplo temprano de este enfoque se encuentra en el texto de astronomía matemática llamado *Brāhmasphutasiddhānta*, escrito por Brahmagupta en el año 628. Este texto combina un tratamiento bastante sistemático de los cálculos astronómicos con una selección más dispersa de capítulos sobre diversos temas relacionados, que abarcan desde aritmética y álgebra general hasta instrumentos astronómicos ([**28**], págs. 357–358) y [**51**], pág. 230).

Las prácticas combinatorias en China se remontan a la antigüedad, cuando las técnicas adivinatorias dependían de configuraciones de líneas rotas e intactas. El Yijing o I Ching (Libro de Cambios), compilado durante la dinastía Zhou, ha transmitido estas prácticas hasta el presente y ha sido una fuente ampliamente comentada y leída. Sin embargo, las prácticas combinatorias en China no se limitaron a la adivinación y los cuadrados mágicos: numerosas fuentes tempranas también describieron juegos como Go y ajedrez, así como juegos con cartas, dominó y dados, que muestran un interés combinatorio desde un punto de vista más matemático. La fuente más temprana que discute sistemáticamente permutaciones y combinaciones es un manuscrito del siglo XVIII. Aunque para entonces las matemáticas ya se habían introducido desde Europa, el manuscrito se basa claramente en conceptos matemáticos tradicionales y modos algorítmicos.

Durante la dinastía Song (960-1279), los juegos surgieron como otro campo de práctica combinatoria en relación con la escritura matemática. Shen Gua (1031-95), un polímata y funcionario estatal, discutió explícitamente las posibles configuraciones en el juego de Go, con una cuadrícula de 19 × 19 líneas, donde cada posición podía estar vacía o contener una piedra negra o una piedra blanca. Además, textos de finales del siglo XVI, generalmente referidos por los historiadores como “Riyong leishu” (Enciclopedias para el Uso Diario), describen el juego de “azulejos de marfil” (yapai).

Los cuadrados mágicos también han sido una referencia frecuentemente citada para las teorías combinatorias en la antigua China. Sin embargo, como señala Cammann [**15**], solo dos diagramas, el Hetu (Diagrama del Río Amarillo) y el Luoshu (Escritura del Río Luo), que se atribuyen legendaria y mitológicamente a dos figuras semidivinas de los

milenios 3 a.C. y 2 a.C., aparecen en los textos matemáticos y otros textos sobrevivientes antes de la dinastía Song.

Muchos eruditos judíos desde los primeros años de nuestra era estaban interesados en calcular permutaciones y combinaciones. Entre los problemas que llevaron al estudio de estas nociones estaban encontrar el número de palabras que podían formarse con las letras del alfabeto hebreo y determinar el número de conjunciones de los planetas. Fue Levi ben Gerson en el siglo XIV quien logró formalizar estas nociones y derivar rigurosamente las fórmulas para los números de permutaciones y combinaciones.

El pensamiento combinatorio en el Renacimiento tuvo raíces filosóficas, religiosas y teóricas de juegos. El concepto de Llullismo, en el cual todo conocimiento se deriva combinando un número finito de atributos, se originó en el siglo XIII y se extendió por toda Europa; en el mismo siglo encontramos estudios combinatorios relacionados con juegos de dados. A partir del siglo XVI, los jesuitas, cistercienses y miembros de otras órdenes religiosas desempeñaron un papel crucial en el desarrollo de la combinatoria. Las operaciones combinatorias básicas se explicaron e ilustraron con ejemplos de la vida cotidiana y tablas, normalmente sin demostración: la teoría de números y la teoría musical fueron los campos matemáticos de aplicación más importantes. En el siglo XVII, los autores insertaban con frecuencia secciones sobre combinatoria en sus tratados de aritmética o álgebra.

En 1654, Fermat y Pascal utilizaron medios combinatorios y de otro tipo para resolver cuestiones teóricas que surgían de los juegos de azar. El tratado de Pascal sobre el triángulo aritmético podría considerarse el primer tratado moderno de combinatoria. Leibniz también estaba profundamente interesado en este tema, pero casi todas sus contribuciones a funciones simétricas, particiones y determinantes permanecieron inéditas hasta hace poco. También se publicaron las aportaciones de Frénicle de Bessy a la combinatoria después de su fallecimiento. Ars Conjectandi, publicado póstumamente por Jacob Bernoulli ([**6**]) presentó un tratamiento exhaustivo de la combinatoria moderna temprana. Después de la muerte de Bernoulli, Pierre Rémond de Montmort y Abraham de Moivre analizaron matemáticamente los juegos de cartas y de dados en términos de desarreglos. Las contribuciones de James Stirling a la combinatoria fueron motivadas por estudios algebraicos.

El triángulo aritmético es el más famoso de todos los patrones numéricos. Siendo aparentemente una simple lista de los coeficientes binomiales, contiene los números triangulares y piramidales de la antigua Grecia, los números combinatorios que surgieron en los estudios hindúes de arreglos y selecciones, y (apenas disimulados) los números de Fibonacci de la Italia medieval. Revela patrones que deleitan la vista, plantea preguntas que desafían a los teóricos de números y, entre los coeficientes, "Hay tantas relaciones presentes que cuando alguien encuentra una nueva identidad, no hay muchas personas que se entusiasmen, ¡excepto el descubridor!"([**74**]). Para quien esté interesado en conocer más sobre la historia de la combinatoria, se sugiere consultar la referencia [**118**].

Esta tesis se enfoca en el estudio de grupos de automorfismos que actúan de manera regular y semirregular sobre diversas estructuras combinatorias, como grafos dirigidos fuertemente regulares, arreglos ortogonales y cuasi arreglos ortogonales.

El trabajo se inicia con una perspectiva diferente sobre la investigación realizada en mi trabajo de fin de máster, que se centra en la construcción de una nueva familia de grafos dirigidos fuertemente regulares con grupos de automorfismos semirregulares.

Esta investigación se expande más allá al revisar y ampliar los contenidos presentes en el artículo [**38**], incorporando además material presentado en el "9th PhD Summer School in Discrete Mathematics" celebrado en Rogla, Eslovenia, en 2019. Esta ampliación se presenta como una continuación directa de los desarrollos presentados en el trabajo de fin de máster.

Otro aspecto importante de la investigación se refiere a la construcción de conjuntos de diferencias parciales utilizando cilotomía estándar uniforme sobre el producto de dos cuerpos finitos iguales. Este segmento del estudio fue presentado en el "IV Encuentro Matemático del Caribe" en Cartagena de Indias, Colombia, en 2022.

Asimismo, se aborda la temática de cuasi matrices de diferencias cíclicas en la construcción de arreglos ortogonales. En esta tesis, se desarrolla y amplía lo expuesto en el artículo [**90**], que fue colaborativamente elaborado con Luis Martínez y María Merino.

Dada la dificultad en obtener arreglos ortogonales en muchas situaciones, se propone la construcción de cuasi arreglos ortogonales. Este aspecto del trabajo es resultado de una colaboración con Luis Martínez, María Merino y Josué Tonelli que está próximo a ser sometido a publicación en una revista científica indexada.

Finalmente, la tesis inicia la exploración del estudio de arreglos ortogonales infinitos, dejando este aspecto como trabajo futuro. En conjunto, el trabajo aborda una variedad de problemas en el campo de las estructuras combinatorias, presentando contribuciones originales y ampliaciones significativas de investigaciones previas.

En general, una estructura combinatoria es un objeto matemático que se puede construir a partir de un conjunto finito, como un grafo, una matriz, un diseño de bloques o un código. El grupo de automorfismos de una estructura combinatoria es el conjunto de todas las biyecciones del conjunto subyacente que preservan la estructura en cuestión.

Una acción de un grupo es una manera de "mover" los elementos de un conjunto utilizando las operaciones del grupo. Formalmente, se tiene la siguiente definición.

DEFINICIÓN 1.1. *Una acción de grupo de un grupo G sobre un conjunto X es una función que asigna a cada par ordenado (g, x) de $G \times X$ un elemento $g \cdot x$ de X, de manera que se cumplen las siguientes propiedades:*

- *La identidad del grupo actúa como la identidad en el conjunto, es decir, si e es el elemento neutro de G, $e \cdot x = x$ para todo x en X.*
- *La acción es compatible con la multiplicación del grupo, es decir, $(gh) \cdot x = g \cdot (h \cdot x)$ para todos g, h en G y x en X.*

Esta acción se dice que es **semirregular** si no hay elementos no triviales del grupo que fijan los elementos del conjunto. Formalmente, la acción es semirregular si $g \cdot x = x$ para algún $x \in X$, implica que $g = e$. Las acciones semirregulares son utilizadas en la clasificación de grupos finitos simples ([**41**], Capítulo 12). De hecho, algunos de los grupos finitos simples se definen precisamente como grupos que actúan semirregularmente en ciertos conjuntos. También son útiles en la teoría de representación de grupos finitos, ya que por ejemplo, si un grupo actúa semirregularmente en un conjunto, entonces la dimensión de cualquier representación irreducible de ese grupo es un divisor del orden del grupo ([**41**], Capítulo 12).

Por otro lado, una acción de un grupo G sobre un conjunto X se dice que es **transitiva** si para cada par de elementos x, y del conjunto X, existe un elemento g del grupo G que lleva x a y, es decir, $g \cdot x = y$. En otras palabras, una acción es transitiva si la órbita de cualquier elemento del conjunto X bajo la acción del grupo G es todo el conjunto X. La noción de acción transitiva es importante en la teoría de grupos y se utiliza en la clasificación de grupos finitos simples, ya que la transitividad de una acción a menudo

implica ciertas propiedades del grupo en cuestión. Por ejemplo, si un grupo finito G actúa transitivamente en un conjunto X, entonces el grupo G tiene orden divisible por $|X|$ (Teorema de Lagrange).

Se dice que una acción de un grupo sobre un conjunto es **regular** si es semirregular y transitiva. Las acciones regulares de un grupo en un conjunto tienen varias aplicaciones importantes en la teoría de grupos. Un ejemplo común de una estructura combinatoria con una acción regular de un grupo de automorfismos es un grafo de Cayley.

Los orígenes de la teoría de grafos son humildes, incluso frívolos. Mientras que muchas ramas de las matemáticas fueron motivadas por problemas fundamentales de cálculo, movimiento y medición, los problemas que llevaron al desarrollo de la teoría de grafos eran a menudo poco más que acertijos, diseñados para poner a prueba la astucia y estimular la imaginación. Pero a pesar del enfoque más lúdico en términos matemáticos que aparentan tener tales acertijos, éstos capturaron el interés de los matemáticos, con el resultado de que la teoría de grafos se ha convertido en un tema rico en resultados teóricos de una variedad y profundidad sorprendentes.

El primer artículo científico relativo a grafos fue escrito por el matemático suizo Leonhard Euler en 1741 ([**30**]). En dicho artículo, Euler se basó en el problema de los puentes de Königsberg. La ciudad de Kaliningrado, originalmente Königsberg, era famosa por sus siete puentes que unían ambos márgenes del río Pregel con dos de sus islas. Dos de los puentes unen la isla mayor con el margen oriental y otros dos con el margen occidental. La isla menor está conectada a cada margen por un puente y el séptimo puente une ambas islas. El problema planteaba lo siguiente: ¿es posible dar un paseo comenzando desde cualquiera de estas regiones, pasando por todos los puentes, recorriendo solo una vez cada uno y regresando al mismo punto de partida? La Figura 1.1 muestra un mapa de la antigua ciudad de Königsberg. Dicha figura junto con todas las demás figuras de esta tesis son de dominio público y se pueden hallar en la web [**59**].

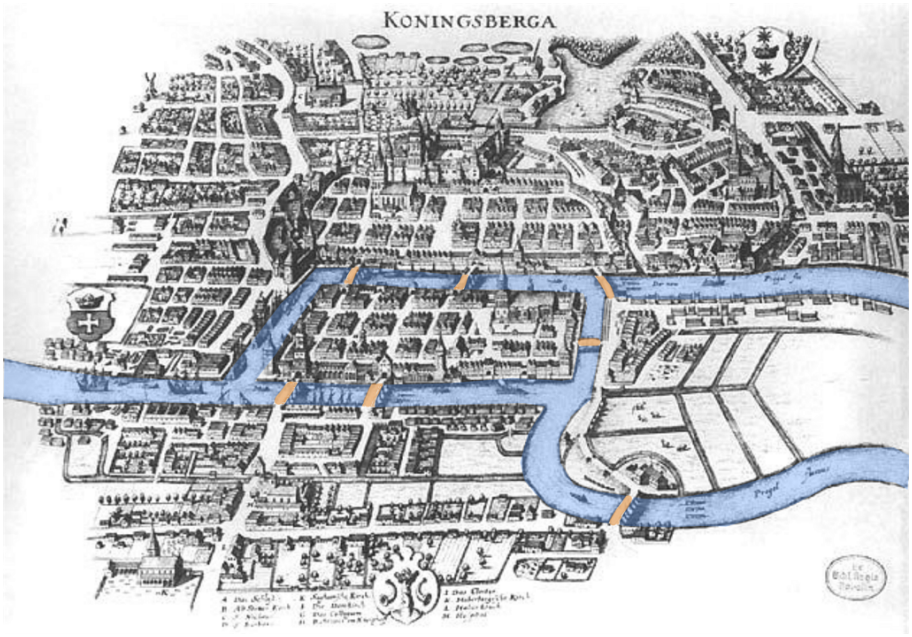

FIGURA 1.1. Mapa de Königsberg del siglo 17

Para lo que interesa estudiar en dicho problema, no son importantes ni las edificaciones de cada región, ni las dimensiones de las regiones, ni la longitud de los puentes, ni las dimensiones del río; es por esto por lo que Euler hizo el siguiente esquema de la región de Königsberg (Figura 1.2):

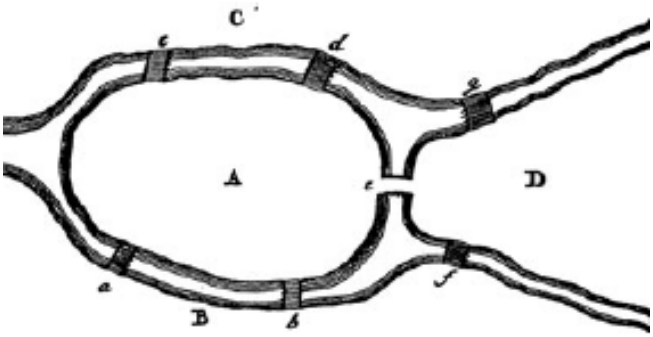

FIGURA 1.2. Esquema de Königsberg dado por Euler en [**30**]

Finalmente, Euler identificó cada región por un punto y cada puente por una línea, para así obtener el diagrama del primer grafo existente. Dichos puntos recibirían posteriormente el nombre de **vértices** y las líneas se llamarían **aristas**. Euler consiguió demostrar, utilizando un argumento de paridad sobre los grados de los vértices, que el problema asociado al grafo de los puentes de Königsberg no tiene solución, es decir, no es posible regresar al vértice de partida sin pasar por alguna arista dos veces. A continuación vemos en la Figura 1.3 un grafo isomorfo al construido por Euler:

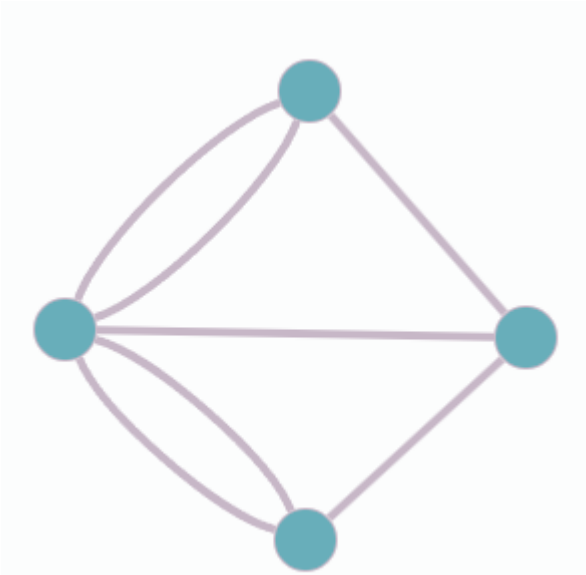

FIGURA 1.3. Grafo de Königsberg

Como anécdota, cabe destacar que dos de los siete puentes fueron destruidos por el bombardero de Königsberg durante la Segunda Guerra Mundial. Otros dos fueron posteriormente demolidos y reemplazados por carreteras modernas. Los tres puentes restantes aún permanecen en pie aunque solo dos de ellos desde la época de Euler, ya que uno de ellos fue reconstruido en 1935.

A partir de las ideas introducidas por Euler, se puede definir el concepto de grafo, el cual contiene elementos sobre los que se define una relación de vecindad o adyacencia. Un vértice puede relacionarse con cualquier otro vértice y establecer cualquier número de relaciones.

En 1809, el matemático francés Louis Poinsot escribió una memoria sobre polígonos y poliedros [**100**] en la que describió los cuatro poliedros regulares no convexos y planteó varios problemas geométricos, incluido el siguiente:

"*Dado algunos puntos situados al azar en el espacio, se requiere organizar un hilo flexible único que los una de dos en dos de todas las formas posibles, de modo que finalmente los dos extremos del hilo se unan y la longitud total sea igual a la suma de todas las distancias mutuas.*"

Poinsot señaló que una solución es posible solo para un número impar de puntos y proporcionó un método ingenioso para unir los puntos en cada uno de estos casos.

De hecho, hay millones de soluciones, como observó más tarde M. Reiss [**103**] en el contexto de determinar la cantidad de formas en que se pueden colocar todas las fichas de dominó en un anillo.

Un tipo de problema de grafos que es similar a los problemas eulerianos ya descritos es el de encontrar un ciclo que pase solo una vez por cada vértice, en lugar de solo una vez a lo largo de cada arista. Por ejemplo, si se nos da el grafo del cubo, entonces es imposible cubrir cada arista solo una vez porque hay ocho vértices de grado 3, pero podemos encontrar un ciclo que pase por cada vértice solo una vez. Estos grafos ahora se llaman grafos hamiltonianos, y los ciclos correspondientes son ciclos hamiltonianos.

Un ejemplo de un problema de ciclo hamiltoniano es el célebre problema del recorrido del caballo. El problema consiste en encontrar una sucesión de movimientos del caballo en un tablero de ajedrez que visite cada una de las sesenta y cuatro casillas solo una vez y regrese al punto de partida. La conexión con los grafos hamiltonianos se puede ver al considerar las casillas como vértices de un grafo y unir dos casillas siempre que estén conectadas por un solo movimiento del caballo.

Las soluciones al problema del recorrido del caballo han sido conocidas durante muchos cientos de años, incluidas soluciones propuestas por de Montmort y de Moivre en el siglo XVII. Sin embargo, no fue hasta mediados del siglo XVIII que el problema fue sometido a un análisis matemático sistemático, realizado por Leonhard Euler [**29**]. Euler mostró en particular que no es posible encontrar una solución para el problema análogo en un tablero de ajedrez con un número impar de casillas. Poco después, A.T. Vandermonde [**110**] analizó el problema, refiriéndose a la solución de Euler de la siguiente manera:

"*mientras que ese gran geómetra presupone que uno tiene un tablero de ajedrez a mano, yo he reducido el problema a una simple aritmética*".

Muchos matemáticos han intentado generalizar el problema a otros tipos de tablero o encontrar soluciones que satisfagan condiciones adicionales. Por ejemplo, Major Carl von Jaenisch [**64**] escribió un relato de tres volúmenes sobre el problema del recorrido del caballo e incluyó una solución ingeniosa en la que la numeración sucesiva de las casillas en un recorrido del caballo produce un cuadrado semimágico en el que las entradas en cada fila o columna suman 260.

Otro problema clásico referente a la teoría de grafos es el famoso **teorema de los cuatro colores**.

La referencia más antigua conocida al problema de los cuatro colores sobre la coloración de mapas se encuentra en una carta fechada el 23 de octubre de 1852, de Augustus De Morgan a Sir William Rowan Hamilton. En esta carta ([**117**]), De Morgan describió cómo uno de sus estudiantes le había preguntado si cada mapa se puede colorear con solo cuatro colores.

El estudiante fue identificado más tarde como Frederick Guthrie, quien afirmó que el problema se debía a su hermano Francis; este último lo formuló mientras coloreaba los condados de un mapa de Inglaterra. En su carta, De Morgan observó que se necesitan cuatro colores para algunos mapas; por ejemplo, si hay cuatro países vecinos, entonces cada país debe tener un color diferente al de sus vecinos, como es mostrado en la Figura 1.4.

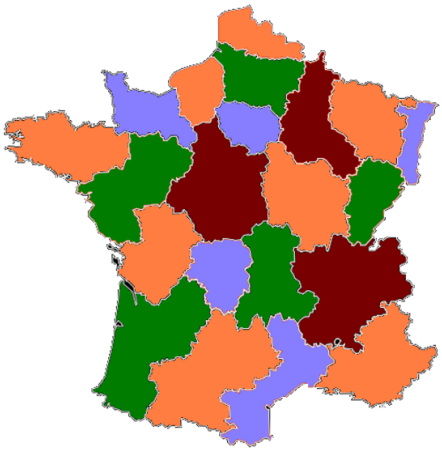

FIGURA 1.4. Un mapa que necesita cuatro colores

De Morgan se interesó rápidamente por el problema y lo comunicó a varios otros matemáticos, por lo que pronto se convirtió en parte de la tradición matemática. En 1860, lo mencionó, en términos bastante oscuros, en una reseña de libros sin firmar [**21**] en el Athenaeum, una revista científica y literaria. Durante muchos años, se creyó que esta era la primera referencia impresa al problema, pero una referencia anterior en el Athenaeum, fechada en 1854 y firmada por “F.G.”, fue encontrada recientemente por Brendan McKay [**92**]. La reseña de De Morgan fue leída en los Estados Unidos por el lógico y filósofo C. S. Peirce, quien posteriormente presentó un intento de demostración ante una sociedad matemática en la Universidad de Harvard.

No fue hasta después de la muerte de De Morgan en 1871 que se lograron avances en la resolución del problema de los cuatro colores. El 13 de junio de 1878, en una reunión de la London Mathematical Society, Cayley preguntó si el problema se había resuelto y poco después escribió un breve artículo [**17**] para la Royal Geographical Society en el que intentaba explicar de manera sencilla dónde radicaban las dificultades. También demostró que se puede hacer la suposición simplificadora de que exactamente tres países se encuentran en cada punto, es decir, que el mapa es cúbico.

En 1879 apareció una de las demostraciones fallidas más famosas en matemáticas. Su autor fue Alfred Bray Kempe, un abogado de Londres que había estudiado con Cayley en Cambridge. Kempe había asistido a la reunión de la London Mathematical Society y se había hecho conocido por su trabajo en mecanismos. Al enterarse de esta demostración, Cayley sugirió que Kempe la enviara al American Journal of Mathematics, recién fundado y editado por Sylvester.

Aunque el artículo de Kempe [**71**] contenía un defecto fatal, incluía algunas ideas importantes que aparecerían en muchos intentos posteriores de resolver el problema.

En 1890, Percy Heawood, quien había conocido el problema mientras estudiaba en la Universidad de Oxford, publicó un artículo [**52**] que señalaba el error de Kempe.

Heawood logró rescatar lo suficiente del argumento de Kempe como para demostrar que cada mapa puede ser coloreado con cinco colores (lo cual es en sí mismo un resultado notable), pero no pudo cerrar la brecha ([**117**], Capítulo 14).

En su artículo de 1879, Kempe había demostrado que cada mapa necesariamente contiene un dígono, un triángulo, un cuadrilátero o un pentágono. Dado que al menos una de estas configuraciones debe aparecer, llamamos a dicho conjunto de configuraciones un conjunto inevitable. También demostró que si un mapa contiene un dígono, un triángulo o un cuadrilátero, entonces cualquier coloración del resto del mapa se puede extender para incluir esta configuración. Cualquier configuración de países para la cual esto sea cierto se llama reducible. Nótese que ninguna configuración reducible puede aparecer en un contraejemplo mínimo al teorema de los cuatro colores.

Donde falló la prueba de Kempe es que no logró demostrar que un pentágono es reducible, y comenzó la búsqueda de configuraciones que pudieran reemplazar al pentágono en el conjunto inevitable. En 1904, Paul Wernicke [**115**] demostró que se puede reemplazar por un par de pentágonos adyacentes y un pentágono adyacente a

un hexágono, obteniendo así un conjunto inevitable más complicado que luego se podría probar que es reducible. Más tarde, en 1922, Philip Franklin [**35**] demostró que todo mapa cúbico que no contiene dígonos, triángulos ni cuadriláteros debe tener al menos doce pentágonos y debe incluir al menos uno de los siguientes:

- un pentágono adyacente a otros dos pentágonos;
- un pentágono adyacente a un pentágono y a un hexágono;
- un pentágono adyacente a dos hexágonos.

Usando este conjunto inevitable, demostró el teorema de los cuatro colores para mapas con hasta veinticinco países. También se proporcionaron conjuntos inevitables por C. N. Reynolds, Henri Lebesgue (principalmente conocido por su trabajo en el cálculo integral) y otros, y a lo largo de los años, el teorema de los cuatro colores se demostró para mapas cada vez más grandes.

Alrededor de 1970, Heinrich Heesch [**54**] presentó argumentos que indicaban que existía un conjunto finito de configuraciones reducibles inevitables y que el número de tales configuraciones no superaría las 9000. Además, desarrolló una técnica para construir conjuntos inevitables, posteriormente llamada método de descarga, y notó que hay ciertas características de un mapa que parecen evitar que una configuración sea reducible.

Estas ideas fueron desarrolladas por Kenneth Appel y Wolfgang Haken, quienes pasaron varios años diseñando programas de computadora que ayudarían en la búsqueda de configuraciones inevitables y asistirían en la prueba de su irreducibilidad. A diferencia de otros investigadores, que crearon grandes cantidades de configuraciones reducibles y luego intentaron empaquetarlas en conjuntos inevitables, el enfoque de Appel y Haken fue construir conjuntos inevitables de configuraciones “probablemente reducibles” y luego verificar su reducibilidad, modificando el conjunto según fuera necesario. Este enfoque ahorró mucho tiempo y esfuerzo. Después de alrededor de 1200 horas de tiempo de computadora, finalmente produjeron un conjunto inevitable de 1936 configuraciones reducibles (posteriormente reducido a 1482), completando así la prueba del teorema de los cuatro colores. Para obtener más detalles sobre su prueba, consulte [**117**].

Desde entonces, los detalles técnicos de la prueba se han simplificado en cierta medida, principalmente por Robertson, Sanders, Seymour y Thomas (consulte [**104**]

y [**109**]), y las configuraciones se han verificado en otras computadoras, pero aún no se ha encontrado una prueba fácilmente verificable. Debido a esto, y porque el trabajo de Appel y Haken planteó interesantes preguntas filosóficas sobre la naturaleza de la prueba matemática, el mundo matemático fue lento en aclamar su magnífico logro (ver Capítulo 11 de [**117**]).

Desde sus inicios, la teoría de grafos ha tenido un gran desarrollo, tanto a nivel teórico como en sus aplicaciones. Hay muchas situaciones prácticas en las que lo más conveniente es modelar los datos de una aplicación a través de grafos, por ejemplo la representación de una red de carreteras, calles, telecomunicaciones, electrificación, internet, planificación de tareas, etapas de un proceso industrial, etc ([**36**], [**69**], [**98**]).

DEFINICIÓN 1.2. *Un **grafo dirigido** (o **digrafo**) G consiste de un conjunto no vacío y finito V de elementos llamados **vértices** y un conjunto finito A de pares ordenados de vértices distintos llamados **arcos**. A menudo se suele escribir el digrafo como $G = (V, A)$, lo que significa que V y A son el conjunto de vértices y el conjunto de arcos de G, respectivamente. El **orden** de G es el número de vértices en G y el **tamaño** de G es el número de arcos en G. El orden de G se denota por $|G|$.*

Gráficamente, los digrafos tienen una representación donde los vértices se representan por puntos y un arco (u, v) se representa mediante una flecha que comienza en u y termina en v. Las flechas en ambas direcciones se suelen reemplazar simplemente por líneas entre los dos puntos.

Por ejemplo, el grafo dirigido G en la Figura 1.5 tiene orden 6 y tamaño 9. El conjunto de vértices es $V = \{1, 2, 3, 4, 5, 6\}$ y el conjunto de arcos es $A = \{(1, 3), (1, 5), (2, 1), (2, 4), (3, 4), (3, 6), (5, 1), (6, 3), (6, 5)\}$.

Veamos algunas definiciones importantes relativas a digrafos:

DEFINICIÓN 1.3. *Sea $G = (V, A)$ un digrafo.*

- *Para un arco (u, v) de G, el primer vértice u es su **origen** (o **cola**) y el segundo vértice v es su **destino** (o **cabeza**). También decimos que el arco (u, v) sale de u y entra en v.*
- *La cabeza y la cola de un arco son sus **vértices finales**.*
- *Si (u, v) es un arco, también decimos que u **domina** a v (o v es **dominado** por u). También se dice que u es **adyacente** a v.*

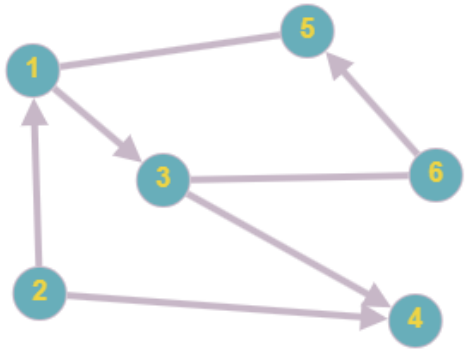

FIGURA 1.5. Ejemplo de grafo dirigido

- *Decimos que un vértice u es **incidente** a un arco a si u es la cabeza o la cola de a. A menudo, se representa un arco (u, v) como uv.*
- *El **grado (o valencia) de entrada** de un vértice v de G es el número de aristas con cabeza v. El **grado (o valencia) de salida** de un vértice u de G es el número de arcos con cola u.*
- *G es k-**regular** si para todo $u \in V$, u domina a k vértices y es dominado por k vértices. Si se entiende por el contexto (o no es importante), se puede eliminar el parámetro k y decir simplemente que G es regular.*
- *El **complemento** de G es el digrafo $\overline{G} = (V, A')$ donde A' contiene todos los posible arcos que no están en A.*
- *Un **camino** desde un vértice u hasta un vértice v es cualquier secuencia de vértices $v_1, v_2, \ldots, v_p$ de tal forma que $v_1 = u$, $v_p = v$ y $(v_i, v_{i+1}) \in A$ para todo $i = 1, 2, \ldots, p-1$.*
- *Un **camino simple** esun camino en el que no hay vértices repetidos en la secuencia, salvo quizás, el primero y el último, que pueden coincidir. Un **ciclo** es un camino simple donde el vértice inicial y el final son el mismo.*
- *La **longitud** de un camino es el número de arcos que forman el camino.*
- *G es **fuertemente conexo** si existe como mínimo un camino desde cualquier vértice hasta cualquier otro vértices.*
- *G es **conexo** si para todos $u, v \in V$ existe un camino de u a v y/o de v a u. Es decir, si nos olvidamos de las direcciones, existe un camino entre todo par de vértices.*

DEFINICIÓN 1.4. *Un **grafo no dirigido** (o simplemente **grafo**)* $G = (V, E)$ *consta de un conjunto no vacío y finito* V *de elementos llamados **vértices** y un conjunto finito* E *de subconjuntos de* V *con cardinalidad 2 llamados **aristas**.*

Los grafos no dirigidos se pueden entender como casos particulares de los digrafos. En un digrafo, las aristas se representan como pares ordenados (u, v), mientras que en un grafo, las aristas son conjuntos de cardinalidad 2 $\{u, v\}$. Si para cualquier par de vértices u, v en el digrafo se cumple la propiedad de que (u, v) es un arco si y solo si (v, u) también es un arco, entonces el digrafo se transforma naturalmente en un grafo no dirigido. Ambos enfoques, aunque utilizan representaciones distintas, son formas equivalentes de modelizar la misma idea, facilitando la transición de un formalismo a otro.

Nótese que, en las definiciones 1.2 y 1.4, no permitimos bucles (pares que consisten del mismo vértice) ni aristas paralelas (múltiples pares con los mismos vértices finales).

Veamos algunos conceptos básicos, pero importantes, acerca de grafos no dirigidos.

DEFINICIÓN 1.5. *Sea* $G = (V, E)$ *un grafo.*

- *Si* $\{x, y\} \in E$*, decimos que los vértices* x *e* y *son **adyacentes**.*
- *Si* e *es una arista entre dos vértices* x *y* y *decimos que* x *e* y *son **incidentes** a* e*.*
- *El **complemento*** $\overline{G}$ *de un grafo* G *es el grafo con el conjunto de vértices* V *en el cual dos vértices distintos son adyacentes si y solo si no son adyacentes en* G*.*
- *El **orden** de* G *es el número de vértices de* G*.*
- *El **grado (o valencia)** de un vértice* $x \in V$ *es el número de vértices adyacentes a* x*.*
- G *es **regular** si todos los vértices tienen el mismo grado.*

Gráficamente, los vértices de un grafo los representamos por puntos y una arista $\{x, y\}$ por una línea que conecta a los vértices representados por x e y. La Figura 1.6 muestra la representación gráfica de un grafo.

A lo largo de esta tesis proporcionamos construcciones de estructuras combinatorias usando sus grupos de automorfismos. Para el caso de los grafos y digrafos, intuitivamente, un automorfismo de un grafo se puede pensar como una proyección de un grafo en sí mismo de manera que preserve la conexión entre vértices y aristas. Estos automorfismos, bajo la composición, forman el grupo de automorfismos. Veamos la definición formal:

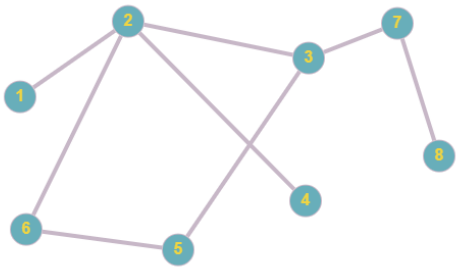

FIGURA 1.6. Ejemplo de grafo no dirigido

DEFINICIÓN 1.6.

- *Sea $G = (V, A)$ un digrafo. Un **automorfismo** de G es una permutación σ del conjunto de vértices V tal que $(u, v) \in A$ si y solo si $(\sigma(u), \sigma(v)) \in A$.*
- *Sea $G = (V, E)$ un grafo. Un **automorfismo** de G es una permutación σ del conjunto de vértices V tal que $\{x, y\} \in E$ si y solo si $\{\sigma(x), \sigma(y)\} \in E$.*
- *Si G es un digrafo (o grafo) la composición de dos automorfismos es otro automorfismo y el conjunto de automorfismos de G bajo la operación de composición forma un grupo, llamado el **grupo completo de automorfismos** del digrafo (o grafo), denotado por. $Aut(G)$. Cada subgrupo de $Aut(G)$ se denomina **grupo de automorfismo** de G.*

En el trabajo de Bose ([**7**]), se presentaron los **grafos fuertemente regulares** de parámetros v, k, μ, λ como grafos regulares no dirigidos, en los cuales, dados dos vértices distintos x e y, el número de caminos de longitud 2 de x a y depende únicamente de si $\{x, y\}$ es una arista o no. Aquí, v es el número de vértices del grafo, k es el grado (o valencia) de cada vértice, μ es el número de caminos de longitud 2 entre cada par de vértices no adyacentes y λ es el número de caminos de longitud 2 entre cada par de vértices adyacentes.

Estos grafos desempeñan un papel crucial en la teoría de grafos y, además de su interés intrínseco en la combinatoria pura, también tienen relevancia en diversas áreas de las matemáticas. Por ejemplo, se descubrió que uno de los grupos esporádicos simples es un subgrupo de índice 2 en el grupo de automorfismos de un grafo fuertemente regular de orden 100 ([**56**]). Además, los grafos fuertemente regulares son herramientas útiles en aplicaciones más prácticas de las matemáticas, como en criptografía ([**5**]) o teoría de codificación ([**48**]).

En el año 1988, A. Duval ([**26**]), generalizó este concepto para grafos dirigidos de la siguiente manera:

DEFINICIÓN 1.7. *Un grafo dirigido de orden v se dice que es un **grafo dirigido fuertemente regular con parámetros** v, k, μ, λ, t (para abreviar escribimos (v, k, μ, λ, t) - **GDFR**) si se cumple:*

i) Cada vértice tiene grado de entrada y salida k.

ii) El número de caminos de longitud 2 de un vértice x a sí mismo es t. Podemos interpretar también este parámetro como el número de aristas no dirigidas del grafo incidentes con un vértice cualquiera.

iii) El número de caminos de longitud 2 de un vértice x a otro vértice distinto y es λ si existe una arista dirigida que empieza en x y termina en y, y μ si no existe tal arista.

EJEMPLO 1.8. *Considérese el siguiente digrafo.*

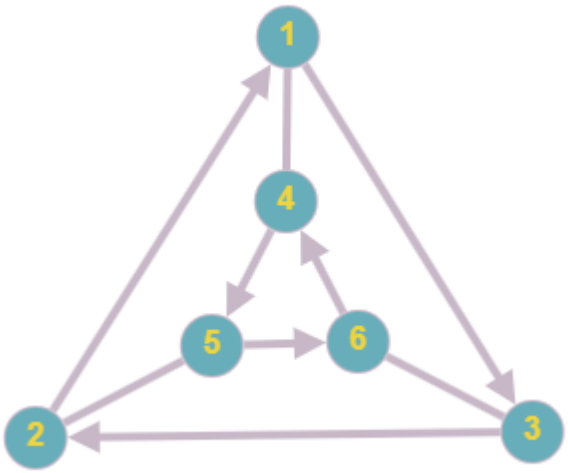

FIGURA 1.7. Un GDFR

Podemos notar que este digrafo tiene 6 vértices (luego $v = 6$), de cada vértice salen 2 aristas y además a cada vértice entran 2 aristas (luego $k = 2$), de cada vértice, sale una única arista no dirigida (luego $t = 1$), existe un único camino de longitud dos entre dos vértices no adyacentes (luego $\mu = 1$) y no existe ningún camino de longitud dos entre cada par de vértices adyacentes (luego $\lambda = 0$).

Por lo tanto, este digrafo es un $(6, 2, 1, 0, 1) - GDFR$.

Se han escrito numerosos artículos sobre grafos dirigidos fuertemente regulares, como se evidencia en obras como [**27**], [**33**], [**46**], [**47**], [**57**], [**65**], [**66**], [**67**], [**73**] o [**93**]. En particular, se ha dedicado considerable atención al estudio de las simetrías en grafos fuertemente regulares, tanto dirigidos como no dirigidos. Se han analizado grafos y digrafos cuyo grupo completo de automorfismos presenta subgrupos con propiedades especiales relacionadas con la estructura de los estabilizadores y el número de órbitas.

Gran parte de la investigación se ha centrado en grafos fuertemente regulares que admiten grupos de automorfismos semirregulares con dos órbitas ([**79**], [**91**], [**22**]) y con tres órbitas ([**77**]). En el año 2010, Martínez y Araluze ([**89**]) ampliaron este estudio a grafos dirigidos fuertemente regulares y, como caso particular, también a grafos fuertemente regulares no dirigidos que admiten un grupo de automorfismos (que no es necesariamente el grupo completo de automorfismos) actuando de manera semirregular en el conjunto de vértices, con un número arbitrario de órbitas. Presentaron las denominadas **familias de sumas parciales** en el contexto general y las **cuádruplas de sumas parciales** para digrafos que admiten grupos de automorfismos semirregulares con dos órbitas. Estas familias de sumas parciales fueron posteriormente objeto de estudio en [**2**], [**3**] y [**88**]. Asimismo, se estudiaron en [**62**] y [**76**] grafos fuertemente regulares que poseen un grupo de automorfismos que fija un vértice y que actúa semirregularmente sobre el resto de los vértices.

En el artículo [**2**] se logró caracterizar a los grafos dirigidos fuertemente regulares que admiten la presencia de un grupo de automorfismos cíclico semirregular con dos órbitas. Como resultado de esta investigación, se identificaron ocho series infinitas de posibles parámetros que describen estos grafos dirigidos fuertemente regulares.

Los grafos fuertemente regulares tienen diversas aplicaciones en diferentes campos, entre ellas se pueden mencionar:

- Teoría de códigos y criptografía: los grafos fuertemente regulares tienen una estrecha relación con la teoría de códigos y criptografía; en particular, se utilizan en la construcción de códigos correctores de errores y esquemas criptográficos ([**40**]).
- Teoría de la información: los grafos fuertemente regulares se utilizan en el estudio de la información y la codificación de datos ([**37**]).

Vamos a introducir algunas nociones.

DEFINICIÓN 1.9. *Un automorfismo (distinto de la identidad) de un digrafo es semirregular, en particular* (m,n)*−semirregular, si tiene* m *ciclos de igual longitud* n *en su descomposición de ciclos.*

DEFINICIÓN 1.10. *Un digrafo es* n*-bicirculante (*bicirculante*, para abreviar) si admite un automorfismo* $(2,n)$*-semirregular.*

DEFINICIÓN 1.11. *Sean* $G=(V,A)$ *un digrafo que admite un automorfismo* (m,n)*-semirregular y* H *un grupo de automorfismo de* G*. Sean* $U_0,U_1,\ldots,U_{m-1}$ *las* m *órbitas de longitud* n *de* H*. Si* $u_k\in U_k$ *para todo* $k=0,\ldots,m-1$*, una familia de subconjuntos* $\{S_{ij}\}$ *de* H*, con* $i,j\in\{0,\ldots,m-1\}$*, se denomina* **símbolo** *de* G *relativo a* $(H;u_0,\ldots,u_{m-1})$*, con*

$$S_{ij}=\{\rho\in H\ :\ (u_i,\rho(u_j))\in A\}$$

La existencia de un automorfismo $(2,n)$-semirregular en un bicirculante nos permite etiquetar su conjunto de vértices y conjunto de aristas de la siguiente manera. Sea G un digrafo $n-$*bicirculante* conexo. Entonces existe un automorfismo $(2,n)$-semirregular ρ y los vértices de G se pueden etiquetar con x_i y y_i con $i=0,1,\ldots,n-1$, tal que $\rho=(x_0\,x_1\,\ldots\,x_{n-1})(y_0\,y_1\,\ldots\,y_{n-1})$. Además, el conjunto de arcos A se puede dividir en los cuatro subconjuntos

$$\bigcup_{i=0}^{n-1}\{(x_i,x_{i+s})\ :\ s\in S_{00}\},\qquad \bigcup_{i=0}^{n-1}\{(x_i,y_{i+s})\ :\ s\in S_{01}\},$$
$$\bigcup_{i=0}^{n-1}\{(y_i,x_{i+s})\ :\ s\in S_{10}\},\qquad \bigcup_{i=0}^{n-1}\{(y_i,y_{i+s})\ :\ s\in S_{11}\}.$$

Denotaremos a este digrafo por $BC_n[S_{00},S_{01},S_{10},S_{11}]$ y por q y r las cardinalidades de S_{10} y S_{00}, respectivamente (se ha introducido una notación similar en **[75]** para grafos bicirculantes).

Si ordenamos los elementos del grupo H de la manera natural, sea H_t el elemento en la posición t de H. La matriz de adyacencia de $BC_n[S_{00},S_{01},S_{10},S_{11}]$ es

$$A=\left(\begin{array}{c|c} A_{S_{00}} & A_{S_{01}} \\ \hline A_{S_{10}} & A_{S_{11}} \end{array}\right), \tag{1.1}$$

donde $A_{S_{ij}}=(a_{k,l})$ con

$$a_{1,l} = \begin{cases} 0 & \textbf{si} \quad H_l \notin S_{ij} \\ 1 & \textbf{si} \quad H_l \in S_{ij} \end{cases},$$

y si $k > 1$,

$$a_{k,l} = \begin{cases} a_{k-1,n} & \textbf{si} \quad l = 1 \\ a_{k-1,l-1} & \textbf{si} \quad l > 1 \end{cases}.$$

EJEMPLO 1.12. *Consideremos el grupo* $\mathbb{Z}_5$*. La matriz de adyacencia del grafo* $BC_5[S_{00}, S_{01}, S_{10}, S_{11}]$*, donde* $S_{00} = \{\overline{1}, \overline{2}, \overline{4}\}$*,* $S_{01} = \{\overline{0}, \overline{2}\}$*,* $S_{10} = \{\overline{1}, \overline{4}\}$ *y* $S_{11} = \{\overline{2}, \overline{3}, \overline{4}\}$ *es*

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

Uno de los temas centrales de esta tesis es el estudio de arreglos ortogonales, los cuales tienen una muy estrecha relación con los grafos fuertemente regulares.

Los arreglos ortogonales provienen de los cuadrados latinos.

Un cuadrado latino de orden n es un arreglo $n \times n$ con entradas de un conjunto de n símbolos, dispuestos de tal manera que cada símbolo aparece exactamente una vez en cada fila y exactamente una vez en cada columna. A partir de este punto de partida simple, la teoría de los cuadrados latinos se ha desarrollado en una disciplina interesante por derecho propio, así como una herramienta importante en la teoría de diseños en general.

Las primeras apariciones conocidas de cuadrados latinos parecen haber sido en su uso en amuletos y rituales en ciertas comunidades árabes e indias desde quizás el año 1000; la naturaleza de las fuentes dificulta la datación. La mayoría de los amuletos similares contienen no un cuadrado latino, sino un cuadrado mágico, un arreglo $n \times n$

lleno con los símbolos $1, 2, \ldots, n^2$, para el cual la suma de los números en cualquier fila, columna o diagonales (principal y secundaria) es la misma. Los amuletos de cuadrado latino, al igual que los de cuadrado mágico, se llevaban para combatir a los espíritus malignos, mostrar reverencia por los dioses, celebrar el sol y los planetas, etc.; en los libros medievales sobre magia y cuadrados latinos, a menudo están enmarcados por estructuras ornamentales caprichosas ([**83**]).

Los cuadrados latinos fueron introducidos en la comunidad matemática por Leonhard Euler. Euler les dio su nombre y parece haber sido el primero en definirlos utilizando terminología matemática, así como en investigar sus propiedades matemáticamente. Aunque ya los conocía y había hecho uso de ellos un poco antes, Euler publicó por primera vez sobre los cuadrados latinos en un artículo que comenzó con su famoso "problema de los treinta y seis oficiales" (una traducción del artículo se puede en encontrar en [**31**]), presentado a la Academia de Ciencias de San Petersburgo en 1779 y publicado en 1782. Con esto, Euler introdujo un concepto más complicado: los *cuadrados latinos ortogonales*.

Se dice que dos cuadrados latinos del mismo orden son *ortogonales* si tienen la propiedad de que cuando dos lugares tienen la misma entrada en un cuadrado, entonces tienen entradas distintas en el otro; se sigue que si los dos cuadrados se superponen, las n^2 celdas contienen cada posible combinación de un símbolo del primer cuadrado y uno del segundo. Así, el problema de los oficiales pide dos cuadrados latinos ortogonales de orden 6.

Leonhard Euler observó que un par de cuadrados latinos ortogonales de orden n se puede describir mediante una lista de n^2 cuádruplas, cada una consistente en un número de fila, un número de columna, el número en esta posición en el primer cuadrado y el número en la misma posición en el segundo cuadrado; esto anticipó la noción posterior de un **arreglo ortogonal**. Euler se dio cuenta de que el significado de las posiciones en las cuádruplas es intercambiable, de modo que dada una pareja de cuadrados latinos ortogonales de un orden dado, podría haber veinticuatro tales parejas, aunque sabía que éstas no podrían ser todas distintas. También afirmó que consideraba el problema de enumerar cuadrados latinos como muy importante pero también muy difícil.

DEFINICIÓN 1.13. *Una matriz A de tamaño $N \times k$ con entradas en $\{0, 1, \ldots, s-1\}$ se dice que es un **arreglo ortogonal** con s niveles (o símbolos), fuerza t ($0 \leq t \leq k$) e índice λ si cada submatriz de A de tamaño $N \times t$ contiene cada t-tupla de elementos en*

$\{0, 1, \ldots, s-1\}$ *exactamente* λ *veces en una fila.* N *es el número de ejecuciones y* k *es el número de factores.*

Denotaremos dicho arreglo ortogonal por $OA(N, k, s, t)$. Los parámetros de un arreglo ortogonal satisfacen la igualdad $N = \lambda s^t$.

En [**11**], vemos que un arreglo ortogonal $OA(n^2, m, n, 2)$ (en este caso se suele denotar simplemente por $OA(m, n)$) induce un grafo fuertemente regular de parámetros $\nu = n^2$, $k = m(n-1)$, $\mu = m(n-1)$, $\lambda = (m-1)(m-2)+n-2$ (no confundir este λ como parámetro del grafo fuertemente regular con el índice λ del arreglo ortogonal, que en este caso es 1). El grafo fuertemente regular asociado a un $OA(m, n)$ se construye de la siguiente manera:

- Se colocan tantos vértices como filas tiene el arreglo ortogonal.
- Se etiquetan los vértices del grafo con las m-túplas que aparecen en cada fila del arreglo ortogonal.
- Hay una arista entre dos vértices dados si las m-tuplas correspondientes a los dos vértices coinciden en al menos una componente (respetando la posición).

Este procedimiento se ve ilustrado en el Ejemplo 1.14.

Un problema importante en el estudio de arreglos ortogonales es el de determinar el número mínimo de ejecuciones N que se necesitan para garantizar la existencia de un $OA(N, k, s, t)$, para valores dados de k, s y t.

Un problema relacionado, que aborda la cuestión de la existencia de arreglos ortogonales de una manera ligeramente diferente, puede formularse de la siguiente manera. Eliminando factores de un $OA(N, k, s, t)$ podemos obtener un $OA(N, k', s, t)$ para $t \leq k' \leq k$. Entonces para valores fijos de N, s y t, el problema de determinar todos los valores de k para los que existe un $OA(N, k, s, t)$ puede resolverse si se sabe el número máximo de factores k en cualquier $OA(N, k, s, t)$.

Para obtener una descripción general de los arreglos ortogonales, remitimos al lector interesado a [**8**], [**11**], [**24**] y [**53**].

Permutar los niveles de un factor en un $OA(m, n)$ se llama hacer una *permutación de niveles*. Dos $OA(m, n)$s se llaman isomorfos si uno puede obtenerse del otro permutando sus columnas, filas y aplicando permutaciones de niveles en sus factores. $OA(m_1, n_1)$ y $OA(m_2, n_2)$ son arreglos ortogonales isomorfos si y solo si el grafo fuertemente regular de $OA(m_1, n_1)$ y el grafo fuertemente regular de $OA(m_2, n_2)$ son grafos isomorfos. En

particular, un automorfismo de arreglos ortogonales es un isomorfismo de un arreglo ortogonal en sí mismo.

EJEMPLO 1.14. *Consideremos el arreglo ortogonal* $OA(2,3)$ *siguiente:*

	Col 1	*Col 2*
Fila 1	*0*	*0*
Fila 2	*0*	*1*
Fila 3	*0*	*2*
Fila 4	*1*	*0*
Fila 5	*1*	*1*
Fila 6	*1*	*2*
Fila 7	*2*	*0*
Fila 8	*2*	*1*
Fila 9	*2*	*2*

TABLA 1.1. $OA(2,3)$

Hagamos las siguientes permutaciones:

- Permutación de niveles (nivel 0 con nivel 1) en cada factor del arreglo ortogonal. Así, el arreglo ortogonal obtenido es

	Col 1	Col 2
Fila 1	1	1
Fila 2	1	0
Fila 3	1	2
Fila 4	0	1
Fila 5	0	0
Fila 6	0	2
Fila 7	2	1
Fila 8	2	0
Fila 9	2	2

- Permutación de fila 1 con fila 5; fila 2 con fila 4; fila 3 con fila 6; y fila 7 con fila 8. Así, el arreglo ortogonal obtenido es

Obtenemos de esta manera un automorfismo del arreglo ortogonal $OA(2,3)$ inicial, dado por $[(0,1)|(1,5)(2,4)(3,6)(7,8)]$, donde la primera componente representa la permutación de niveles y la segunda componente representa las permutaciones de filas.

Además, el grafo fuertemente regular de este arreglo ortogonal tiene parámetros

$$\nu = 9,\ k = 4,\ \lambda = 1,\ \mu = 2,$$

	Col 1	Col 2
Fila 1	0	0
Fila 2	0	1
Fila 3	0	2
Fila 4	1	0
Fila 5	1	1
Fila 6	1	2
Fila 7	2	0
Fila 8	2	1
Fila 9	2	2

el cual representa el grafo de Hamming $H(2,3)$, como vemos en la Figura 1.8.

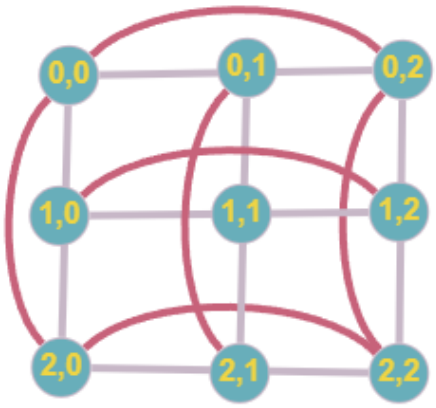

FIGURA 1.8. Grafo de Hamming

Los arreglos ortogonales tienen una amplia variedad de aplicaciones en diversos campos. Algunas de las aplicaciones más comunes incluyen:

- Diseño de experimentos: Los arreglos ortogonales se utilizan comúnmente en el diseño de experimentos para estudiar la relación entre múltiples factores que pueden afectar un proceso o sistema. Por ejemplo, se pueden utilizar para determinar la mejor combinación de ingredientes en una receta de cocina o para determinar la configuración óptima de un proceso de fabricación ([**23**], [**119**]).
- Pruebas de software: Los arreglos ortogonales también se utilizan en el desarrollo de software para probar la funcionalidad de un programa en diferentes entornos. Se pueden utilizar para probar la interacción de diferentes opciones de software y hardware, y para evaluar cómo un programa funciona bajo diferentes condiciones ([**95**]).

- Investigación de mercado: En la investigación de mercado, los arreglos ortogonales se utilizan para evaluar la preferencia del consumidor por diferentes productos y para determinar qué características son las más importantes para los consumidores. También se pueden utilizar para realizar pruebas de concepto y evaluar la efectividad de diferentes estrategias de marketing ([**42**], [**49**]).
- Psicología: Los arreglos ortogonales se utilizan en psicología para estudiar la interacción de diferentes variables en el comportamiento humano, como la relación entre diferentes tipos de estímulos y la respuesta emocional o cognitiva de los sujetos. También se pueden utilizar para estudiar la efectividad de diferentes terapias y tratamientos en pacientes con trastornos mentales ([**43**], [**94**]).

Hay una conocida relación entre los arreglos ortogonales del tipo $OA(n+1, n)$ y los planos proyectivos de orden n. Un plano proyectivo de orden n es un conjunto A de $n^2 + n + 1$ puntos y un conjunto B de n^2+n+1 subconjuntos de A, llamados líneas, con una relación de incidencia entre puntos y líneas con las siguientes propiedades:

- Cada línea contiene exactamente $n + 1$ puntos.
- Cada punto esta contenido en exactamente $n + 1$ líneas.
- Dos líneas diferentes se intersectan en exactamente un punto.
- Dos puntos diferentes estan conectados por exactamente una línea.

Hay planos proyectivos especialmente interesantes, que son los que cumplen la configuración de Desargues. En esta configuración, se encuentran dispuestos diez puntos y diez líneas de manera específica: cada línea contiene tres de los puntos, y, a su vez, por cada punto pasan tres de las líneas. Esta configuración lleva el nombre del ilustre geómetra francés Girard Desargues (1591-1661).

La configuración de Desargues puede ser elaborada en dos dimensiones, a partir de los puntos y líneas involucrados en la definición del teorema de Desargues, el cual establece que dos triángulos son proyectivos desde un punto si y solo si son proyectivos desde una línea. También es factible construirla en tres dimensiones, mediante cinco planos en posición general, o incluso en cuatro dimensiones, empleando un pentácoron, que es el símplex regular de cuatro dimensiones. Esta configuración exhibe un extenso conjunto de simetrías, posibilitando la transformación de cualquier punto en cualquier otro punto y de cualquier línea en cualquier otra línea. Asimismo, presenta la propiedad

de autodualidad, lo que implica que si los puntos son sustituidos por línea, y viceversa, mediante el concepto de dualidad, se obtiene la misma configuración. La Figura 1.9 ilustra la configuración desarguesiana.

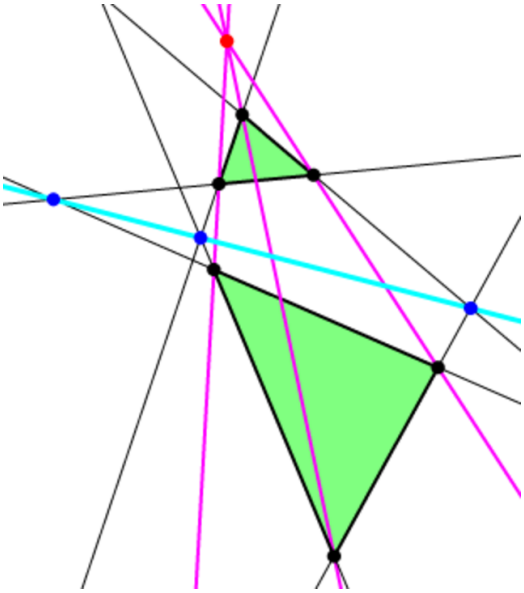

FIGURA 1.9. Configuración Desarguesiana

Estos planos proyectivos se llaman **planos proyectivos desarguesianos**.

Un plano proyectivo desarguesiano se puede definir mediante un conjunto de rectas que pasan por el origen de un espacio vectorial de dimensión 3 sobre un cuerpo K. Podemos suponer, sin perder generalidad, que dicho espacio vectorial es K^3.

Se define una relación de equivalencia $\sim$ sobre los elementos no nulos de K^3 como $(x, y, z) \sim (x', y', z')$ si y solo si existe un elemento r de K tal que $(x, y, z) = r(x', y', z')$. El caso que más nos interesa es aquel en el que K es finito, ya que queremos relacionarlo con los arreglos ortogonales, los cuales son matrices finitas.

Sea $\mathscr{P}$ el conjunto de clases de equivalencia de K^3. Nótese que una clase de equivalencia, o *punto proyectivo*, esta formada por algunos de los vectores no nulos y todos sus múltiplos por escalares diferentes de cero. La clase de equivalencia que contiene a un vector (p, q, r) se suele denotar por $\langle p, q, r\rangle$; los escalares p, q y r se denominan **coordenadas homogéneas del punto** (no son únicas). Claramente, una clase de equivalencia consiste de todos los puntos no nulos que contiene alguna línea que pasa por el origen de K^3.

Sea el conjunto de puntos proyectivos $\langle p, q, r \rangle$ que satisfacen una ecuación homogénea de la forma

$$ax + by + cz = 0$$

con $(a, b, c) \neq (0, 0, 0)$. Recuérdese que $ax + by + cz = 0$ es la ecuación de un plano que pasa por $(0, 0, 0)$ en K^3. Dados dos puntos proyectivos, se puede, resolviendo ecuaciones simultáneas, obtener una única (salvo multiplicación por un escalar distinto de cero) ecuación homogénea que las satisface. Del mismo modo, dadas ecuaciones homogéneas

$$ax + by + cz = 0$$

y

$$dx + ey + fz = 0$$

de tal forma que una no es múltiplo escalar de la otra, existe un único punto proyectivo en el cual las dos ecuaciones se intersectan.

En resumen, el plano proyectivo desarguesiano se construye como el conjunto de todas las rectas que pasan por el origen del espacio vectorial tridimensional, representadas mediante vectores de coordenadas homogéneas. Esta construcción permite representar puntos y líneas en el plano proyectivo y establecer relaciones proyectivas entre ellos.

En este sentido, los puntos del plano proyectivo son los subespacios de dimensión 1 del espacio tridimensional y las lineas son los subespacios de dimensión 2.

Uno de los ejemplos más famosos es el Plano de Fano, el cual es un plano proyectivo de orden 2 y se suele representar gráficamente como sigue:

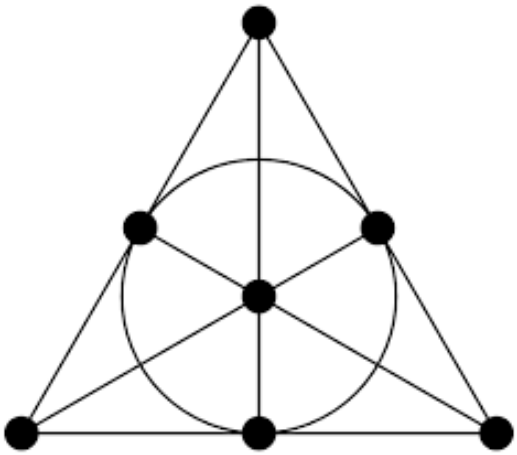

FIGURA 1.10. Plano de Fano

Los planos proyectivos (desarguesianos o no) de orden superior, como los de orden 3, 4, 5, 7, 8, 9, 11, 13, etc, siguen las mismas propiedades básicas pero con un número mayor de puntos y líneas. ¿Por qué no se menciona a los planos proyectivos de orden 6, 10, 12, etc?. Veblen y Bussey ([**111**]) demostraron que existen planos proyectivos finitos de orden p^m con p un número primo y m un entero positivo. Por tanto, existen planos proyectivos de órdenes 2, 3, 4, 5, 7, 8, 9, 11, 13, etc. Se conjetura que los únicos órdenes para los que existe un plano proyectivo de orden n son los números primos elevados a alguna potencias entera positiva. Euler conjeturó que no existe un plano proyectivo de orden $n = 2 \mod 4$. Ésta es la famosa conjetura de Euler. Tarry alrededor del año 1900 ([**107**]) comprobó mediante una enumeración sistemática que la conjetura de Euler se cumple para $n = 6$. Sin embargo, hay algo desagradable en una enumeración manual sistemática: es confusa y propensa a errores. Los matemáticos encontraron una mejor explicación en el célebre teorema de Bruck-Ryser ([**12**]), publicado en 1949. Bruck y Ryser lograron demostrar que no existe un plano proyectivo de orden n, si n es congruente con $1 \mod 4$ o $2 \mod 4$, y n no puede escribirse como la suma de dos cuadrados. Este resultado demostró que n no puede ser 6, 14, 21, 22, etc.

Los planos proyectivos son casos particulares de una clase de objetos combinatorios llamados diseños de bloques simétricos. No vamos a discutir diseños de bloques, excepto mencionar que Chowla y Ryser han generalizado el teorema de Bruck-Ryser a diseños de bloques simétricos ([**18**]), que ahora se conoce como teorema de Bruck-Ryser-Chowla. Aquí nuevamente existe una demostración parcial, lo que da más credibilidad a la esperanza de que las condiciones del teorema de Bruck-Ryser-Chowla sean necesarias y suficientes. Esta esperanza ahora se ve destrozada por la inexistencia del plano proyectivo finito de orden 10.

Ahora que tenemos una buena explicación de la inexistencia de un plano de orden 6, ¿cuál es el siguiente caso desconocido? Es $n = 10$. Dado que $10 = 12 + 32$, existiría un plano de orden 10 si la condición necesaria del teorema de Bruck-Ryser también fuera suficiente. Por otro lado, $10 = 2 \mod 4$, por lo que, si uno cree en la conjetura de Euler, entonces no existe.

Primero, se demostró que la conjetura de Euler era falsa. En 1959, Bose y Shrikhande ([**9**]) construyeron un par de cuadrados latinos ortogonales de orden 22. Luego Parker ([**96**], [**97**]) construyó un par de cuadrados latinos ortogonales de orden 10. Juntos

demostraron que la conjetura de Euler es falsa para todos los órdenes mayores de seis ([**10**]). Esto generó esperanzas de la existencia de un plano de orden 10.

La historia indicó que se lograron avances significativos cuando se demostró que una rama de las matemáticas estaba relacionada con otra rama diferente. No es sorprendente que el fin del plano de orden 10 se produjera cuando la gente empezó a estudiar el código binario de corrección de errores asociado a él [**78**].

Actualmente, el orden más bajo para el cual no se ha demostrado la conjetura es 12.

Existe una conexión conocida entre los arreglos ortogonales del tipo $OA(n+1,n)$ y los planos proyectivos de orden n. Para construir un $OA(n+1,n)$ a partir de un plano proyectivo de orden n se sigue el siguiente procedimiento:

- Se selecciona una línea cualquiera L del plano proyectivo y se etiquetan por P_0, P_1,...,P_n los $n+1$ puntos que contiene la línea L.
- Se etiquetan por Q_1, Q_2,...,Q_{n^2} los n^2 puntos restantes (los que no están en L).
- Para todo $j = 1, 2, \ldots, n+1$, se toma un etiquetado con $1, \ldots, n$ de todas las líneas incidentes en P_{j-1}, pero distintas de L.
- Se construye la matriz

$$A = (a_{ij}) \qquad i = 1, 2, \ldots, n^2; \quad j = 1, 2, \ldots n+1,$$

donde a_{ij} es la etiqueta que se le puso a la línea que contiene a Q_i y a P_{j-1}

Esta matriz A resulta ser un $OA(n+1,n)$.

Recíprocamente, si A es un $OA(n+1,n)$, se puede construir un plano proyectivo de orden n de la siguiente manera:

- Se construye una línea L que contenga $n+1$ puntos, los cuales llevarán las etiquetas $P_0, P_1, \ldots, P_n$.
- Cada fila del arreglo ortogonal determina un punto no incidente a L. Estos puntos los etiquetamos $Q_1, Q_2, \ldots, Q_{n^2}$.
- La columna j-ésima del arreglo ortogonal la asociamos con el punto P_{j-1}.
- Por P_{j-1} pasan tantas líneas (distintas de L) como elementos tenga el conjunto de símbolos del arreglo ortogonal (es decir, n). Estas líneas llevarán las etiquetas sacadas del conjunto de símbolos del arreglo ortogonal.

- Si el elemento ij del arreglo ortogonal es, por ejemplo, k (elemento del conjunto de símbolos) se tiene que la k-ésima línea (distinta de L) que incide en P_{j-1} contiene al punto Q_i.

EJEMPLO 1.15. *El arreglo ortogonal asociado al plano de Fano es el* $OA(3,2)$

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

Esta conexión es utilizada en algunos estudios para analizar diseños de experimentos utilizando propiedades geométricas de los planos proyectivos, o para explorar estructuras de planos proyectivos utilizando propiedades de los arreglos ortogonales.

Es importante destacar que esta relación está limitada a los arreglos ortogonales del tipo $OA(n+1,n)$ y los planos proyectivos de orden n. Otros tipos de arreglos ortogonales o planos proyectivos de diferentes órdenes pueden no estar relacionados de la misma manera.

Otra estructura combinatoria que analizamos en esta tesis son los conjuntos de diferencias parciales obtenidos a partir de la ciclotomía estándar uniforme sobre un producto de dos cuerpos finitos iguales. Describimos las órbitas correspondientes a esta ciclotomía y usamos el software computacional GAP ([**61**]) para describir el grupo completo de automorfismos de los conjuntos de diferencias parciales dados por dicha ciclotomía.

Ante la dificultad, en la mayoría de los casos, de obtener arreglos ortogonales, nos vemos en la necesidad de relajar este concepto permitiendo una discrepancia en la cantidad de veces que aparecen cada combinación en tuplas de columnas. Es decir, unos arreglos que no cumplen la propiedad de ortogonalidad de un arreglo ortogonal, pero se acercan a ella. Estos arreglos se denominan **cuasi arreglos ortogonales.** En un cuasi arreglo ortogonal, cada columna sigue representando un factor y cada fila representa una combinación única de valores para esos factores. La principal diferencia entre un cuasi arreglo ortogonal y un arreglo ortogonal es que en un arreglo ortogonal cada combinación de tuplas tiene una misma cantidad predefinida de coincidencias. En cambio, en un cuasi arreglo ortogonal, las tuplas pueden tener algunas coincidencias limitadas. Esta

diferencia significa que los cuasi arreglos ortogonales pueden ser más flexibles y útiles, en algunos casos, que los arreglos ortogonales.

Los cuasi arreglos ortogonales son una herramienta útil para la optimización y el diseño de sistemas en una amplia variedad de campos, como la ingeniería, la ciencia de materiales, la medicina, la biología, la química y la psicología, entre otros.

Capítulo 2

UNA NUEVA FAMILIA DE GRAFOS DIRIGIDOS FUERTEMENTE REGULARES CON GRUPOS DE AUTOMORFISMOS SEMIRREGULARES

Los grafos dirigidos fuertemente regulares son versiones dirigidas de grafos fuertemente regulares y fueron definido originalmente por Duval [**26**].

Muchos resultados para grafos fuertemente regulares tienen análogos para la versión dirigida. Los grafos fuertemente regulares son un tema interesante a trata debido a su estructura bien definida, sus aplicaciones en diseño experimental y sus propiedades algebraicas y combinatorias que iremos viendo más adelante.

En este capítulo, los símbolos (como en la definición 1.11 de esta tesis) con los que trabajaremos serán subconjuntos de un grupo finito H, que los indentificaremos con elementos del anillo de grupo $\mathbb{Z}[H]$, por lo que las operaciones internas entre estos conjuntos son las operaciones en el anillo de grupo. Esto es, si A y B son subconjuntos de $\mathbb{Z}[H]$ y $\alpha \in \mathbb{N}$:

- $A + B$ es el multiconjunto que está compuesto tanto por los elementos de A como por los elementos de B, admitiendo todas las repeticiones si aplica.
- AB es el multiconjunto formado por todas las sumas posibles (entiéndase esta suma como la suma en H) de elementos de A con elementos de B, admitiendo repeticiones.
- αA es el multiconjunto que contiene todos los elementos de A una cantidad α de veces.

Adicionalmente a esto, decimos que $A = B$ si cada elemento de A aparece la misma cantidad de veces en B y viceversa.

En este capítulo se intruduce un tipo de símbolo, el cual está directamente relacionado con los GDFRs.

DEFINICIÓN 2.1. *Sea H un grupo de orden n y m un número entero tal que $m \geq 1$. Una familia $\mathfrak{G} = \{S_{i,j}\}$, con $0 \leq i, j \leq m-1$, de subconjuntos de H es una $(m, n, k, \mu, \lambda, t)$-**familia de sumas parciales** (para abreviar, $(m, n, k, \mu, \lambda, t)$-**FSP, o simplemente FSP**) si satisface lo siguiente:*

i) Para cada i, se cumple que $e \notin S_{i,i}$, donde e es la identidad de H.

ii) Para todo i, se cumple que $\sum_{j=0}^{m-1} |S_{i,j}| = \sum_{j=0}^{m-1} |S_{j,i}| = k$.

iii) Para todos i y j, se cumple $\sum_{l=0}^{m-1} S_{l,j}S_{i,l} = \delta_{i,j}\gamma\{e\} + \beta S_{i,j} + \mu H$, donde $\delta_{i,j}$ es la delta de Kronecker, $\gamma = t - \mu$ y $\beta = \lambda - \mu$.

EJEMPLO 2.2. *Sea $H = \mathbb{Z}_6$ el grupo de clases residuales módulo 6 y $m = 2$. Los conjuntos*

$$\begin{aligned} S_{0,0} &= \{2, 3, 5\} \\ S_{0,1} &= \{0, 3\} \\ S_{1,0} &= \{0, 3\} \\ S_{1,1} &= \{1, 3, 4\} \end{aligned}$$

*forman una $(2, 6, 5, 2, 2, 3)$-**FSP**. En efecto, $0 \notin S_{0,0} \cup S_{1,1}$, por lo que la condición i) se cumple.*

Por otro lado,

$$|S_{0,0}| + |S_{0,1}| = |S_{0,0}| + |S_{1,0}| = 5 \quad \textit{y}$$

$$|S_{1,0}| + |S_{1,1}| = |S_{0,1}| + |S_{1,1}| = 5,$$

luego $k = 5$.

Por último, analicemos todas las sumas que proporciona la condición iii):

- $S_{0,0}S_{0,0} + S_{1,0}S_{0,1} = \{4, 5, 1, 5, 0, 2, 1, 2, 4\} + \{0, 3, 3, 0\} = \{4, 5, 1, 5, 0, 2, 1, 2, 4, 0, 3, 3, 0\} = 1\{0\} + 0S_{0,0} + 2\mathbb{Z}_6$.
- $S_{0,1}S_{0,0} + S_{1,1}S_{0,1} = \{2, 5, 3, 0, 5, 2\} + \{1, 3, 4, 4, 0, 1\} = \{2, 5, 3, 0, 5, 2, 1, 3, 4, 4, 0, 1\} = 0S_{0,1} + 2\mathbb{Z}_6$.

- $S_{0,0}S_{1,0} + S_{1,0}S_{1,1} = \{2,5,3,0,5,2\} + \{1,3,4,4,0,1\} = \{2,5,3,0,5,2,1,3,4,4,0,1\} = 0S_{1,0} + 2\mathbb{Z}_6$.
- $S_{0,1}S_{1,0}+S_{1,1}S_{1,1} = \{0,3,3,0\}+\{2,4,5,4,0,1,5,1,2\} = \{0,3,3,0,2,4,5,4,0,1,5,1,2\} = 0\{0\} + \beta S_{1,1} + 2\mathbb{Z}_6$.

de donde se tiene que $\mu = 2$*,* $\beta = \lambda - \mu = \lambda - 2 = 0$*, esto es,* $\lambda = 2$*, y* $\gamma = t - \mu = t - 2 = 1$*, de donde* $t = 3$*.*

Si H es cíclico (respectivamente, abeliano), se dice que la FSP es circulante (respectivamente, abeliana).

En el artículo [**2**] se presentó sin demostración el siguiente resultado, por lo que en esta tesis se presenta una demostración de la misma.

PROPOSICIÓN 2.3. *La familia* $\mathfrak{G} = \{S_{i,j}\}$ *es una* (m,n,k,μ,λ,t)*-FSP si y solo si el digrafo asociado al símbolo* $S_{i,j}$ *es un* (mn,k,μ,λ,t)*-GDFR (que admite* H *como un grupo de automorfismos* (m,n)*-semirregular).*

DEMOSTRACIÓN. Sea $\mathfrak{G} = \{S_{i,j}\}$ una (m,n,k,μ,λ,t)-FSP. Ya vimos en la introducción de esta tesis la manera de construir el grafo asociado a dicho símbolo. El hecho de que $e \notin S_{i,i}$, implica que la diagonal de la matriz de adyacencia no contiene ningún 1, por lo que el grafo no tiene bucles. La condición ii) implica que el número de 1s en cada fila y cada columna es k, es decir, el grado de entrada y salida de cada vértice es k. Finalmente, la condición iii) implica que el número de caminos de longitud 2 de un vértice a sí mismo es t, que el número de caminos de longitud 2 de un vértice a otro distinto es λ si existe una arista dirigida entre los dos vértices y μ si no existe tal arista. Por tanto, esta matriz es la matriz de adyacencia de un (mn,k,μ,λ,t)-GDFR.

El recíproco sigue un razonamiento similar, pudiéndose etiquetar las órbitas asociadas al grupo de automorfismos por los elementos de H, de forma que el digrafo quede caracterizado por su correspondiente símbolo. Ahora, las condiciones combinatorias de ser fuertemente regular se traducen en las condiciones algebraicas que aparecen en el enunciado. ■

EJEMPLO 2.4. *La matriz de adyacencia del digrafo asociado a la* $(2,6,5,2,2,3)$*-FSP del ejemplo 2.2 es*

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

Para demostrar que este digrafo es un GDFR utilizamos el siguiente conocido resultado:

"Un digrafo G *es un* (v,k,μ,λ,t)*-GDFR si y solo si la matriz de adyacencia* A *satisface las siguientes dos condiciones:*

- $AJ = JA = kJ$
- $A^2 = tI + \lambda A + \mu(J - I - A)$,

donde I *denota la matriz identidad y* J *la matriz con todo unos."*

Se tiene que

$$AJ = JA = \begin{pmatrix} 5&5&5&5&5&5&5&5&5&5&5&5\\ 5&5&5&5&5&5&5&5&5&5&5&5\\ 5&5&5&5&5&5&5&5&5&5&5&5\\ 5&5&5&5&5&5&5&5&5&5&5&5\\ 5&5&5&5&5&5&5&5&5&5&5&5\\ 5&5&5&5&5&5&5&5&5&5&5&5\\ 5&5&5&5&5&5&5&5&5&5&5&5\\ 5&5&5&5&5&5&5&5&5&5&5&5\\ 5&5&5&5&5&5&5&5&5&5&5&5\\ 5&5&5&5&5&5&5&5&5&5&5&5\\ 5&5&5&5&5&5&5&5&5&5&5&5\\ 5&5&5&5&5&5&5&5&5&5&5&5 \end{pmatrix} = 5J$$

y que

$$A^2 = \begin{pmatrix} 3 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \\ 2 & 3 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \\ 2 & 2 & 3 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 3 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 & 3 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 & 2 & 3 & 2 & 2 & 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 & 2 & 2 & 3 & 2 & 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 & 2 & 2 & 2 & 3 & 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 3 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 3 & 2 & 2 \\ 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 3 & 2 \\ 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 3 \end{pmatrix} = 3I + 2A + 2(J - I - A)$$

*Así, el digrafo con matriz de adyacencia A es un $(12, 5, 2, 2, 3)$-**GDFR**.*

DEFINICIÓN 2.5. *Cuando $m = 2$, llamaremos a una FSP una **cuádrupla de sumas parciales** (para abreviar, **CSP**). En este caso omitiremos el término m en la lista de parámetros y diremos que es una (n, k, μ, λ, t)-cuádrupla de sumas parciales. En este caso, denotaremos a los elementos del símbolo por $Q := S_{10}$, $R := S_{00}$, $S := S_{11}$ y $T := S_{01}$. De ahora en adelante denotaremos por $\mathbf{q}$, $\mathbf{r}$, $\mathbf{s}$ y $\mathbf{t}$ a las cardinalidades de Q, R, S y T, respectivamente, y el grupo H será abeliano. Para las CSPs, las igualdades en la parte iii) de la Definición 2.1 tienen la siguiente forma:*

$$R^2 + QT = \gamma\{e\} + \beta R + \mu H \tag{2.1}$$

$$T(R + S) = \beta T + \mu H \tag{2.2}$$

$$Q(R + S) = \beta Q + \mu H \tag{2.3}$$

$$S^2 + QT = \gamma\{e\} + \beta S + \mu H \tag{2.4}$$

El siguiente teorema permite clasificar los parámetros de las CSPs.

TEOREMA 2.6. *(**[2]**, Theorem 4.1) Sea $\mathfrak{G}$ una CSP no trivial sobre un grupo cíclico H. Entonces los parámetros de $\mathfrak{G}$ tienen alguna de las siguiente formas, donde $U = k - t$ y g, f son enteros positivos:*

i) $n = g(2f + 1), \mathbf{q} = gf, \mathbf{r} = gf, k = 2gf, \mu = gf, \lambda = g(f - 1), t = gf$.

ii) $n = g(2f + 1), \mathbf{q} = g(f + 1), \mathbf{r} = gf, k = g(2f + 1), \mu = g(f + 1), \lambda = gf, t = g(f + 1)$.

iii) $n = 4g, \mathbf{q} = 2g, \mathbf{r} = 2g - 1, k = 4g - 1, \mu = g, \lambda = 3g - 2, t = 3g - 1$.

iv) $n = 2g^2 + 2g + 1 + 2U, \mathbf{q} = g^2 + U, \mathbf{r} = g^2 + g + U, k = 2g^2 + g + 2U$, $\mu = g^2 + U, \lambda = g^2 - 1 + U, t = 2g^2 + g + U$.

v) $n = 2g^2 + 2U, \mathbf{q} = g^2 + U, \mathbf{r} = g^2 + g + U, k = 2g^2 + g + 2U$,
$\mu = g^2 + g + U, \lambda = g^2 + g + U, t = 2g^2 + g + U$, ***donde*** $2g|(g^2 + U)$.

vi) $n = 2g^2 + 2U, \mathbf{q} = g^2 + U, \mathbf{r} = g^2 - g + U, k = 2g^2 - g - 2U$,
$\mu = g^2 - g + U, \lambda = g^2 - g + U, t = 2g^2 - g + U$, ***donde*** $2g|(g^2 + U)$.

vii) $n = 2g^2 + 2U, \mathbf{q} = g^2 \pm g + U, \mathbf{r} = g^2 + U, k = 2g^2 \pm g + 2U$,
$\mu = g^2 \pm g + U, \lambda = g^2 \pm g + U, t = 2g^2 \pm g + U$, ***donde*** $g|U$.

viii) $n = 4g^2, \mathbf{q} = 2g^2 \pm 2g, \mathbf{r} = 2g^2 \pm g, k = 4g^2 \pm 3g, \mu = (g \pm 1)(2g \pm 1)$, $\lambda = (g \pm 1)(2g \pm 1)$,
$t = g^2 + (g \pm 1)(2g \pm 1)$.

A continuación, daremos algunos resultados sobre la existencia de CSPs sobre grupos cíclicos para las familias de parámetros presentadas en el Teorema 2.6.

En relación a las familias i), ii) y iii), las CSPs circulantes con esos parámetros siempre existen según las Proposiciones 3.7, 3.8 y 4.14 en [**2**].

En lo que respecta a la familia iv), los autores de [**89**] hallaron ejemplos de GDFRs para $(g, U) \in \{(1, 5), (1, 6), (2, 2)\}$.

Para la familia v), los autores de [**2**] identificaron un ejemplo con valores repetidos en R y S para $g = 2$, $U = 2$. Este caso puede interpretarse como multidigrafos fuertemente regulares. El ejemplo encontrado es el siguiente:

$$Q = \{2, 3, 4, 8, 9, 10\}, \qquad R = \{1, 2, 3, 6, 6, 7, 8, 9\},$$
$$S = \{3, 4, 5, 6, 6, 9, 10, 11\}, \qquad T = \{2, 3, 4, 8, 9, 10\}.$$

En relación con la familia vi), Leung y Ma proporcionaron un ejemplo en [**79**] para $g = 2$, $U = 0$ (el caso no dirigido). Aparte de esta CSP, los únicos ejemplos identificados son aquellos en los que $g = 1$ y U puede tomar cualquier valor arbitrario. En estos casos, los parámetros de los GDFRs coinciden con la misma forma que se describe en el Teorema 1 del artículo [**65**] de Jørgensen.

Con respecto a la familia vii), Leung y Ma presentaron en [**79**] un ejemplo para $g = 2$, $U = 0$ (el caso no dirigido). Para el signo más, los autores de [**89**] descubrieron una FSP cuyo complemento proporciona un ejemplo para $g = 2$, $U = 6$. Para el signo menos, los autores de [**2**] identificaron los siguientes ejemplos:

- $g = 1, U = 2 : Q = \{0, 3\}, R = \{2, 3, 5\}, S = \{1, 3, 4\}, T = \{0, 3\}$.
- $g = 1, U = 4 : Q = \{0, 1, 5, 6\}, R = \{1, 4, 5, 6, 9\}, S = \{2, 3, 5, 7, 8\}, T = \{1, 3, 6, 8\}$.
- $g = 1, U = 6 : Q = \{0, 4, 6, 7, 11, 13\}, R = \{1, 3, 6, 7, 8, 10, 13\}, S = \{2, 4, 5, 7, 9, 11, 12\}$, $T = \{1, 4, 6, 8, 11, 13\}$.

En lo que respecta a la familia viii), se han descubierto ejemplos de CSPs en [**89**] para $g = 2$ con el signo negativo, así como el complemento para $g = 2$ con el signo positivo. Sin embargo, es importante destacar que estos ejemplos no eran circulantes. Hasta el momento, no se han encontrado ejemplos circulantes dentro de esta familia.

El objetivo principal en este capítulo es completar el trabajo realizado por los autores de [**2**] obteniendo CSPs con parámetros con la forma de la familia vii), con el signo menos, $g = 1$ y U un número par.

A continuación daremos una construcción de CSPs con parámetros con la forma de la familia vii) del Teorema 2.6 con el signo menos, para $g = 1$ y U un número par arbitrario. Este resultado es producto de la investigación realizada en el trabajo de fin de máster de mi autoría.

TEOREMA 2.7. *Sea $U > 4$ un número par (digamos $U = 2r$, con $r > 2$ un entero). Entonces (Q, R, S, T) es una cuádrupla de sumas parciales, donde*

$$\begin{aligned} Q &= \{0, 1, r+3, r+4, ..., 2r, 2r+1, 2r+2, 3r+4, 3r+5, ..., 4r+1\}, \\ R &= \{1, 2, ..., r, 2r+1, 2r+2, .., 3r+1\}, \\ S &= \{r+1, ..., 2r, 2r+1, 3r+2, ..., 4r+1\}, \\ T &= \{0, 1, 2, ..., r-2, 2r, 2r+1, ..., 3r-1, 4r+1\}. \end{aligned}$$

DEMOSTRACIÓN. Nótese que en este caso $\beta = 0$, $\gamma = 1$ y $\mu = 2r$. Entonces debemos probar que

1) $R^2 + QT = \{e\} + 2rH$,
2) $T(R + S) = 2rH$,
3) $Q(R + S) = 2rH$,
4) $S^2 + QT = \{e\} + 2rH$,

donde $H = (\mathbb{Z}_n, +)$ es el grupo cíclico de orden $n = 4r + 2$ y e es el elemento identidad de H. Durante toda la prueba, los cálculos se harán módulo $4r + 2$, pero se omitirá en la notación para simplificar la escritura.

Para probar esto, necesitamos hacer una descripción de $e + 2rH$ y $2rH$; esto implica saber cuántas veces aparece cada número entre 0 y $4r + 1$ en $e + 2rH$ y $2rH$. Podemos

observar que $2rH$ contiene $2r$ veces cada elemento entre 0 y $4r+1$. De la misma manera, $e+2rH$ contiene $2r+1$ veces el elemento 0 y $2r$ veces cada elemento entre 1 y $4r+1$.

Por lo tanto, en 1) debemos probar que en R^2+QT, 0 aparece $2r+1$ veces, y cada elemento entre 1 y $4r+1$ aparece $2r$ veces. En 2) debemos probar que cada elemento entre 0 y $4r+1$ aparece $2r$ veces en $T(R+S)$ (o sea, en $TR+TS$). En 3) debemos probar que cada elemento entre 0 y $4r+1$ aparece $2r$ veces en $Q(R+S)$ (o sea, en $QR+QS$). Finalmente en 4) debemos demostrar que en S^2+QT, 0 aparece $2r+1$ veces, y cada elemento entre 1 y $4r+1$ aparece $2r$ veces.

Veamos 1):

En este ítem analizamos R^2 y QT por separado para finalmente analizar R^2+QT.

Nótese que

$$R^2 \ = \{a+1, a+2, ..., a+r, a+2r+1, a+2r+2, ..., a+3r+1 \ : \ a \in R\} = \bigcup_{i=1}^{3} R_i,$$

donde

- R_1 es la parte de R^2 donde a varía entre 1 y r.
- R_2 es la parte de R^2 donde $a = 2r+1$.
- R_3 es la parte de R^2 donde a varía entre $2r+2$ y $3r+1$.

Nótese que, reorganizando los elementos, podemos escribir R_1 como

$$R_1 = \left\{ 2, 3, 3, 4, 4, 4, 5, 5, 5, 5, ..., \overbrace{r+1, r+1, ..., r+1}^{r \text{ veces}}, \overbrace{r+2, ..., r+2}^{r-1 \text{ veces}}, \right.$$
$$..., 2r-1, 2r-1, 2r, 2r+2, 2r+3, 2r+3, ..., \overbrace{3r+1, 3r+1, ..., 3r+1}^{r \text{ veces}},$$
$$\left. \overbrace{3r+2, ..., 3r+2}^{r \text{ veces}}, \overbrace{3r+3, ..., 3r+3}^{r-1 \text{ veces}}, ..., 4r, 4r, 4r+1 \right\}.$$

Para R_2 y R_3 obtenemos una expresión similar

$$R_2 = \ \{2r+2, 2r+3, ..., 3r+1, 0, 1, 2, ..., r\}.$$
$$R_3 = \left\{ 1, 2, 2, 3, 3, 3, ..., \overbrace{r, r, ..., r}^{r \text{ veces}}, \overbrace{r+1, r+1, ..., r+1}^{r \text{ veces}}, \overbrace{r+2, ..., r+2}^{r-1 \text{ veces}}, ..., 2r-1, \right.$$
$$2r-1, 2r, 2r+3, 2r+4, 2r+4, ..., \overbrace{3r+2, 3r+2, ..., 3r+2}^{r \text{ veces}},$$
$$\left. \overbrace{3r+3, ..., 3r+3}^{r-1 \text{ veces}}, ..., 4r, 4r, 4r+1 \right\}.$$

TABLA 2.1. Número de elementos en $\mathbf{R_1}$, $\mathbf{R_2}$ y $\mathbf{R_3}$

Elementos	**Veces en** $\mathbf{R_1}$
0, 1	0
2	1
3	2
⋮	⋮
$r+1$	r
$r+2$	$r-1$
$r+3$	$r-2$
⋮	⋮
$2r$	1
$2r+1$	0
$2r+2$	1
⋮	⋮
$3r+1$	r
$3r+2$	r
$3r+3$	$r-1$
$3r+4$	$r-2$
⋮	⋮
$4r+1$	1

Elementos	**Veces en** $\mathbf{R_3}$
0	0
1	1
⋮	⋮
r	r
$r+1$	r
$r+2$	$r-1$
$r+3$	$r-2$
⋮	⋮
$2r$	1
$2r+1$, $2r+2$	0
$2r+3$	1
$2r+4$	2
⋮	⋮
$3r+2$	r
$3r+3$	$r-1$
$3r+4$	$r-2$
⋮	⋮
$4r+1$	1

Elementos	**Veces en** $\mathbf{R_2}$
0, 1, ..., r	1
$r+1$, $r+2$, ..., $2r+1$	0
$2r+2$, $2r+3$, ..., $3r+1$	1
$3r+2$, $3r+3$, ..., $4r+1$	0

En la Tabla 2.1 podemos observar la cantidad de veces que aparece cada elemento en R_i, con $i = 1, 2, 3$.

Ahora analicemos el conjunto QT. Nótese que

$$QT = \{a, a+1, ..., a+r-2, a+2r, a+2r+1, ..., a+3r-1, a+4r+1 \ : \ a \in Q\} = \bigcup_{i=1}^{4} QT_i,$$

donde

- QT_1 es la parte de QT donde $a = 0$ y $a = 1$.
- QT_2 es la parte de QT donde a varía entre $r+3$ y $2r$.
- QT_3 es la parte de QT donde $a = 2r+1$ y $a = 2r+2$.
- QT_4 es la parte de QT donde a varía entre $3r+4$ y $4r+1$.

Nósete que, reorganizando los elementos, podemos escribir QT_1, QT_2, QT_3 y QT_4 como

$$\begin{aligned} QT_1 = \ & \{0,0,1,1,2,2,3,3,...,r-2,r-2,r-1,2r,2r+1,2r+1,2r+2,2r+2,..., \\ & 3r-1,3r-1,3r,4r+1\}. \end{aligned}$$

$$\begin{aligned} QT_2 = \ & \Big\{\overbrace{0,0,...,0}^{r-2 \text{ veces}},\overbrace{1,...,1}^{r-3 \text{ veces}},...,r-4,r-4,r-3,r+2,r+3,r+3,...,\overbrace{2r-1,...,2r-1}^{r-2 \text{ veces}}, \\ & \overbrace{2r,...,2r}^{r-2 \ times},\overbrace{2r+1,...,2r+1}^{r-2 \ times},\overbrace{2r+2,...,2r+2}^{r-3 \text{ veces}},...,3r-3,3r-3,3r-2,3r+3, \\ & 3r+4,3r+4,...,\overbrace{4r,...,4r}^{r-2 \text{ veces}},\overbrace{4r+1,...,4r+1}^{r-2 \text{ veces}}\Big\}. \end{aligned}$$

$$\begin{aligned} QT_3 = \ & \{0,0,1,1,2,2,...,r-2,r-2,r-1,2r,2r+1,2r+1,2r+2,2r+2,..., \\ & 3r-1,3r-1,3r,4r+1\}. \end{aligned}$$

$$\begin{aligned} QT_4 = \ & \Big\{\overbrace{0,0,...,0}^{r-2 \text{ veces}},\overbrace{1,1,...,1}^{r-3 \text{ veces}},...,r-4,r-4,r-3,r+2,r+3,r+3,...,\overbrace{2r-1,...,2r-1}^{r-2 \text{ veces}}, \\ & \overbrace{2r,...,2r}^{r-2 \text{ veces}},\overbrace{2r+1,...,2r+1}^{r-2 \text{ veces}},\overbrace{2r+2,...,2r+2}^{r-3 \text{ veces}},\overbrace{2r+3,...,2r+3}^{r-4 \text{ veces}},...,3r-3, \\ & 3r-3,3r-2,3r+3,3r+4,3r+4,...,\overbrace{4r,...,4r}^{r-2 \text{ veces}},\overbrace{4r+1,...,4r+1}^{r-2 \text{ veces}}\Big\}. \end{aligned}$$

En la Tabla 2.2, podemos observar el número de veces que aparece cada elemento de $\mathbb{Z}_{4r+2}$ en QT_i, con $i = 1, 2, 3, 4$.

Sumando los valores de las Tablas 2.1 y 2.2, podemos ver en la Tabla 2.3 la cantidad de veces que aparece cada elemento en QT y en R^2.

Finalmente, uniendo los resultados obtenidos para R^2 y QT, obtenemos que en $R^2 + QT$, 0 aparece $2r + 1$ veces y todos los elementos entre 1 y $4r + 1$ aparecen $2r$ veces, lo que demuestra que se cumple la condición 1).

Ahora, veamos la condición 2).

En este ítem primero analizamos $R + S$ para finalmente analizar $T(R + S)$.

Nótese que

$$R + S = \{1, 2, ..., r, 2r + 1, 2r + 2, ..., 3r + 1, r + 1, ..., 2r, 2r + 1, 3r + 2, ..., 4r + 1\}.$$

Reorganizando los elementos, tenemos

$$R + S = \{1, 2, ..., 2r, 2r + 1, 2r + 1, 2r + 2, ..., 4r + 1\}.$$

TABLA 2.2. Número de elementos en QT_1, QT_2, QT_3 y QT_4

Elementos	**Veces en QT_1**
$0, 1, \ldots, r-2$	2
$r-1$	1
$r, r+1, \ldots, 2r-1$	0
$2r$	1
$2r+1, 2r+2 \ldots, 3r-1$	2
$3r$	1
$3r+1, 3r+2, \ldots, 4r$	0
$4r+1$	1

Elementos	**Veces en QT_3**
$0, 1, \ldots, r-2$	2
$r-1$	1
$r, r+1, \ldots, 2r-1$	0
$2r$	1
$2r+1, 2r+2, \ldots, 3r-1$	2
$3r$	1
$3r+1, 3r+2, \ldots, 4r$	0
$4r+1$	1

Elementos	**Veces en QT_2**
0	$r-2$
1	$r-3$
$\vdots$	$\vdots$
$r-3$	1
$r-2, r-1 \ldots, p+1$	0
$r+2$	1
$r+3$	2
$\vdots$	$\vdots$
$2r-1$	$r-2$
$2r, 2r+1$	$r-2$
$2r+2$	$r-3$
$\vdots$	$\vdots$
$3r-2$	1
$3r-1, 3r, \ldots, 3r+2$	0
$3r+3$	1
$3r+4$	2
$\vdots$	$\vdots$
$4r, 4r+1$	$r-2$

Elementos	**Veces en QT_4**
0	$r-2$
1	$r-3$
$\vdots$	$\vdots$
$r-3$	1
$r-2, r-1 \ldots, r+1$	0
$r+2$	1
$r+3$	2
$\vdots$	$\vdots$
$2r-1$	$r-2$
$2r, 2r+1$	$r-2$
$2r+2$	$r-3$
$\vdots$	$\vdots$
$3r-2$	1
$3r-1, 3r, \ldots, 3r+2$	0
$3r+3$	1
$3r+4$	2
$\vdots$	$\vdots$
$4r, 4r+1$	$r-2$

Entonces, obtenemos que en $R+S$ nunca aparece 0, todo elemento entre 1 y $2r$ y todo elemento entre $2r+2$ y $4r+1$ aparece una vez y $2r+1$ aparece dos veces.

Ahora, nótese que

$$T(R+S) = \{a+1, a+2, ..., a+2r, a+2r+1, a+2r+1, a+2r+2, ..., a+4r+1 \ : \ a \in T\} = \bigcup_{i=1}^{4} T_i,$$

donde

- T_1 es la parte de $T(R+S)$ cuando a varía entre 0 y $r-2$.

TABLA 2.3. Número de elementos en R^2 y QT

Elementos	**Veces en $\mathbf{R^2}$**
0	**1**
1	**2**
2	**4**
$\vdots$	$\vdots$
r	$2r$
$r+1$	$2r$
$r+2$	$2r-2$
$r+3$	$2r-4$
$\vdots$	$\vdots$
$2r$	**2**
$2r+1$	**0**
$2r+2$	**2**
$2r+3$	**4**
$\vdots$	$\vdots$
$3r+1$	$2r$
$3r+2$	$2r$
$3r+3$	$2r-2$
$3r+4$	$2r-4$
$\vdots$	$\vdots$
$4r+1$	**2**

Elementos	**Veces en QT**
0	$2r$
1	$2r-2$
2	$2r-4$
$\vdots$	$\vdots$
r	**0**
$r+1$	**0**
$r+2$	2
$r+3$	**4**
$\vdots$	$\vdots$
$2r+1$	$2r$
$2r+2$	$2r-2$
$2r+3$	$2r-4$
$\vdots$	$\vdots$
$3r+1$	**0**
$3r+2$	**0**
$3r+3$	**2**
$3r+4$	**4**
$\vdots$	$\vdots$
$4r+1$	$2r-2$

- T_2 **es la parte de** $T(R+S)$ **cuando** $a = 2r$.
- T_3 **es la parte de** $T(R+S)$ **cuando** a **varía entre** $2r+1$ **y** $3r-1$.
- T_4 **es la parte de** $T(R+S)$ **cuando** $a = 4r+1$.

Nótese que, reorganizando los elementos, se pueden escribir T_1, T_2, T_3 **y** T_4 **como**

$$T_1 = \left\{ \overbrace{0,...,0}^{r-2 \text{ veces}}, \overbrace{1,...,1}^{r-2 \text{ veces}}, ..., \overbrace{r-2,...,r-2}^{r-2 \text{ veces}}, \overbrace{r-1,...,r-1}^{r-1 \text{ veces}}, \overbrace{r,...,r}^{r-1 \text{ veces}}, ..., \overbrace{2r,...,2r}^{r-1 \text{ veces}}, \overbrace{2r+1,...,2r+1}^{r \text{ veces}}, \right.$$
$$\left. \overbrace{2r+2,...,2r+2}^{r \text{ veces}}, ..., \overbrace{3r-1,...,3r-1}^{r \text{ veces}}, \overbrace{3r,...,3r}^{r-1 \text{ veces}}, \overbrace{3r+1,...,3r+1}^{r-1 \text{ veces}}, ..., \overbrace{4r+1,...,4r+1}^{r-1 \text{ veces}} \right\}.$$

$$T_2 = \{0, 1, ..., 2r-1, 2r+1, 2r+2, ..., 4r, 4r+1, 4r+1\}.$$

$$T_3 = \left\{ \overbrace{0,0,...,0}^{r \text{ veces}}, \overbrace{1,1,...,1}^{r \text{ veces}}, ..., \overbrace{r-2,...,r-2}^{r \text{ veces}}, \overbrace{r-1,...,r-1}^{r-1 \text{ veces}}, \overbrace{r,...,r}^{r-1 \text{ veces}}, ..., \overbrace{2r,...,2r}^{r-1 \text{ veces}}, \overbrace{2r+1,...,2r+1}^{r-2 \text{ veces}}, \right.$$
$$\left. \overbrace{2r+2,...,2r+2}^{r-2 \text{ veces}}, ..., \overbrace{3r-1,...,3r-1}^{r-2 \text{ veces}}, \overbrace{3r,...,3r}^{r-1 \text{ veces}}, \overbrace{3r+1,...,3r+1}^{r-1 \text{ veces}}, ..., \overbrace{4r+1,...,4r+1}^{r-1 \text{ veces}} \right\}.$$

$$T_4 = \{0, 1, ..., 2r-1, 2r, 2r, 2r+1, ..., 4r\}.$$

En la Tabla 2.4, podemos observar las veces que aparece cada elemento en T_i, con $i = 1, 2, 3, 4$. Juntando estos cuatro casos, concluimos que todo elemento entre 0 y $4r + 1$ aparece $2r$ veces en $T(R + S)$, lo que prueba que se cumple la condición 2).

TABLA 2.4. Número de elementos en T_1, T_2, T_3 y T_4

Elementos	**Veces en T_1**
0, 1, ..., $r-2$	$r-2$
$r-1$, r, ..., $2r$	$r-1$
$2r+1$, ..., $3r-1$	r
$3r$, ..., $4r+1$	$r-1$

Elementos	**Veces en T_3**
0, 1, ..., $r-2$	r
$r-1$, r, ..., $2r$	$r-1$
$2r+1$, ..., $3r-1$	$r-2$
$3r$, ..., $4r+1$	$r-1$

Elementos	**Veces en T_2**
0, 1, ..., $2r-1$	1
$2r$	0
$2r+1$, ..., $4r$	1
$4r+1$	2

Elementos	**Veces en T_4**
0, 1, ..., $2r-1$	1
$2r$	2
$2r+1$, ..., $4r$	1
$4r+1$	0

Veamos la condición 3):

Como en la condición 2) ya obtuvimos $R + S$, solo tenemos que analizar directamente $Q(R + S)$.

Nótese que podemos escribir $Q(R + S)$ como

$$Q(R+S) = \{a+1, a+2, ..., a+2r, a+2r+1, a+2r+1, a+2r+2, ..., a+4r+1 \ : \ a \in Q\} = \bigcup_{i=1}^{4} Q_i,$$

donde

- Q_1 es la parte de $Q(R + S)$ cuando $a = 0$ y $a = 1$.
- Q_2 es la parte $Q(R + S)$ cuando a varía entre $r + 3$ y $2r$.
- Q_3 es la parte de $Q(R + S)$ cuando $a = 2r + 1$ y $a = 2r + 2$.
- Q_4 es la parte de $Q(R + S)$ cuando a varía entre $3r + 4$ y $4r + 1$.

Nótese que, reorganizando los elementos, se pueden escribir Q_1, Q_2, Q_3 y Q_4 como

$$\begin{aligned} Q_1 = \; & \{0,1,2,2,3,3,...,2r,2r,2r+1,2r+1,2r+1,2r+2,2r+2,2r+2,2r+3,\\ & 2r+3,2r+4,2r+4,...,4r+1,4r+1\}. \end{aligned}$$

$$\begin{aligned} Q_2 = \; & \Big\{ \overbrace{0,0,...,0}^{r-2 \text{ times}}, \overbrace{1,1,...,1}^{r-2 \text{ veces}}, ..., \overbrace{r+2,...,r+2}^{r-2 \text{ veces}}, \overbrace{r+3,...,r+3}^{r-3 \text{ veces}}, \overbrace{r+4,...,r+4}^{r-3 \text{ veces}}, ..., \\ & \overbrace{2r,...,2r}^{r-3 \text{ veces}}, \overbrace{2r+1,...,2r+1}^{r-2 \text{ veces}}, \overbrace{2r+2,...,2r+2}^{r-2 \text{ veces}}, ..., \overbrace{3r+3,...,3r+3}^{r-2 \text{ veces}}, \\ & \overbrace{3r+4,...,3r+4}^{r-1 \text{ veces}}, \overbrace{3r+5,...,3r+5}^{r-1 \text{ veces}}, ..., \overbrace{4r+1,...,4r+1}^{r-1 \text{ veces}} \Big\}. \end{aligned}$$

$$\begin{aligned} Q_3 = \; & \{0,0,0,1,1,1,2,2,3,3,...,2r,2r,2r+1,2r+2,2r+3,2r+3,2r+4,\\ & 2r+4,...,4r+1,4r+1\}. \end{aligned}$$

$$\begin{aligned} Q_4 = \; & \Big\{ \overbrace{0,0,...,0}^{r-2 \text{ veces}}, \overbrace{1,1,...,1}^{r-2 \text{ veces}}, ..., \overbrace{r+2,...,r+2}^{r-2 \text{ veces}}, \overbrace{r+3,...,r+3}^{r-1 \text{ veces}}, \overbrace{r+4,...,r+4}^{r-1 \text{ veces}}, ..., \\ & \overbrace{2r,...,2r}^{r-1 \text{ veces}}, \overbrace{2r+1,...,2r+1}^{r-2 \text{ veces}}, \overbrace{2r+2,...,2r+2}^{r-2 \text{ veces}}, ..., \overbrace{3r+3,...,3r+3}^{r-2 \text{ veces}}, \\ & \overbrace{3r+4,...,3r+4}^{r-3 \text{ veces}}, \overbrace{3r+5,...,3r+5}^{r-3 \text{ veces}}, ..., \overbrace{4r+1,...,4r+1}^{r-3 \text{ veces}} \Big\}. \end{aligned}$$

En la Tabla 2.5 podemos observar las veces que aparece cada elemento en Q_i, siendo $i = 1,2,3,4$. Juntando estos cuatro casos, concluimos que todo elemento entre 0 y $4r+1$ aparece $2r$ veces en $Q(R+S)$, lo que prueba que se cumple la condición 3).

TABLA 2.5. Número de elementos en Q_1, Q_2, Q_3 y Q_4

Elementos	**Veces en Q_1**
0, 1	1
2, 3, ..., $2r$	2
$2r+1$, $2r+2$	3
$2r+3$, ..., $4r+1$	2

Elementos	**Veces en Q_3**
0, 1	3
2, 3, ..., $2r$	2
$2r+1$, $2r+2$	1
$2r+3$, ..., $4r+1$	2

Elementos	**Veces en Q_2**
0, 1, ..., $r+2$	$r-2$
$r+3$, $r+4$, ..., $2r$	$r-3$
$2r+1$, ..., $3r+3$	$r-2$
$3r+4$, ..., $4r+1$	$r-1$

Elementos	**Veces en Q_4**
0, 1, ..., $r+2$	$r-2$
$r+3$, $r+4$, ..., $2r$	$r-1$
$2r+1$, ..., $3r+3$	$r-2$
$3r+4$, ..., $4r+1$	$r-3$

Finalmente, verifiquemos la condición 4).

Ya que en la condición 1) hicimos $R^2 + QT$ y en este caso debemos hacer $S^2 + QT$, sabiendo que se debe cumplir $R^2 + QT = S^2 + QT$, basta con calcular S^2 y ver que todos los elementos aparecen el mismo número de veces en S^2 y en R^2.

Nótese que

$$S^2 = \{a + r + 1, a + r + 2, ..., a + 2r, a + 2r + 1, a + 3r + 2, ..., a + 4r + 1 \ : \ a \in S\} = \bigcup_{i=1}^{3} S_i$$

donde

- S_1 es la parte de S^2 cuando a varía entre $r + 1$ y $2r$.
- S_2 es la parte de S^2 cuando $a = 2r + 1$.
- S_3 es la parte de S^2 cuando a varía entre $3r + 2$ y $4r + 1$.

Nótese que, reorganizando los elementos, se pueden escribir S_1, S_2 y S_3 como

$$\begin{aligned} S_1 = \ & \Big\{ 1, 2, 2, 3, 3, 3, ..., \overbrace{r, ..., r}^{r \text{ veces}}, \overbrace{r + 1, ..., r + 1}^{r-1 \text{ veces}}, \overbrace{r + 2, ..., r + 2}^{r-2 \text{ veces}}, ..., 2r - 2, 2r - 2, \\ & 2r - 1, 2r + 2, 2r + 3, 2r + 3, ..., \overbrace{3r + 1, ..., 3r + 1}^{r \text{ veces}}, \overbrace{3r + 2, ..., 3r + 2}^{r \text{ veces}}, \\ & \overbrace{3r + 3, ..., 3r + 3}^{r-1 \text{ veces}}, \overbrace{3r + 4, ..., 3r + 4}^{r-2 \text{ veces}}, ..., 4r, 4r, 4r + 1 \Big\}. \end{aligned}$$

$$S_2 = \ \{0, r + 1, r + 2..., 2r, 3r + 2, 3r + 3, ..., 4r + 1\}$$

.

$$\begin{aligned} S_3 = \ & \Big\{ 1, 2, 2, 3, 3, 3, ..., \overbrace{r, ..., r}^{r \text{ veces}}, \overbrace{r + 1, ..., r + 1}^{r \text{ veces}}, \overbrace{r + 2, ..., r + 2}^{r-1 \text{ veces}}, \overbrace{r + 3, ..., r + 3}^{r-2 \text{ veces}}, ..., \\ & 2r - 1, 2r - 1, 2r, 2r + 2, 2r + 3, 2r + 3, ..., \overbrace{3r + 1, ..., 3r + 1}^{r \text{ veces}}, \overbrace{3r + 2, ..., 3r + 2}^{r-1 \text{ veces}}, \\ & \overbrace{3r + 3, ..., 3r + 3}^{r-2 \text{ veces}}, ..., 4r - 1, 4r - 1, 4r \Big\}. \end{aligned}$$

En la Tabla 2.6, podemos observar las veces que aparece cada elemento en S_i, con $i = 1, 2, 3$.

TABLA 2.6. Número de elementos en S_1, S_2 y S_3

Elementos	**Veces en S_1**
0	0
1	1
⋮	⋮
r	r
$r+1$	$r-1$
$r+2$	$r-2$
⋮	⋮
$2r-1$	1
$2r$, $2r+1$	0
$2r+2$	1
$2r+3$	2
⋮	⋮
$3r+1$	r
$3r+2$	r
$3r+3$	$r-1$
$3r+4$, $3r+5$, …, $4r$	$r-2$
$4r+1$	1

Elementos	**Veces en S_3**
0	0
1	1
⋮	⋮
r	r
$r+1$	r
$r+2$	$r-1$
⋮	⋮
$2r$	1
$2r+1$	0
$2r+2$	1
$2r+3$	2
⋮	⋮
$3r+1$	r
$3r+2$	$r-1$
$3r+3$	$r-2$
$4r$	1
$4r+1$	0

Elementos	**Veces en S_2**
0	1
1, 2, …, r	0
$r+1$, $r+2$, …, $2r$	1
$2r+1$, $2r+2$, …, $3r+1$	0
$3r+2$, $3r+3$, …, $4r+1$	1

Juntando estos tres casos, tenemos que todos los elementos aparecen el mismo número de veces en S^2 y en R^2, por tanto, en $S^2 + QT$, 0 aparece $2r+1$ veces y todos los elementos entre 1 y $4r+1$ aparecen $2r$ veces, lo que concluye la demostración del teorema. ■

La siguiente tabla muestra algunas cuádruplas de sumas parciales de diferentes tamaños, que obtendremos usando el Teorema 2.7. Usando el software GAP ([**61**]), calculamos el grupo de automorfismos del digrafo asociado a cada CSP. A partir de esto, se conjeturó en mi Trabajo de Fin de Master una forma general para deducir cuántos elementos son necesarios para generar el grupo y el orden del grupo. Dicha conjetura se trabajó posteriormente y finalmente se demostró. Esto se verá reflejado en el siguiente capítulo de esta tesis.

En la Tabla 2.7, $|G|$ es el orden del grupo de automorfismos asociados a la CSP y $|g|$ es el número de generadores del grupo.

TABLA 2.7. Cuádruplas de sumas parciales construidas

U	**Símbolo (Q,R,S,T)**	|g|	|G|
6	({0,1,6,7,8,13},{1,2,3,7,8,9,10}, {4,5,6,7,11,12,13},{0,1,6,7,8,13})	15	14×2^{14}
8	({0,1,7,8,9,10,16,17},{1,2,3,4,9,10,11,12,13}, {5,6,7,8,9,14,15,16,17},{0,1,2,8,9,10,11,17})	19	18×2^{18}
10	({0,1,8,9,10,11,12,19,20,21}, {1,2,3,4,5,11,12,13,14,15,16}, {6,7,8,9,10,11,17,18,19,20,21}, {0,1,2,3,10,11,12,13,14,21})	23	22×2^{22}
12	({0,1,9,10,11,12,13,14,22,23,24,25}, {1,2,3,4,5,6,13,14,15,16,17,18,19}, {7,8,9,10,11,12,13,20,21,22,23,24,25}, {0,1,2,3,4,12,13,14,15,16,17,25})	27	26×2^{26}

Con base en los ejemplos de la Tabla 2.7 obtenidos del Teorema 2.7 podemos intuir que el grupo de automorfimos asociado a cada familia es de orden $(4r + 2) \times 2^{4r+2}$ y que además, este grupo tiene $4r + 3$ generadores. Este es un resultado que se demostrará con todo detalle en el siguiente capítulo de esta tesis, y que fue objeto de estudió de un artículo posterior ([**38**]).

A modo de ilustración construyamos la matriz de adyacencia del grafo obtenido para el caso $U = 6$ en la Tabla 2.7.

El bloque correspondiente a $R = \{1, 2, 3, 7, 8, 9, 10\}$ se construye de la siguiente manera:

De acuerdo con la expresión (1.1), si indexamos cada columna con $0, 1, 2, \ldots, 13$, se tiene que en la primera fila, la entrada será 1 en las posiciones 1, 2, 3, 7, 8, 9 y 10. En el resto de posiciones la entrada será 0.

Las demás filas se construyen de forma recursiva donde el elemento i de la fila será el elemento $(i - 1) \mod 14$ de la fila anterior.

Se tiene entonces que dicho bloque es

$$\begin{pmatrix}
0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\
1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\
1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\
1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\
0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\
1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\
1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\
1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0
\end{pmatrix}.$$

De forma similar, se tiene que el bloque correspondiente a $Q = \{0, 1, 6, 7, 8, 13\}$ es

$$\begin{pmatrix}
1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\
1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\
1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\
1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\
1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\
1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1
\end{pmatrix},$$

el bloque correspondiente a $T = \{0, 1, 6, 7, 8, 13\}$ es

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

y el bloque correspondiente a $S = \{4, 5, 6, 7, 11, 12, 13\}$ es

$$\begin{pmatrix}
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\
1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\
1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\
1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\
0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\
1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\
1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\
1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0
\end{pmatrix}.$$

Por lo tanto, la matriz de adyacencia del grafo construido es

$$\left(\begin{array}{cccccccccccccc|cccccccccccccc}
0&1&1&1&0&0&0&1&1&1&1&0&0&0&1&1&0&0&0&0&1&1&1&0&0&0&0&1\\
0&0&1&1&1&0&0&0&1&1&1&1&0&0&1&1&1&0&0&0&0&1&1&1&0&0&0&0\\
0&0&0&1&1&1&0&0&0&1&1&1&1&0&0&1&1&1&0&0&0&0&1&1&1&0&0&0\\
0&0&0&0&1&1&1&0&0&0&1&1&1&1&0&0&1&1&1&0&0&0&0&1&1&1&0&0\\
1&0&0&0&0&1&1&1&0&0&0&1&1&1&0&0&0&1&1&1&0&0&0&0&1&1&1&0\\
1&1&0&0&0&0&1&1&1&0&0&0&1&1&0&0&0&0&1&1&1&0&0&0&0&1&1&1\\
1&1&1&0&0&0&0&1&1&1&0&0&0&1&1&0&0&0&0&1&1&1&0&0&0&0&1&1\\
1&1&1&1&0&0&0&0&1&1&1&0&0&0&1&1&0&0&0&0&1&1&1&0&0&0&0&1\\
0&1&1&1&1&0&0&0&0&1&1&1&0&0&1&1&1&0&0&0&0&1&1&1&0&0&0&0\\
0&0&1&1&1&1&0&0&0&0&1&1&1&0&0&1&1&1&0&0&0&0&1&1&1&0&0&0\\
0&0&0&1&1&1&1&0&0&0&0&1&1&1&0&0&1&1&1&0&0&0&0&1&1&1&0&0\\
1&0&0&0&1&1&1&1&0&0&0&0&1&1&0&0&0&1&1&1&0&0&0&0&1&1&1&0\\
1&1&0&0&0&1&1&1&1&0&0&0&0&1&0&0&0&0&1&1&1&0&0&0&0&1&1&1\\
1&1&1&0&0&0&1&1&1&1&0&0&0&0&1&0&0&0&0&1&1&1&0&0&0&0&1&1\\
\hline
1&1&0&0&0&0&1&1&1&0&0&0&0&1&0&0&0&0&1&1&1&1&0&0&0&1&1&1\\
1&1&1&0&0&0&0&1&1&1&0&0&0&0&1&0&0&0&0&1&1&1&1&0&0&0&1&1\\
0&1&1&1&0&0&0&0&1&1&1&0&0&0&1&1&0&0&0&0&1&1&1&1&0&0&0&1\\
0&0&1&1&1&0&0&0&0&1&1&1&0&0&1&1&1&0&0&0&0&1&1&1&1&0&0&0\\
0&0&0&1&1&1&0&0&0&0&1&1&1&0&0&1&1&1&0&0&0&0&1&1&1&1&0&0\\
0&0&0&0&1&1&1&0&0&0&0&1&1&1&0&0&1&1&1&0&0&0&0&1&1&1&1&0\\
1&0&0&0&0&1&1&1&0&0&0&0&1&1&0&0&0&1&1&1&0&0&0&0&1&1&1&1\\
1&1&0&0&0&0&1&1&1&0&0&0&0&1&1&0&0&0&1&1&1&0&0&0&0&1&1&1\\
1&1&1&0&0&0&0&1&1&1&0&0&0&0&1&1&0&0&0&1&1&1&0&0&0&0&1&1\\
0&1&1&1&0&0&0&0&1&1&1&0&0&0&1&1&1&0&0&0&1&1&1&0&0&0&0&1\\
0&0&1&1&1&0&0&0&0&1&1&1&0&0&1&1&1&1&0&0&0&1&1&1&0&0&0&0\\
0&0&0&1&1&1&0&0&0&0&1&1&1&0&0&1&1&1&1&0&0&0&1&1&1&0&0&0\\
0&0&0&0&1&1&1&0&0&0&0&1&1&1&0&0&1&1&1&1&0&0&0&1&1&1&0&0\\
1&0&0&0&0&1&1&1&0&0&0&0&1&1&0&0&0&1&1&1&1&0&0&0&1&1&1&0
\end{array}\right).$$

Capítulo 3

UNA NUEVA CONSTRUCCIÓN DE GRAFOS DIRIGIDOS FUERTEMENTE REGULARES VÉRTICE-TRANSITIVOS

Un grafo (o digrafo) G se dice que es vértice-transitivo si para cualesquiera dos vértices v_1 y v_2 de G, existe un automorfismo del grafo que envía v_1 a v_2.

Por ejemplo, el grafo de Petersen

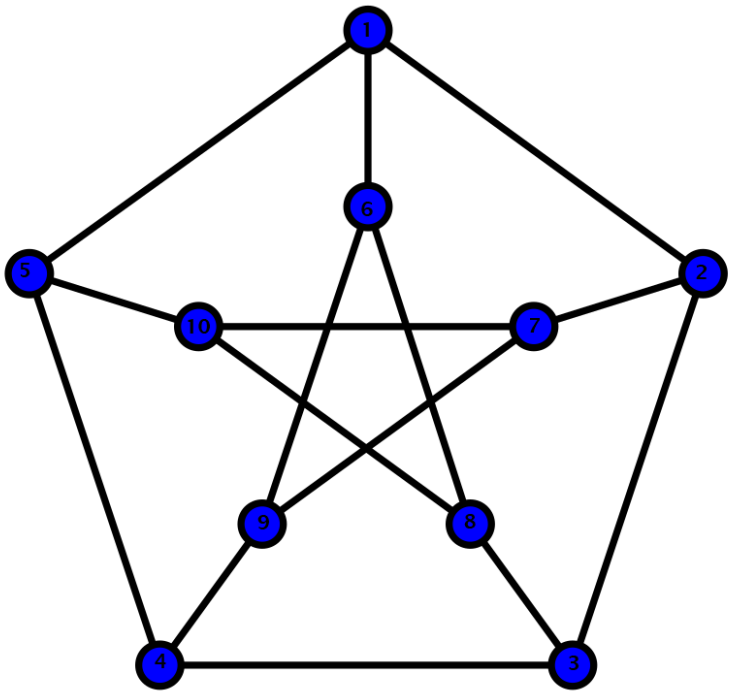

FIGURA 3.1. Grafo de Petersen

es vértice-transitivo. El grafo de Petersen, como se observa en la Figura 3.1, es un grafo no dirigido con 10 vértices y 15 aristas. Se trata de un grafo fuertemente regular de parámetros $v = 10$, $k = 5$, $\mu = 0$, $\lambda = 1$.

En la Figura 3.1 podemos observar que los vértices 1, 2, 3, 4, 5 son en cierto sentido equivalentes: están en el mismo "pentágono". De igual forma los vértices 6, 7, 8, 9, 10 cumplen está propiedad con el pentágono interior. El grupo completo de automorfismos del grafo de Petersen es el grupo simétrico S_5 ([**58**]).

En este capítulo se construye una familia infinita de grupos de permutaciones, a partir de la cual se obtienen dos familias infinitas de grafos dirigidos fuertemente regulares que serán bicirculantes y vértice-transitivos (véanse los Teoremas 3.3 y 3.5).

Sea $p \equiv 3 \mod 4$ un número primo.

Considérese el siguiente grupo de permutaciones sobre el conjunto $V_p = \left(\bigcup_{j\in\mathbb{Z}_2}\{x_{i,j} \mid i \in \mathbb{Z}_p\}\right) \cup \left(\bigcup_{j\in\mathbb{Z}_2}\{y_{i,j} \mid i \in \mathbb{Z}_p\}\right)$, donde los $x_{i,j}, y_{i,j}$ son expresiones formales para todo $(i, j) \in \mathbb{Z}_p \times \mathbb{Z}_2$:

$$G_p = \langle \alpha, \beta, \gamma_{0,0}, \gamma_{1,0}, \ldots, \gamma_{p-1,0}, \gamma_{0,1}, \gamma_{1,1}, \ldots, \gamma_{p-1,1}\rangle,$$

donde

$$\alpha = (x_{0,0}x_{1,0}\ldots x_{p-1,0}x_{0,1}x_{1,1}\ldots x_{p-1,1})(y_{0,0}y_{1,0}\ldots y_{p-1,0}y_{0,1}y_{1,1}\ldots y_{p-1,1}),$$

$$\beta = (x_{0,0}y_{0,0})(x_{0,1}y_{0,1})\prod_{i=1}^{p-1}(x_{i,0}y_{-i,1})\prod_{i=1}^{p-1}(x_{i,1}y_{-i,0}),$$

$$\gamma_{i,0} = (x_{i,0}x_{i,1}) \quad \text{y} \quad \gamma_{i,1} = (y_{i,0}y_{i,1}) \ \text{ para todo } \ i = 0, \ldots, p-1.$$

Ahora, si θ es una raíz primitiva módulo p, consideramos el grupo

$$G_p^* = \langle G_p, \delta\rangle$$

sobre V_p, donde

$$\begin{aligned}\delta = &(x_{1,0}x_{\theta^2,0}x_{\theta^4,0}\ldots x_{\theta^{p-3},0})(x_{\theta,0}x_{\theta^3,0}x_{\theta^5,0}\ldots x_{\theta^{p-2},0})\\ &(x_{1,1}x_{\theta^2,1}x_{\theta^4,1}\ldots x_{\theta^{p-3},1})(x_{\theta,1}x_{\theta^3,1}x_{\theta^5,1}\ldots x_{\theta^{p-2},1})\\ &(y_{1,0}y_{\theta^2,0}y_{\theta^4,0}\ldots y_{\theta^{p-3},0})(y_{\theta,0}y_{\theta^3,0}y_{\theta^5,0}\ldots y_{\theta^{p-2},0})\\ &(y_{1,1}y_{\theta^2,1}y_{\theta^4,1}\ldots y_{\theta^{p-3},1})(y_{\theta,1}y_{\theta^3,1}y_{\theta^5,1}\ldots y_{\theta^{p-2},1}).\end{aligned}$$

Cuando elegimos la acción de G_p^* sobre $V_p \times V_p$, podemos obtener el conjunto de órbitas $Orb(G_p^*)$ de pares en $V_p \times V_p$. Ahora bien, si elegimos la acción de G_p sobre cada órbita de $Orb(G_p^*)$ podemos obtener el conjunto de órbitas $\widehat{Orb(G_p^*)}$ de pares en $V_p \times V_p$, es decir, el conjunto de órbitas de la acción del grupo G_p en $V_p \times V_p$. Para todo $u, v \in V_p$, denotamos por $\overline{(u,v)}$ la órbita en $\widehat{Orb(G_p^*)}$ representada por (u,v). Ahora, consideraremos las siguientes dos familias de digrafos con conjunto de vértices V_p:

1. El digrafo $\widetilde{X}'_p$ cuyo conjunto de arcos es la unión de órbitas

$$\left(\bigcup_{i\in Q} \overline{(x_{0,0}, x_{i,0})}\right) \cup \left(\bigcup_{i\in Q} \overline{(x_{0,0}, y_{i,0})}\right).$$

2. El digrafo $\widetilde{X}''_p$ cuyo conjunto de órbitas es la unión de órbitas

$$\left(\bigcup_{i\in Q} \overline{(x_{0,0}, x_{i,0})}\right) \cup \{\overline{(x_{0,0}, x_{0,1})}\} \cup \left(\bigcup_{i\in Q} \overline{(x_{0,0}, y_{i,0})}\right).$$

Donde Q es el conjunto de cuadrados distintos de cero en $\mathbb{Z}_p$, esto es, $Q = \{1, \theta^2, \theta^4, \ldots, \theta^{p-3}\}$

Por construcción, el grupo G_p^* es un grupo de automorfismo tanto de $\widetilde{X}'_p$ como de $\widetilde{X}''_p$.

EJEMPLO 3.1. *Sea el cuerpo $\mathbb{Z}_3$ y un conjunto de vértices*

$$V_3 = \{x_{0,0}, x_{1,0}, x_{2,0}, x_{0,1}, x_{1,1}, x_{2,1}, y_{0,0}, y_{1,0}, y_{2,0}, y_{0,1}, y_{1,1}, y_{2,1}\}.$$

Tomamos el grupo de permutaciones sobre V_3 :

$$G_3 = \langle \alpha, \beta, (x_{0,0}x_{0,1}), (x_{1,0}x_{1,1}), (x_{2,0}x_{2,1}), (y_{0,0}y_{0,1}), (y_{1,0}y_{1,1}), (y_{2,0}y_{2,1})\rangle,$$

donde

$$\alpha = (x_{0,0}x_{1,0}x_{2,0}x_{0,1}x_{1,1}x_{2,1})(y_{0,0}y_{1,0}y_{2,0}y_{0,1}y_{1,1}y_{2,1}),$$

$$\beta = (x_{0,0}y_{0,0})(x_{0,1}, y_{0,1})(x_{1,0}y_{2,1})(x_{2,0}y_{1,1})(x_{1,1}y_{2,0})(x_{2,1}y_{1,0}).$$

En este ejemplo, podemos ver que $\theta = \overline{2}$ es la raíz primitiva módulo 3 y δ sería la permutación identidad, por lo que $G_3^* = G_3$.

Para ver el conjunto de arcos de $\widetilde{X}'_3$, debemos hallar las órbitas de la acción de G_3 sobre $V_3 \times V_3$. En particular, el conjunto de arcos es la unión entre la órbita $\overline{(x_{0,0}, x_{1,0})}$ y $\overline{(x_{0,0}, y_{1,0})}$. Se tiene que las órbitas son:

$$\begin{aligned}\overline{(x_{0,0},x_{1,0})} &= \{(x_{0,0},x_{1,0}),(x_{1,0},x_{2,0}),(y_{0,0},y_{2,1}),(x_{0,1},x_{1,0}),(x_{0,0},x_{1,1}),(x_{2,0},x_{0,1}),(y_{2,1},y_{1,1}),\\ &\quad (x_{1,1},x_{2,0}),(x_{1,0},x_{2,1}),(y_{1,0},y_{0,0}),(y_{0,1},y_{2,1}),(y_{0,0},y_{2,0}),(x_{0,1},x_{1,1}),(y_{1,1},y_{0,1}),\\ &\quad (x_{2,0},x_{0,0}),(x_{2,1},x_{0,1}),(y_{2,1},y_{1,0}),(y_{2,0},y_{1,1}),(x_{1,1},x_{2,1}),(y_{2,0},y_{1,0}),(x_{2,1},x_{0,0}),\\ &\quad (y_{1,0},y_{0,1}),(y_{1,1},y_{0,0}),(y_{0,1},y_{2,0})\}.\end{aligned}$$

$$\begin{aligned}\overline{(x_{0,0},y_{1,0})} &= \{(x_{0,0},y_{1,0}),(x_{1,0},y_{2,0}),(y_{0,0},x_{2,1}),(x_{0,1},y_{1,0}),(x_{0,0},y_{1,1}),(x_{2,0},y_{0,1}),(y_{2,1},x_{1,1}),\\ &\quad (x_{1,1},y_{2,0}),(x_{1,0},y_{2,1}),(y_{1,0},x_{0,0}),(y_{0,1},x_{2,1}),(y_{0,0},x_{2,0}),(x_{0,1},y_{1,1}),(y_{1,1},x_{0,1}),\\ &\quad (x_{2,0},y_{0,0}),(x_{2,1},y_{0,1}),(y_{2,1},x_{1,0}),(y_{2,0},x_{1,1}),(x_{1,1},y_{2,1}),(y_{2,0},x_{1,0}),(x_{2,1},y_{0,0}),\\ &\quad (y_{1,0},x_{0,1}),(y_{1,1},x_{0,0}),(y_{0,1},x_{2,0})\}.\end{aligned}$$

El conjunto de arcos será entonces $\overline{(x_{0,0},x_{1,0})} \cup \overline{(x_{0,0},y_{1,0})}$.

Tenemos que el digrafo $\widetilde{X}_3'$ *es aquel cuya matriz de adyacencia es*

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

Podemos ver que $\widetilde{X}_3'$ *es un grafo dirigido fuertemente regular. Para ello se puede observar que*

$$AJ = JA = \begin{pmatrix} 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 \end{pmatrix} = 4J$$

y que

$$A^2 = \begin{pmatrix} 2 & 0 & 2 & 2 & 0 & 2 & 2 & 0 & 2 & 2 & 0 & 2 \\ 2 & 2 & 0 & 2 & 2 & 0 & 2 & 2 & 0 & 2 & 2 & 0 \\ 0 & 2 & 2 & 0 & 2 & 2 & 0 & 2 & 2 & 0 & 2 & 2 \\ 2 & 0 & 2 & 2 & 0 & 2 & 2 & 0 & 2 & 2 & 0 & 2 \\ 2 & 2 & 0 & 2 & 2 & 0 & 2 & 2 & 0 & 2 & 2 & 0 \\ 0 & 2 & 2 & 0 & 2 & 2 & 0 & 2 & 2 & 0 & 2 & 2 \\ 2 & 2 & 0 & 2 & 2 & 0 & 2 & 2 & 0 & 2 & 2 & 0 \\ 0 & 2 & 2 & 0 & 2 & 2 & 0 & 2 & 2 & 0 & 2 & 2 \\ 2 & 0 & 2 & 2 & 0 & 2 & 2 & 0 & 2 & 2 & 0 & 2 \\ 2 & 2 & 0 & 2 & 2 & 0 & 2 & 2 & 0 & 2 & 2 & 0 \\ 0 & 2 & 2 & 0 & 2 & 2 & 0 & 2 & 2 & 0 & 2 & 2 \\ 2 & 0 & 2 & 2 & 0 & 2 & 2 & 0 & 2 & 2 & 0 & 2 \end{pmatrix} = 2I + 0A + 2(J - I - A)$$

Así, $\widetilde{X}_3'$ *es un grafo dirigido fuertemente regular con parámetros*

$$v = 12, \quad k = 4, \quad \mu = 2, \quad \lambda = 0, \quad t = 2.$$

Otra propiedad que podemos ver de este grafo es que es un bicirculante. Para analizar esto lo tomamos sobre $\mathbb{Z}_3 \times \{0,1\} = \{(0,0),(1,0),(2,0),(0,1),(1,1),(2,1)\}$.

Sean $S_{00} = \{(1,0),(1,1)\}$, $S_{01} = \{(1,0),(1,1)\}, S_{10} = \{(2,0),(2,1)\}$ *y* $S_{11} = \{(2,0),(2,1)\}$. *Podemos notar que* $\widetilde{X}'_3$ *es un* $BC_6[S_{00}, S_{01}, S_{10}, S_{11}]$.

Para construir el digrafo $\widetilde{X}''_3$, *además de las órbitas halladas para* $\widetilde{X}'_3$, *también necesitamos la órbita* $\overline{(x_{0,0}, x_{0,1})}$, *la cual es*

$$\begin{aligned}\overline{(x_{0,0}, x_{0,1})} &= \{(x_{0,0}, x_{0,1}), (x_{1,0}, x_{1,1}), (y_{0,0}, y_{0,1}), (x_{0,1}, x_{0,0}), (x_{2,0}, x_{2,1}), (y_{2,1}, y_{2,0}), (x_{1,1}, x_{1,0}),\\ &\quad (y_{1,0}, y_{1,1}), (y_{0,1}, y_{0,0}), (y_{1,1}, y_{1,0}), (y_{2,1}, x_{2,0}), (y_{2,0}, y_{2,1})\}.\end{aligned}$$

El conjunto de arcos de $\widetilde{X}''_3$ *es* $\overline{(x_{0,0}, x_{1,0})} \cup \overline{(x_{0,0}, x_{0,1})} \cup \overline{(x_{0,0}, y_{1,0})}$. *Así, la matriz de adyacencia de* $\widetilde{X}''_3$ *es*

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

Veamos que este grafo también es un grafo dirigido fuertemente regular. Se tiene que

$$BJ = JB = \begin{pmatrix} 5&5&5&5&5&5&5&5&5&5&5&5\\ 5&5&5&5&5&5&5&5&5&5&5&5\\ 5&5&5&5&5&5&5&5&5&5&5&5\\ 5&5&5&5&5&5&5&5&5&5&5&5\\ 5&5&5&5&5&5&5&5&5&5&5&5\\ 5&5&5&5&5&5&5&5&5&5&5&5\\ 5&5&5&5&5&5&5&5&5&5&5&5\\ 5&5&5&5&5&5&5&5&5&5&5&5\\ 5&5&5&5&5&5&5&5&5&5&5&5\\ 5&5&5&5&5&5&5&5&5&5&5&5\\ 5&5&5&5&5&5&5&5&5&5&5&5\\ 5&5&5&5&5&5&5&5&5&5&5&5 \end{pmatrix} = 5J.$$

Además,

$$B^2 = \begin{pmatrix} 3&2&2&2&2&2&2&2&2&2&2&2\\ 2&3&2&2&2&2&2&2&2&2&2&2\\ 2&2&3&2&2&2&2&2&2&2&2&2\\ 2&2&2&3&2&2&2&2&2&2&2&2\\ 2&2&2&2&3&2&2&2&2&2&2&2\\ 2&2&2&2&2&3&2&2&2&2&2&2\\ 2&2&2&2&2&2&3&2&2&2&2&2\\ 2&2&2&2&2&2&2&3&2&2&2&2\\ 2&2&2&2&2&2&2&2&3&2&2&2\\ 2&2&2&2&2&2&2&2&2&3&2&2\\ 2&2&2&2&2&2&2&2&2&2&3&2\\ 2&2&2&2&2&2&2&2&2&2&2&3 \end{pmatrix} = 3I + 2B + 2(J - I - B).$$

Por lo tanto, $\widetilde{X}_3''$ es un grafo dirigido fuertemente regular de parámetros

$$v = 12, \quad k = 5, \quad \mu = 2, \quad \lambda = 2, \quad t = 3.$$

También se puede analizar que este digrafo es bicirculante. Nuevamente, tomándolo sobre $\mathbb{Z}_3 \times \{0,1\}$, se tiene que si $S_{00} = \{(1,0),(0,1),(1,1)\}$, $S_{01} = \{(1,0),(1,1)\}$, $S_{10} = \{(2,0),(2,1)\}$ y $S_{11} = \{(2,0),(0,1),(2,1)\}$ entonces $\widetilde{X}_3''$ es un $BC_6[S_{00},S_{01},S_{10},S_{11}]$.

Estas propiedades estudiadas en este ejemplo son propiedades que se van a cumplir en general y que demostraremos a continuación.

TEOREMA 3.2. *El digrafo $\widetilde{X}'_p$ es el bicirculante $BC_{2p}[S, S, -S, -S]$, donde $S = (Q \times \{0\}) \cup (Q \times \{1\})$ y $Q = \{1, \theta^2, \ldots, \theta^{p-3}\}$. Es vértice-transitivo y su grupo de automorfismos es G^*_p.*

DEMOSTRACIÓN. En esta prueba y de aquí en adelante, denotaremos $Q_0 := Q \times \{0\}$, $Q_1 := Q \times \{1\}$. Además, $-Q_0 = (-Q) \times \{0\}$ y $-Q_1 = (-Q) \times \{0\}$, luego $-S = -Q_0 \cup -Q_1$.

En lo anterior, y en lo que resta de capítulo, el símbolo "$-$" no representa la diferencia conjuntista usual. Una expresión de la forma $A - B$ es el conjunto $\{a - b \ : \ a \in A, \ b \in B\}$. De forma similar, una expresión de la forma $A + B$ será el conjunto $\{a + b \ : \ a \in A, \ b \in B\}$. Para indicar la diferencia conjuntista usual entre los conjuntos A y B escribiremos $A \setminus B$.

Es obvio que $S_{00} = S$, $S_{01} = S$, $S_{10} = -S$ y $S_{11} = -S$, esto es, $\widetilde{X}'_p = BC_{2p}[S, S, -S, -S]$. Primero veamos que $\widetilde{X}'_p$ es un digrafo vértice-transitivo.

Podemos ver fácilmente que $\langle \alpha, \beta \rangle$ es un subgrupo transitivo de $\mathrm{Aut}(\widetilde{X}'_p)$ isomorfo al grupo diédrico D_{2p}. A continuación, podemos notar que

$$\Gamma = \langle \gamma_{i,j} \ : \ (i, j) \in \{0, 1, \ldots, p-1\} \times \{0, 1\} \rangle \cong \mathbb{Z}_2^{2p}.$$

Si $B_i = \{x_{i,0}, x_{p+i,0}\}$ y $\overline{B}_i = \{y_{i,0}, y_{p+i,0}\}$, entonces la partición

$$\mathcal{B} = \{B_i \ : \ i \in \{0, 1, \ldots, p-1\}\} \cup \{\overline{B}_i \ : \ i \in \{0, 1, \ldots, p-1\}\}$$

es una partición invariante del conjunto de vértices de $\widetilde{X}'_p$, dado que tanto los pares de vértices en B_i como los pares de vértices en $\overline{B}_i$ se caracterizan por el hecho de que estos vértices son exactamente los pares de vértices con los mismos conjuntos de vecinos. El núcleo de la acción de $\mathrm{Aut}(\widetilde{X}'_p)$ en esta partición es claramente igual al subgrupo Γ. Se sigue que Γ es normal en $\mathrm{Aut}(\widetilde{X}'_p)$.

Ahora, consideremos la acción del grupo cociente $\mathrm{Aut}(\widetilde{X}'_p)/\Gamma$ sobre el sistema de bloques $\mathcal{B}$. Afirmamos que la acción es regular e isomorfa a $\langle \alpha, \beta \rangle \cong D_{2p}$. Para probar esto basta mostrar que un automorfismo dado α que fija el bloque $B_0 = \{x_{0,0}, x_{p,0}\}$ también fija todos los otros bloques en $\mathcal{B}$, es decir, pertenece a Γ. Primero observamos que los vecinos salientes de B_0 son $B_1, \ldots, B_{(p-1)/2}$ y $\overline{B}_1, \ldots, \overline{B}_{(p-1)/2}$. Supongamos que la acción de α sobre los vecinos salientes de B_0 tienen un ciclo de longitud mayor o igual a 2. Dado que las aristas entre B_0 y B_i son dirigidas y las aristas entre B_0 y $\overline{B}_i$ son no dirigidas,

los bloques en este ciclo de α pertenecen todos al conjunto $\{B_i : i \in \{1, \ldots, (p-1)/2\}\}$ o todos pertenecen al conjunto $\{\overline{B}_i : i \in \{1, \ldots, (p-1)/2\}\}$. Supongamos que lo primero se cumple y que B_i es el bloque con el índice más pequeño i contenido en el ciclo de α. Entonces, todos los bloques dentro de este ciclo de α son vecinos salientes de B_i, lo que contradice la condición de que α preserva la orientación de las aristas. Ahora, supongamos que se cumple lo segundo y que $\overline{B}_i$ es el bloque con el índice más pequeño i contenido en el ciclo de α. Entonces, todos los bloques dentro de este ciclo de α son vecinos entrantes de $\overline{B}_i$ y esto contradice nuevamente el hecho de que α preserva la orientación de las aristas. Así hemos probado que α fija todos los elementos en $\{B_1, \ldots, B_{(p-1)/2}\} \cup \{\overline{B}_1, \ldots, \overline{B}_{(p-1)/2}\}$. Usando el mismo argumento comenzando con un B_i, con $i \in \{1, \ldots, (p-1)/2\}$, demostramos que α fija también todos los elementos en $\{B_{(p+1)/2}, \ldots, B_{(p-1)}\} \cup \{\overline{B}_{(p+1)/2}, \ldots, \overline{B}_{(p-1)}\}$. Como α es biyectiva, también debe fijar a $\overline{B}_0$. Por tanto, la acción de α sobre $\mathcal{B}$ es la identidad. Esto implica que $\alpha \in \Gamma$. En consecuencia, $\mathrm{Aut}(\widetilde{X}'_p)/\Gamma$ es regular e isomorfo a D_{2p}, lo que implica que

$$\mathrm{Aut}(\widetilde{X}'_p) = \Gamma \rtimes \langle \alpha, \beta \rangle \cong \mathbb{Z}_2 \wr D_{2p}.$$

■

TEOREMA 3.3. *El digrafo $\widetilde{X}'_p$ es un grafo dirigido fuertemente regular con parámetros*

$$v = 4p, \quad k = 2p - 2, \quad t = p - 1, \quad \lambda = p - 3, \quad \mu = p - 1.$$

DEMOSTRACIÓN. Es evidente que el digrafo $\widetilde{X}'_p$ es de orden $4p$ y de grado $k = 2|S| = 2p - 2$. Como $S \cap -S = \emptyset$, también tenemos $t = p - 1$. Para probar que X'_p es un grafo dirigido fuertemente regular, basta con considerar el número de caminos de longitud 2 desde un vértice u hasta un vértice w para los siguientes pares:

$$(u, v) \in \{(x_{0,0}, x_{s,i}), (x_{0,0}, y_{s,i}), (x_{0,0}, x_{-s,i}), (x_{0,0}, x_{0,1}), (x_{0,0}, y_{-s,i}), (x_{0,0}, y_{0,1}), (x_{0,0}, y_{0,0})\}$$

donde $s \in Q$ y $i \in \{0, 1\}$.

a) Caminos de longitud 2 de $x_{0,0}$ a $x_{s,i}$.

Nótese que, en caso de existir un camino de longitud 2 de $x_{0,0}$ a $x_{s,i}$, debe ocurrir una de las siguientes afirmaciones:

i. Existe $k \in \mathbb{Z}_p$ tal que $(x_{0,0}, x_{k,0})$ y $(x_{k,0}, x_{s,i})$ son arcos de $\widetilde{X}'_p$.

ii. Existe $k \in \mathbb{Z}_p$ tal que $(x_{0,0}, x_{k,1})$ y $(x_{k,1}, x_{s,i})$ son arcos de $\widetilde{X}'_p$.

iii. Existe $k \in \mathbb{Z}_p$ tal que $(x_{0,0}, y_{k,0})$ y $(y_{k,0}, x_{s,i})$ son arcos de $\widetilde{X}'_p$.

iv. Existe $k \in \mathbb{Z}_p$ tal que $(x_{0,0}, y_{k,1})$ y $(y_{k,1}, x_{s,i})$ son arcos de $\widetilde{X}'_p$.

Si ocurre la afirmación **i**, como $(x_{0,0}, x_{k,0})$ es un arco, existe $s^* \in S$ tal que $(0,0) + s^* = (k,0)$, entonces $(k,0) \in S$; y como $(x_{k,0}, x_{s,i})$ es un arco, existe $\tilde{s} \in S$ tal que $(k,0) + \tilde{s} = (s,i)$, luego $(k,0) \in (s,i) - S$.

Si ocurre la afirmación **ii**, como $(x_{0,0}, x_{k,1})$ es un arco, existe $s^* \in S$ tal que $(0,0) + s^* = (k,1)$, luego $(k,1) \in S$; y como $(x_{k,1}, x_{s,i})$ es un arco, existe $\tilde{s} \in S$ tal que $(k,1) + \tilde{s} = (s,i)$, y entonces $(k,1) \in (s,i) - S$. Por lo tanto, debemos contar todos los elementos en común entre S y $(s,i) - S$.

Si ocurre la afirmación **iii**, como $(x_{0,0}, y_{k,0})$ es un arco, existe $s^* \in S$ tal que $(0,0) + s^* = (k,0)$, y entonces $(k,0) \in S$; y como $(y_{k,0}, x_{s,i})$ es un arco, existe $\tilde{s} \in -S$ tal que $(k,0) + \tilde{s} = (s,i)$, y entonces $(k,0) \in (s,i) + S$.

Si ocurre la afirmación **iv**, como $(x_{0,0}, y_{k,1})$ es un arco, existe $s^* \in S$ tal que $(0,0) + s^* = (k,1)$, luego $(k,1) \in S$; y como $(y_{k,1}, x_{s,i})$ es un arco, existe $\tilde{s} \in -S$ tal que $(k,1) + \tilde{s} = (s,i)$, luego $(k,1) \in (s,i) + S$. Por lo tanto, debemos contar todos los elementos en común entre S y $s + S$.

Por lo tanto, el número de caminos de longitud 2 desde $x_{0,0}$ hasta $x_{s,i}$ es

$$|S \cap (s,i) - S| + |S \cap (s,i) + S|.$$

Denotaremos por Q' al conjunto $\{\theta, \theta^3, \ldots, \theta^{p-2}\}$. Se tiene que $-S = (Q' \times \{0\}) \cup (Q' \times \{1\})$.

En efecto, supongamos que $-1 \in Q$, es decir, existe $a \in \mathbb{Z}$ tal que $1 + \theta^{2a} \equiv 0 \mod p$. Por el Pequeño Teorema de Fermat , $\theta^{p-1} + \theta^{2a} \equiv 0 \mod p$. Como $p-1$ es un número par, existe $m \in \mathbb{Z}$ tal que $p - 1 = 2m$, y entonces $\theta^{2m} + \theta^{2a} \equiv 0 \mod p$. Si suponemos que $m > a$, entonces existe $k \in \mathbb{Z}$ tal que $\theta^{2a}(\theta^{2(m-a)} + 1) = kp$. Como p no divide θ^{2a}, p divide $\theta^{2(s-a)} + 1$. Por lo tanto, $\theta^{2(m-a)} + 1 \equiv 0 \mod p$. De nuestra hipótesis, $\theta^{2(m-a)} \equiv \theta^{2a} \mod p$ y por lo tanto $m = 2a$. Como $m = \dfrac{p-1}{2}$, tenemos que $p - 1 = 4a$. Esto es una contradicción porque $p \equiv 3 \mod 4$. Obtenemos un resultado similar si suponemos que $a > m$. Así, $-1 \in Q'$. De ahí, existe $m \in \mathbb{Z}$ tal que $-1 = \theta^{2m+1}$ y por lo tanto, para todo $t \in \mathbb{Z}$, $-\theta^{2t} = \theta^{2m+1+2t} = \theta^{2(m+t)+1} \in Q'$. Podemos concluir que $-Q = Q'$ y por lo tanto

$$-S = -Q_0 \cup -Q_1 = Q' \times \{0\} \cup Q' \times \{1\} = Q'_0 \cup Q'_1.$$

Sea $s_i := (s, i)$, por cálculo directo tenemos

$$\begin{aligned}
|S \cap s_i - S| &= |(Q_0 \cup Q_1) \cap ((Q_0' \cup Q_1') + s_i)| \\
&= |(Q_0 \cup Q_1) \cap ((Q_0' + s_i \cup (Q_1' + s_i)| \\
&= |Q_0 \cap (Q_0' + s_i)| + |Q_0 \cap (Q_1' + s_i)| \\
&\quad + |Q_1 \cap (Q_0' + s_i)| + |Q_1 \cap (Q_1' + s_i)| \\
&= 2|Q_0 \cap (Q_0' + s_i)| + 2|Q_0 \cap (Q_1' + s_i)| \\
&= 2|Q_0 \cap (Q_i' + s_i)| \\
&= 2|Q \cap (Q' + s)|.
\end{aligned}$$

De la misma manera obtenemos que

$$\begin{aligned}
|S \cap s_i + S| &= |(Q_0 \cup Q_1) \cap ((Q_0 \cup Q_1) + s_i)| \\
&= |(Q_0 \cup Q_1) \cap ((Q_0 + s_i \cup Q_1 + s_i)| \\
&= 2|Q_0 \cap (Q_0 + s_i)| + 2|Q_0 \cap (Q_1 + s_i)| \\
&= 2|Q_0 \cap Q_i + s_i)| \\
&= 2|Q \cap (Q + s)|.
\end{aligned}$$

Así,

$$|S \cap s_i - S| + |S \cap s_i + S| = 2|(Q \cap Q + s) \cup (Q \cap Q' + s)|.$$

Observemos que

$$(Q \cap Q + s) \cup (Q \cap Q' + s) = Q \setminus \{s\}.$$

En efecto, si $x \in (Q \cap Q + s) \cup (Q \cap Q' + s)$, entonces es obvio que $x \in Q$ y $x \neq s$, porque $0 \notin Q \cup Q'$. Por lo tanto, $(Q \cap Q + s) \cup (Q \cap Q' + s) \subseteq Q \setminus \{s\}$.

Por otro lado, si $x \in Q \setminus \{s\}$, consideramos $w \equiv x - s \mod p$ y entonces $x \equiv w + s \mod p$. Como $\mathbb{Z}_p = Q \cup Q' \cup \{0\}$, tenemos que $w \in Q$ o $w \in Q'$ (claramente $w \neq 0$), y entonces $x \in Q \cap Q + s$ o $x \in Q \cap Q' + s$; por lo tanto, $(Q \cap Q + s) \cup (Q \cap Q' + s) = Q \setminus \{s\}$. A partir de ahí, podemos concluir que

$$|S \cap s_i - S| + |S \cap s_i + S| = 2(|Q| - 1) = p - 3.$$

b) Caminos de longitud 2 de $x_{0,0}$ a $y_{s,i}$.

De una formar similar al item a), el número de caminos de longitud 2 de $x_{0,0}$ a $y_{s,i}$ es

$$|S \cap s_i + S| + |S \cap s_i - S| = p - 3.$$

c) Caminos de longitud 2 de $x_{0,0}$ a $x_{-s,i}$.

El número de caminos de longitud 2 de $x_{0,0}$ a $x_{-s,i}$ es

$$|S \cap -s_i - S| + |S \cap -s_i + S|, \text{ donde } s_i = (s,i),\ i \in \{0,1\}.$$

Como en el item i), denotaremos por Q' al conjunto $\{\theta, \theta^3, \ldots, \theta^{p-2}\}$. Tenemos entonces que $-S = Q'_0 \cup Q'_1$, por tanto

$$\begin{aligned} |S \cap -s_i - S| &= |(Q_0 \cup Q_1) \cap ((Q'_0 \cup Q'_1) - s_i)| = |(Q_0 \cup Q_1) \cap (Q'_0 - s_i \cup Q'_1 - s_i)| \\ &= |Q_0 \cap Q'_0 - s_i| + |Q_0 \cap Q'_1 - s_i| + |Q_1 \cap Q' - s_i| + |Q_1 \cap Q'_1 - s_i| \\ &= 2(|Q_0 \cap Q'_0 - s_i| + |Q_0 \cap Q'_1 - s_i|) \\ &= 2|Q \cap Q'_i - s_i| = 2|Q \cap Q' - s|. \end{aligned}$$

Del mismo modo

$$\begin{aligned} |S \cap -s_i + S| &= |(Q_0 \cup Q_1) \cap ((Q_0 \cup Q_1) - s_i)| = |(Q_0 \cup Q_1) \cap (Q_0 - s_i \cup Q_1 - s_i)| \\ &= |Q_0 \cap Q_0 - s_i| + |Q_0 \cap Q_1 - s_| + |Q_1 \cap Q_0 - s_i| + |Q_1 \cap Q_1 - s_i| \\ &= 2|Q \cap Q - s|. \end{aligned}$$

Así,

$$|S \cap -s_i - S| + |S \cap -s_i + S| = 2|(Q \cap Q - s) \cup (Q \cap Q' - s)|.$$

Podemos observar que

$$(Q \cap Q - s) \cup (Q \cap Q' - s) = Q.$$

En efecto, si $x \in (Q \cap Q - s) \cup (Q \cap Q' - s)$ entonces es obvio que $x \in Q$. Por lo tanto, $(Q \cap Q + s) \cup (Q \cap Q' + s) \subseteq Q$. Por otro lado, si $x \in Q$, existe $w \in \mathbb{Z}_p$ tal que $w = x + s \mod p$. Claramente, $w \neq 0$, porque $Q \cap Q' = \emptyset$, y entonces $w \in Q \cup Q'$. Si $w \in Q$, $x \in Q - s$ y si $w \in Q'$, $x \in Q' - s$. Así, $x \in (Q \cap Q - q) \cup (Q \cap Q' - q)$. A partir de ahí, podemos concluir que

$$|S \cap -s_i - S| + |S \cap -s_i + S| = 2|Q| = p - 1.$$

d) Caminos de longitud 2 de $x_{0,0}$ a $x_{0,1}$.

El número de caminos de longitud 2 de $x_{0,0}$ a $x_{0,1}$ es

$$|S \cap \{(0,1)\} - S| + |S \cap \{(0,1)\} + S|.$$

Tenemos que

$$\begin{aligned} |S \cap \{(0,1)\} - S| &= |(Q_0 \cup Q_1) \cap ((Q_0' \cup Q_1') + \{(0,1)\})| = |(Q_0 \cup Q_1) \cap (Q_0' \cup Q_1')| \\ &= |Q_0 \cap Q_0'| + |Q_0 \cap Q_1'| + |Q_1 \cap Q_0'| + |Q_1 \cap Q_1'| = 0, \end{aligned}$$

$$\begin{aligned} |S \cap \{(0,1)\} + S| &= |(Q_0 \cup Q_1) \cap ((Q_0 \cup Q_1) + \{(0,1)\})| = |(Q_0 \cup Q_1) \cap (Q_1 \cup Q_0)| \\ &= |Q_0 \cup Q_1| = |S| = p - 1. \end{aligned}$$

e) Caminos de longitud 2 de $x_{0,0}$ a $y_{-s,i}$.

De forma similar al item c), el número de caminos de longitud 2 de $x_{0,0}$ a $y_{-s,i}$ es

$$|S \cap -s_i - S| + |S \cap -s_i + S| = p - 1.$$

f) Caminos de longitud 2 de $x_{0,0}$ a $y_{0,1}$.

De forma similar al item d), el número de caminos de longitud 2 de $x_{0,0}$ a $y_{0,1}$ es

$$|S \cap \{(0,1)\} - S| + |S \cap (0,1) + S| = p - 1.$$

g) Caminos de longitud 2 de $x_{0,0}$ a $y_{0,0}$.

El número de caminos de longitud 2 de $x_{0,0}$ a $y_{0,0}$ es

$$|S \cap -S| + |S \cap S| = |S| = p - 1.$$

Como para cada $s \in Q$ los pares ordenados $(x_{0,0}, x_{s,i})$ y $(x_{0,0}, y_{s,i})$, con $i \in \{0,1\}$, son arcos en $\widetilde{X}_p'$ y $(x_{0,0}, x_{-s,i})$, $(x_{0,0}, x_{0,1})$, $(x_{0,0}, y_{-s,i})$, $(x_{0,0}, y_{0,1})$ y $(x_{0,0}, y_{0,0})$ no son arcos en $\widetilde{X}_p'$ podemos concluir que $\widetilde{X}_p'$ es un grafo dirigido fuertemente regular con $\lambda = |S| - 2 = p - 3$ y $\mu = |S| = p - 1$. ■

TEOREMA 3.4. *El digrafo $\widetilde{X}_p''$ es el bicirculante $BC_{2p}[S \cup \{(0,1)\}, S, -S, -S \cup \{(0,1)\}]$, donde $S = Q_0 \cup Q_1$ y $Q = \{1, \theta^2, \ldots, \theta^{p-3}\}$. Es vértice transitivo y su grupo de automorfismos es G_p^**

DEMOSTRACIÓN. Es evidente que $S_{00} = S \cup \{p\}$, $S_{01} = S$, $S_{10} = -S$, $S_{11} = -S \cup \{p\}$ y por tanto

$$\widetilde{X}_p'' = BC_{2p}[S \cup \ \{p\}, S, -S, -S \cup \{p\}].$$

El digrafo $\widetilde{X}_p''$ puede construirse a partir del bicirculante $BC_{2p}[S, S, -S, -S]$ considerado en el Teorema 3.2, añadiendo aristas no dirigidas entre los dos vértices en cada uno de los bloques $B_i = \{x_{i,0}, x_{p+i,0}\}$ y $\overline{B}_i = \{y_{i,0}, y_{p+i,0}\}$ con $i \in \{0, 1, \ldots, p-1\}$. Agregar aristas

dentro de bloques de tamaño 2 significa que todos los bloques inducen el grafo completo K_2 en lugar del grafo vacío $2K_1$. Esto claramente no tiene consecuencias en el grupo completo de automorfismos del digrafo. En particular, sigue siendo válida la prueba del Teorema 3.2.

■

TEOREMA 3.5. *El digrafo $\widetilde{X}''_p$ es un grafo dirigido fuertemente regular con parámetros*

$$v = 4p, \quad k = 2p - 1, \quad t = p, \quad \lambda = p - 1, \quad \mu = p - 1.$$

DEMOSTRACIÓN. Es evidente que el dígrafo $\widetilde{X}''_p$ es de orden $4p$ y de grado $k = 2|S| + 1 = 2p - 1$. Como $S \cap -S = \emptyset$, también tenemos que $t = p$. Para probar que X'_p es un grafo dirigido fuertemente regular, basta con considerar el número de caminos de longitud 2 desde un vértice u hasta un vértice w para los siguientes pares:

$$(u, v) \in \{(x_{0,0}, x_{s,i}), (x_{0,0}, y_{s,i}), (x_{0,0}, x_{-s,0}), (x_{0,0}, x_{0,1}), (x_{0,0}, y_{-s,i}), (x_{0,0}, y_{0,1}), (x_{0,0}, y_{0,0})\}$$

donde $s \in S$.

a) Caminos de longitud 2 de $x_{0,0}$ a $x_{s,i}$.

Note que si existe un camino de longitud 2 de $x_{0,0}$ a $x_{s,i}$, debe ocurrir una de las siguientes afirmaciones:

i. Existe $k \in \mathbb{Z}_{2p}$ tal que $(x_{0,0}, x_{k,i})$ y $(x_{k,i}, x_{s,i})$ son arcos de $\widetilde{X}''_p$.
ii. Existe $k \in \mathbb{Z}_{2p}$ tal que $(x_{0,0}, y_{k,i})$ y $(y_{k,i}, x_{s,i})$ son arcos de $\widetilde{X}''_p$.

Si ocurre la afirmación **i**, como $(x_{0,0}, x_{k,i})$ es un arco, entonces $k_i \in S \cup \{(0,1)\}$, con $k_i = (k, i)$; y como $(x_{k,i}, x_{s,i})$ es un arco, entonces $k_i \in s_i - (S \cup \{(0,1)\})$. Por lo tanto, debemos contar todos los elementos en común entre $S \cup \{(0,1)\}$ y $s_i - (S \cup \{(0,1)\})$.

Si ocurre la afirmación **ii**, como $(x_{0,0}, y_{k,i})$ es un arco, entonces $k_i \in S$; y como $(y_{k,i}, x_{s,i})$ es un arco, entonces $k_i \in s_i + S$. Por lo tanto, debemos contar todos los elementos en común entre S y $s_i + S$.

Por lo tanto, el número de caminos de longitud 2 de $x_{0,0}$ a $x_{s,i}$ es

$$|(S \cup \{(0,1)\}) \cap s_i - (S \cup \{(0,1)\})| + |S \cap s_i + S|.$$

Tenemos que

$$\begin{aligned}|(S\cup\{(0,1)\})\cap s_i-(S\cup\{(0,1)\})| \quad &+|S\cap s_i+S|=|S\cap s_i-S|+|S\cap s_i-\{(0,1)\}|+\\ &+|\{(0,1)\}\cap s_i-S|+|\{(0,1)\}\cap s_i-\{(0,1)\}|\\ &+|S\cap s+S|=|S\cap s_i-S|+1+1+0+|S\cap s_i+S|.\end{aligned}$$

Del item a) del Teorema 3.3,

$$|(S\cup\{(0,1)\})\cap s-(S\cup\{(0,1)\})|+|S\cap s_i+S|=p-1.$$

b) Caminos de longitud 2 de $x_{0,0}$ a $y_{s,i}$.

El número de caminos de longitud 2 de $x_{0,0}$ a $y_{s,i}$ es

$$|(S\cup\{(0,1)\})\cap s_i-S|+|S\cap s_i+(S\cup\{(0,1)\})|.$$

Tenemos que

$$\begin{aligned}|(S\cup\{(0,1)\})\cap s_i-(S\cup\{(0,1)\})| \quad &+|S\cap s_i+S|=|S\cap s_i-S|+|\{(0,1)\}\cap s_i-S|+\\ &+|S\cap s_i+S|+|S\cap s_i+\{(0,1)\}|\\ &=|S\cap s_i-S|+1+|S\cap s_i+S|+1.\end{aligned}$$

Del caso anterior,

$$|(S\cup\{(0,1)\})\cap s_i-S|+|S\cap s_i+(S\cup\{(0,1)\})|=p-1.$$

c) Caminos de longitud 2 de $x_{0,0}$ a $x_{-s,0}$.

El número de caminos de longitud 2 de $x_{0,0}$ a $x_{-s,0}$ es

$$|(S\cup\{(0,1)\})\cap -s_i-(S\cup\{(0,1)\})|+|S\cap -s_i+S|.$$

Tenemos que

$$\begin{aligned}|(S\cup\{(0,1)\})\cap -s_i-(S\cup\{(0,1)\})| \quad &+|S\cap -s_i+S|=|S\cap -s_i-S|+|S\cap -s_i-\{(0,1)\}|+\\ &+|\{(0,1)\}\cap -s_i-S|+|\{(0,1)\}\cap -s_i-\{(0,1)\}|+\\ &+|S\cap -s_i+S|=|S\cap -s_i-S|+|S\cap -s_i+S|.\end{aligned}$$

Del item c) del Teorema 3.3,

$$|(S\cup\{(0,1)\})\cap -s_i-(S\cup\{(0,1)\})|+|S\cap -s_i+S|=p-1.$$

d) Caminos de longitud 2 de $x_{0,0}$ a $x_{0,1}$.

El número de caminos de longitud 2 de $x_{0,0}$ a $x_{0,1}$ es

$$|S \cap \{(0,1)\} - S| + |S \cap \{(0,1)\} + S|.$$

Tenemos que

$$|S \cap \{(0,1)\} - S| + |S \cap \{(0,1)\} + S| = 0 + |S| = p - 1.$$

e) Caminos de longitud 2 de $x_{0,0}$ a $y_{-s,i}$.

El número de caminos de longitud 2 de $x_{0,0}$ a $y_{-s,i}$ es

$$|(S \cup \{(0,1)\}) \cap -s_i - (S \cup \{(0,1)\})| + |S \cap -s_i + S|.$$

Tenemos que

$$\begin{aligned} |(S \cup \{(0,1)\}) \cap -s_i - S| + |S \cap -s_i + (S \cup \{(0,1)\})| &= |S \cap -s_i - S| + |\{(0,1)\} \cap -s_i - S| \\ &\quad + |S \cap -s_i + S| + |S \cap -s_i + \{(0,1)\}| \\ &= |S \cap -s_i - S| + |S \cap -s_i + S| = p - 1. \end{aligned}$$

f) Caminos de longitud 2 de $x_{0,0}$ a $y_{0,1}$.

El número de caminos de longitud 2 de $x_{0,0}$ a $y_{0,1}$ es

$$|(S \cup \{(0,1)\}) \cap \{(0,1)\} - S| + |S \cap \{(0,1)\} + S|.$$

Tenemos que

$$\begin{aligned} |S \cup \{(0,1)\} \cap \{(0,1)\} - S| + |S \cap \{(0,1)\} &+ (S \cup \{(0,1)\})| \\ &= |S \cap \{0,1\} - S| + |\{(0,1)\} \cap \{(0,1)\} - S| \\ &\quad + |S \cap \{0,1\} + S| + |S \cap \{(0,1)\} + \{(0,1)\}| \\ &= |S \cap \{(0,1)\} - S| + 0 \\ &\quad + |S \cap \{(0,1)\} + S| + 0 = p - 1. \end{aligned}$$

g) Caminos de longitud 2 de $x_{0,0}$ a $y_{0,0}$.

El número de caminos de longitud 2 de $x_{0,0}$ a $y_{0,0}$ es

$$|S \cup \{(0,1)\} \cap -S| + |S \cap (S \cup \{(0,1)\})|.$$

Tenemos que

$$\begin{aligned}|S \cup \{(0,1)\} \cap -S| + |S \cap (S \cup \{(0,1)\})| &= |S \cap -S| + |\{(0,1)\} \cap -S| \\ &\quad + |S \cap S| + |S \cap \{(0,1)\}| = |S| = p-1.\end{aligned}$$

Como para todo $s_i \in S$ los pares ordenados $(x_{0,0}, x_{s,i})$ y $(x_{0,0}, y_{s,i})$ son arcos en $\widetilde{X}'_p$ y $(x_{0,0}, x_{-s,i})$, $(x_{0,0}, x_{0,1})$, $(x_{0,0}, y_{-s,0})$, $(x_{0,0}, y_{0,1})$ y $(x_{0,0}, y_{0,0})$ no son arcos en $\widetilde{X}'_p$ podemos concluir que $\widetilde{X}'_p$ es un grafo dirigido fuertemente regular con $\lambda = |S| - 2 = p - 3$ y $\mu = |S| = p - 1$. ■

TEOREMA 3.6. *La permutación δ es un automorfismo de $\widetilde{X}'_p$ y $\widetilde{X}''_p$.*

DEMOSTRACIÓN. Para probar que δ es un automorfismos de $\widetilde{X}'_p$, debemos probar que para todos $i \in Q$ y $k \in \mathbb{Z}_2$, existe $j \in Q$ tal que $\delta(x_{0,0}, x_{i,k}) = (x_{0,0}, x_{j,k})$, $\delta(x_{0,0}, y_{i,k}) = (x_{0,0}, y_{j,k})$, $\delta(y_{0,0}, x_{i,k}) = (y_{0,0}, x_{j,k})$ y $\delta(y_{0,0}, y_{i,k}) = (y_{0,0}, y_{j,k})$.

Sea θ una raíz primitiva módulo p. Si $i \in Q$, existe $n \in \mathbb{Z}$ tal que $i = \theta^{2n}$. De la definición de δ se tiene que para todo $k \in \mathbb{Z}_2$,

$$\delta(x_{0,0}, x_{i,k}) = (x_{0,0}, x_{\theta^{2(n+1)},k}),\ \delta(x_{0,0}, y_{i,k}) = (x_{0,0}, y_{\theta^{2(n+1)},k}),\ \delta(y_{0,0}, x_{i,k}) = (y_{0,0}, x_{\theta^{2(n+1)},k})$$

y

$$\delta(y_{0,0}, y_{i,k}) = (y_{0,0}, y_{\theta^{2(n+1)},k}).$$

Por tanto, δ es un automorfismo del digrafo $\widetilde{X}'_p$.

Como $(x_{0,0}, x_{0,1})$ es un punto fijo de δ, se puede observar que δ es un automorfismo del digrafo $\widetilde{X}''_p$. ■

PROPOSICIÓN 3.7. *Si p es un número primo, $p \equiv 3 \mod 4$, la permutación δ no es una permutación del grupo G_p.*

DEMOSTRACIÓN. Suponemos que δ es una permutación de G_p. Del Teorema de Lagrange, el orden de δ divide al orden de G_p. Dado que el orden de G_p es $2p \cdot 2^{2p}$ (**[38]**) y el orden de δ es, por construcción, $\dfrac{p-1}{2}$, tenemos que existe $k \in \mathbb{Z}$ tal que

$$k(p-1) = p \cdot 2^{2p+2}.$$

De esto, concluimos que p divide a k. Por lo tanto, existe $m \in \mathbb{Z}$ tal que $k = mp$, entonces tenemos $2^{2p+2} = m(p-1)$. Como $p \equiv 3 \mod 4$, existe $r \in \mathbb{Z}$ tal que $p - 3 = 4r$. Así,

$$2^{2p+2} = m(2 + 4r),$$

de donde se obtiene finalmente que

$$2^{2p+1} = m(1+2r).$$

Esto es una contradicción porque $1+2r$ es un número impar. ■

En el artículo [**38**] presentamos una familia infinita de grupos de permutaciones, los cuales resultan ser los grupos completos de automorfismos de dos familias diferentes de grafos dirigidos fuertemente regulares. En ambas familias, identificamos un subgrupo cíclico del grupo de permutaciones que actúa de manera semirregular en el conjunto de vértices del grafo dirigido y genera dos órbitas. De particular interés, una de las dos series revela una cantidad infinita de grafos dirigidos fuertemente regulares que admiten un grupo de automorfismos semirregular cíclico, acompañado de una estructura del símbolo. Este hallazgo representa una expansión significativa, ya que no es necesario un número primo para construir un número infinito de grafos dirigidos fuertemente regulares con un grupo de automorfismos del cual solo se conocían tres ejemplos esporádicos anteriormente. Este resultado amplía considerablemente la comprensión de las propiedades estructurales de los grafos dirigidos fuertemente regulares y sus grupos asociados de automorfismos.

Sea $p \in \mathbb{N}$ un número impar y

$$G_p = \langle \alpha, \beta, \gamma_0, \ldots, \gamma_{2p_1} \rangle$$

un grupo de permutaciones definido sobre el conjunto $V_p = \{x_0, x_1, \ldots, x_{2p-1}, y_0, y_1, \ldots, y_{2p-1}\}$, donde

$$\alpha = (x_0 x_1 \ldots x_{2p-1})(y_0 y_1 \ldots y_{2p-1}), \quad \beta = \prod_{i=0}^{p-1} (x_i y_{-i})$$

y

$$\gamma_i = \begin{cases} (x_i x_{p+1}) & \text{para todo } i = 0, \ldots, p-1; \\ (y_{i-p} y_i) & \text{para todo } i = p, \ldots 2p-1. \end{cases}$$

Se demuestra que G_p es un grupo de orden $2^{2p} \cdot 2p$ y es isomorfo a $\mathbb{Z}_2 \wr D_{2p}$ (producto corona).

Cuando elegimos la acción de G_p sobre $V_p \times V_p$, podemos generar las orbitas de pares en $V_p \times V_p$. Para cualquier par de vértices u y v en V_p, representamos la orbita correspondiente como $\overline{(u,v)}$. Ahora, centrémonos en las siguientes dos familias de grafos dirigidos con un conjunto de vértices dado por V_p:

1. El digrafo X'_p cuyo conjunto de arcos es la unión de orbitas

$$\overline{(x_0, x_1)} \cup \overline{(x_0, x_2)} \cup \ldots \cup \overline{(x_0, x_{(p-1)/2})} \cup \overline{(x_0, y_1)} \cup \overline{(x_0, y_2)} \cup \ldots \cup \overline{(x_0, y_{(p-1)/2})}.$$

2. El digrafo X''_p cuyo conjunto de arcos es la unión de órbitas

$$\overline{(x_0, x_1)} \cup \overline{(x_0, x_2)} \cup \ldots \cup \overline{(x_0, x_{(p-1)/2})} \cup \overline{(x_0, x_p)} \cup \overline{(x_0, y_1)} \cup \overline{(x_0, y_2)} \cup \ldots \cup \overline{(x_0, y_{(p-1)/2})}.$$

Por construcción, el grupo G_p es un grupo de automorfismos tanto para X'_p como X''_p. Además, ambos son bicirculantes, ya que α es $(2, 2p)$-semirregular.

Respecto a estos dos digrafos, se obtuvieron los siguientes resultados, cuyas demostraciones son análogas a las hechas en esta tesis para los Teoremas 3.2, 3.3, 3.4 y 3.5, respectivamente.

TEOREMA 3.8. ***El digrafo*** X'_p ***es el bicirculante*** $BC_{2p}[S, S, -S, -S]$***, donde*** $S = Q \cup Q + p$ ***y*** $Q = \{1, 2, \ldots, (q-1)/2\}$***. Es vértice-transitivo y su grupo de automorfismo es*** G_p***.***

TEOREMA 3.9. ***El digrafo bicirculante*** $BC_{2p}[S, S, -S, -S]$***, donde*** $S = Q \cup Q + p$ ***y*** $Q = \{1, 2, \ldots, (q-1)/2\}$***, es un*** $(4p, 2p-2, p-1, p-3, p-1)$***-GDFR.***

TEOREMA 3.10. ***El digrafo*** X''_p ***es el bicirculante*** $BC_{2p}[S \cup \{p\}, S, -S, -S \cup \{p\}]$***, donde*** $S = Q \cup Q + p$ ***y*** $Q = \{1, 2, \ldots, (q-1)/2\}$***. Es vértice-transitivo y su grupo de automorfismo es*** G_p***.***

TEOREMA 3.11. ***El digrafo bicirculante*** $BC_{2p}[S \cup \{p\}, S, -S, -S \cup \{p\}]$***, donde*** $S = Q \cup Q + p$ ***y*** $Q = \{1, 2, \ldots, (q-1)/2\}$***, es un*** $(4p, 2p-1, p-1, p-1, p)$***-GDFR.***

Se puede notar que los parámetros presentes en el Teorema 3.8 coinciden con aquellos en ([**2**], Proposición 3.7), tomando $e = 2$, $s = 2$ y $f = (p-1)/2$. Dicha proposición establece que para todos e, s y f existe una $(e, s(ef+1), sef, sf, s(f-1), sf)$-FSP circulante. Asimismo, se observa que los parámetros en el Teorema 3.11 son idénticos a los del complemento en ([**2**], Proposición 3.8), con $s = 2$ y $f = (p-1)/2$. Esta propoción establece que para todos f y s existe una $(2, s(2f+1), s(2f+1), s(f+1), sf, s(f+1))$-FSP circulante. No obstante, a pesar de estas similitudes, los cálculos realizados mediante GAP sugieren que los grafos resultantes no son isomorfos y que los grupos de automorfismos correspondientes son más extensos en los Teoremas 3.9 y 3.11 en comparación con las proposiciones mencionadas.

Capítulo 4

CONJUNTOS DE DIFERENCIAS PARCIALES OBTENIDOS USANDO CICLOTOMÍA ESTÁNDAR UNIFORME SOBRE UN PRODUCTO DE DOS CUERPOS FINITOS IGUALES

En el estudio de las extensiones de cuerpos finitos, la teoría de la ciclotomía desempeña un papel fundamental al proporcionar herramientas para comprender la estructura y las propiedades de estas extensiones. La ciclotomía se enfoca en el estudio de las raíces de la unidad en cuerpos finitos y establece conexiones profundas entre la teoría de números y la teoría de cuerpos.

La teoría de la ciclotomía se remonta a Gauss y tiene una serie de aplicaciones en la teoría de números. Recientemente, se ha demostrado su utilidad en campos más aplicados, como la teoría de la codificación y la criptografía. El campo de la combinatoria también se ha beneficiado del uso de la ciclotomía, que se puede aplicar, por ejemplo, para la construcción de conjuntos de diferencias ([**50**], [**106**]).

En el artículo [**32**], G.A. Fernández Alcober, R. Kwashira y L. Martínez introdujeron un nuevo tipo de ciclotomía en productos de cuerpos finitos, que llamaron *ciclotomía estándar*, y la usaron para obtener conjuntos de diferencias parciales, conjuntos de diferencias divisibles, conjuntos de diferencias relativas y esquemas de asociación de tres clases. Usaremos un caso particular de esta ciclotomía para enlazar la ciclotomía estándar uniforme sobre productos de dos cuerpos finitos iguales con los construcciones

de partial spread de conjuntos de diferencias parciales y analizar algunos de sus grupos de automorfismos, y demostraremos que son mayores que los obtenidos cuando se toma un partial spread elegido al azar, por lo que el uso de esta ciclotomía estándar uniforme produce conjuntos de diferencias parciales que son más simétricos que los obtenidos cuando se utiliza un partial spread aleatorio.

DEFINICIÓN 4.1. *Sean v, k, λ y μ enteros positivos tales que $2 \leq k < v$ y sea $(G, +)$ un grupo con elemento neutro 0. Un conjunto $D \subset G$ es un (v, k, λ, μ)-**Conjunto de diferencias parciales** (o simplemente **Conjunto de diferencias parciales**) en $(G, +)$ si $|G| = v$, $|D| = k$, y el multiconjunto de diferencias $\{x - y \ : \ x, y \in D \text{ y } x \neq y\}$ contiene exactamente λ veces los elementos que no son el neutro de D y exactamente μ veces los elementos que no son el neutro de $G - D$.*

EJEMPLO 4.2. *Consideremos el grupo $(G, +)$ (con elementro neutro 0) dado por*

$$G = \{a, b \ : \ a + a = b + b = 0, \ a + b = b + a\}.$$

Este grupo contiene cuatro elementos: $G = \{0, a, b, a + b\}$. Sea $D = \{a, b\}$ y consideremos la tabla de diferencias:

	a	b
a		$b - a = b + a = a + b$
b	$a - b = a + b$	

Así, el multiconjunto de diferencias es

$$\{x - y \ : \ x, y \in D \text{ y } x \neq y\} = \{a + b, b + a\}.$$

Los elementos que no son el neutro de D son $\{a, b\}$, los cuales aparencen $\lambda = 0$ veces en el multiconjunto y los elementos que no son el neutro de $G - D$ son $\{a + b\}$, el cual aparece $\mu = 2$ veces en el multiconjunto.

Así, D es un $(4, 2, 0, 2)$-conjunto de diferencias parciales.

DEFINICIÓN 4.3. *Un partial spread de un conjunto A sobre un espacio vectorial V es una colección $\{S_1, S_2, \ldots, S_n\}$ de subespacios de dimensión finita "próximos a ser" disjuntos dos a dos (en el sentido de que las intersecciones dos a dos tienen como único elemento el neutro) de tal forma que $A = (S_1 \cup S_2 \cup \ldots \cup S_n) \setminus \{e\}$, donde e es el elemento neutro de V.*

EJEMPLO 4.4. *Considemos el espacio vectorial* $\mathbb{R}^3$ *y el conjunto*

$$A = \{(x, y, z) \in \mathbb{R}^3 \ : \ (y = 0 \wedge z = 0) \vee (x = 0 \wedge z = 0) \vee (x = 0 \wedge y = 0)\} \setminus \{(0, 0, 0)\}$$

.

Definamos los tres subespacios de $\mathbb{R}^3$*:*

- $S_1 = \langle (1, 0, 0) \rangle$
- $S_2 = \langle (0, 1, 0) \rangle$
- $S_3 = \langle (0, 0, 1) \rangle$

El único elemento en común de estos tres espacios es el elemento neutro $(0, 0, 0)$ *y además,*

$$(S_1 \cup S_2 \cup S_3) \setminus \{(0, 0, 0)\} = A.$$

Por tanto, $\{S_1, S_2, S_3\}$ *constituye un partial spread de* A *sobre* $\mathbb{R}^3$*.*

Inicialmente, la ciclotomía se desarrolló sobre cuerpos de orden primo, pero la misma teoría también se aplica a cuerpos finitos en general, como veremos a continuación.

DEFINICIÓN 4.5. *Sea* F *un cuerpo finito con* q *elementos. Entonces cada elección de una raíz primitiva* θ *de* F *y un divisor* e *de* $q - 1$ *define una* ***ciclotomía*** *sobre* F*, cuyo objetivo es obtener los valores de los llamados* ***números ciclotómicos*** (i, j) *para todo* $0 \leq i, j \leq e - 1$*. Si* $f = \frac{q-1}{e}$*, el número ciclotómico* (i, j) *es el número de soluciones* (x, y) *de la ecuación* $1 + x = y$*, donde* $x = \theta^{i+se}$ *para algún* $s = 0, 1, \ldots, f - 1$ *y* $y = \theta^{j+te}$ *para algún* $t = 0, 1, \ldots, f - 1$*.*

Introduciremos ahora la ciclotomía estándar antes mencionada.

Sea $R = \mathbb{F}_{q_1} \times \ldots \times \mathbb{F}_{q_n}$, donde $q_1, \ldots, q_n$ son potencias de un primo. Para todo $k = 1, \ldots, n$, sea θ_k una raíz primitiva de $\mathbb{F}_{q_k}$ y e un divisor de todos los $q_k - 1$ para $k = 1, \ldots, n$. Así, podemos escribir $q_k - 1 = e \cdot f_k$. Se puede verificar que el conjunto

$$H = \left\{ (\theta_1^{r_1}, \ldots, \theta_n^{r_n}) \ : \ \sum_{k=1}^{n} r_k \equiv 0 \mod e \right\}$$

es un subgrupo del grupo multiplicativo de las unidades de R.

En efecto, nótese que si $(\theta_1^{r_1}, \ldots, \theta_n^{r_n}), (\theta_1^{s_1}, \ldots, \theta_n^{s_n}) \in H$ entonces

$$(\theta_1^{r_1}, \ldots, \theta_n^{r_n})(\theta_1^{s_1}, \ldots, \theta_n^{s_n}) = (\theta_1^{r_1}\theta_1^{s_1}, \ldots, \theta_n^{r_n}\theta_n^{s_n}) = (\theta_1^{r_1+s_1}, \ldots, \theta_n^{r_n+s_n})$$

y $\sum_{k=1}^{n}(r_k + s_k) = \sum_{k=1}^{n} r_k + \sum_{k=1}^{n} s_k \equiv 0 \mod e$. Es decir, H es cerrado bajo la multiplicación. Por otro lado, véamos que también es cerrado bajo inversos. Nótese que

$$\theta_k^{r_k}\theta_k^{q_k-1-r_k} = \theta^{q_k-1} = 1,$$

luego es suficiente con demostrar que $\sum_{k=1}^{n}(q_k - 1 - r_k) \equiv 0 \mod e$.

$$\sum_{k=1}^{n}(q_k - 1 - r_k) = \sum_{k=1}^{n}(q_k - 1) - \sum_{k=1}^{n} r_k = \sum_{k=1}^{n} e \cdot f_k - \sum_{k=1}^{n} r_k \equiv 0 \mod e.$$

Las órbitas de R bajo la acción de H son los siguientes conjuntos:

- $C_i = \{(\theta_1^{r_1}, \ldots, \theta_n^{r_n}) \ : \ \sum_{k=1}^{n} r_k \equiv i \mod e\}$ para todo $i = 0, 1, \ldots, e-1$.
- $F_S = \{(x_1, \ldots, x_n) \in R \ : \ x_k \neq 0$ para $k \in S$ y $x_k = 0$ para $k \notin S\}$, para todo $S \subset \{1, \ldots, n\}$.

Las órbitas del tipo C_i se llaman *clases ciclotómicas*.

DEFINICIÓN 4.6.

- *Sea $R = \mathbb{F}_{q_1} \times \ldots \times \mathbb{F}_{q_n}$. Se define la **ciclotomía estándar** de orden e con respecto a las raíces primitivas $\theta_1, \ldots, \theta_n$ como la partición de R en las órbitas de la acción de H.*
- *Dada una ciclotomía estandar de orden e sobre $R = \mathbb{F}_{q_1} \times \ldots \times \mathbb{F}_{q_n}$ definida por las raíces primitivas $\theta_1, \ldots, \theta_n$, se define su **inverso ciclotómico** como la ciclotomía de orden e definida por $\theta_1^{-1}, \ldots, \theta_n^{-1}$.*
- *Sean dos ciclotomías estándar de orden e sobre dos anillos $R = \mathbb{F}_{q_1} \times \ldots \times \mathbb{F}_{q_n}$ y $R' = \mathbb{F}_{q'_1} \times \ldots \times \mathbb{F}_{q'_m}$, definidas por las raíces primitivas, $\theta_1, \ldots, \theta_n$ y $\theta'_1, \ldots, \theta'_m$ respectivamente. Entonces el **producto ciclotómico** de las dos ciclotomías es la ciclotomía sobre $R \times R'$ de orden e y raíces primitivas $\theta_1, \ldots, \theta_n, \theta'_1, \ldots, \theta'_m$*

EJEMPLO 4.7. *La ciclotomía estándar de orden 2 sobre $\mathbb{F}_5 \times \mathbb{F}_5$ con respecto al par (θ, θ^{-1}), donde $\theta = \bar{2}$ (por ende, $\theta^{-1} = \bar{3}$) viene dada por:*

- $C_0 = \{(\bar{2}^a, \bar{3}^b) \ : \ a+b \equiv 0 \mod 2\} = \{(\bar{1}, \bar{1}), (\bar{1}, \bar{4}), (\bar{2}, \bar{2}), (\bar{2}, \bar{3}), (\bar{3}, \bar{3}), (\bar{3}, \bar{2}), (\bar{4}, \bar{4}), (\bar{4}, \bar{1})\}$.
- $C_1 = \{(\bar{2}^a, \bar{3}^b) \ : \ a+b \equiv 1 \mod 2\} = \{(\bar{1}, \bar{2}), (\bar{1}, \bar{3}), (\bar{2}, \bar{1}), (\bar{2}, \bar{4}), (\bar{3}, \bar{1}), (\bar{3}, \bar{4}), (\bar{4}, \bar{3}), (\bar{4}, \bar{2})\}$.
- $F_{S_1} = (\mathbb{F}_5 - \{\bar{0}\}) \times \{\bar{0}\} = \{(\bar{1}, \bar{0}), (\bar{2}, \bar{0}), (\bar{3}, \bar{0}), (\bar{4}, \bar{0})\}$.
- $F_{S_2} = \{\bar{0}\} \times (\mathbb{F}_5 - \{\bar{0}\}) = \{(\bar{0}, \bar{1}), (\bar{0}, \bar{2}), (\bar{0}, \bar{3}), (\bar{0}, \bar{4})\}$.

- $O = \{(\bar{0}, \bar{0})\}$

DEFINICIÓN 4.8. *Dado q una potencia de primo, y un divisor e de $q-1$, consideramos una ciclotomía estándar de orden e sobre $\mathbb{F}_q \times \mathbb{F}_q$ con respecto al par (θ, θ^{-1}), donde θ es una raíz primitiva del cuerpo $\mathbb{F}_q$. Dicha ciclotomía la llamamos* ***ciclotomía estándar uniforme.***

TEOREMA 4.9. *Dada una ciclotomía estándar uniforme, cualquier unión D de órbitas que no contenga a $(0, 0)$ es un conjunto de diferencias parciales.*

DEMOSTRACIÓN. El Corolario 3.10 en [**32**] establece que si q es una potencia de un primo y e es un divisor de $q-1$, entonces, el producto ciclotómico entre una ciclotomía de orden e sobre $\mathbb{F}_q$ y su inverso ciclotómico es uniforme. El Colorario 2.4 del mismo artículo establece que si A es una de las órbitas de una unión de órbitas D y $u \in \mathbb{F}_q$, entonces $uA = \{ux \ : \ x \in A\}$ es otra de las órbitas. En particular, si $(x, y) \in D$ entonces $(-x, -y) \in D$. ■

Podemos ver una demostración alternativa:

Si $0 \leq i \leq e-1$ entonces la i-ésima órbita ciclotómica C_i es una unión disjunta de conjuntos de la forma $V_{i,j} - \{(0, 0)\}$, donde $V_{i,j}$ son subespacios de dimensión 1, pues si $(x, y) \in C_i$ entonces x/y pertenece al conjunto $\{\theta^{i+ke} \ : \ 0 \leq k \leq f-1\}$, y obviamente, lo mismo ocurre para $(\lambda x, \lambda y)$ para todo $\lambda \in \mathbb{F}_q - \{0\}$. El apartado (3) en la página 78 del artículo [**82**] establece que G es un espacio vectorial de dimensión $2s$ sobre un cuerpo finito $\mathbb{F}_q$ y $N_1, N_2, \ldots, N_n$ son n subespacios de dimensión s próximos a ser disjuntos dos a dos (el único elemento en común es el neutro), entonces $D = (N_1 \cup N_2 \cup \ldots \cup N_n) \setminus \{e\}$ es un conjunto de diferencias parciales. Esto demuestra que el resultado del teorema se cumple.

EJEMPLO 4.10. *En el ejemplo 4.7, consideremos el conjunto*

$$D = C_0 \cup C_1 \cup F_{S_1} \cup F_{S_2}.$$

D es un conjunto de diferencias parciales. En efecto, consideremos el multiconjunto de diferencias L

```
gap> L;
[ [ 0, 4 ], [ 0, 3 ], [ 0, 2 ], [ 4, 1 ], [ 4, 0 ], [ 4, 4 ], [ 4, 3 ], [ 4, 2 ], [ 3, 1 ], [ 3, 0 ], [ 3, 4 ],
  [ 3, 3 ], [ 3, 2 ], [ 2, 1 ], [ 2, 0 ], [ 2, 4 ], [ 2, 3 ], [ 2, 2 ], [ 1, 1 ], [ 1, 0 ], [ 1, 4 ], [ 1, 3 ],
  [ 1, 2 ], [ 0, 1 ], [ 0, 4 ], [ 0, 3 ], [ 4, 2 ], [ 4, 1 ], [ 4, 0 ], [ 4, 4 ], [ 4, 3 ], [ 3, 2 ], [ 3, 1 ],
  [ 3, 0 ], [ 3, 4 ], [ 3, 3 ], [ 2, 2 ], [ 2, 1 ], [ 2, 0 ], [ 2, 4 ], [ 2, 3 ], [ 1, 2 ], [ 1, 1 ], [ 1, 0 ],
  [ 1, 4 ], [ 1, 3 ], [ 0, 2 ], [ 0, 1 ], [ 0, 4 ], [ 4, 3 ], [ 4, 2 ], [ 4, 1 ], [ 4, 0 ], [ 4, 4 ], [ 3, 3 ],
  [ 3, 2 ], [ 3, 1 ], [ 3, 0 ], [ 3, 4 ], [ 2, 3 ], [ 2, 2 ], [ 2, 1 ], [ 2, 0 ], [ 2, 4 ], [ 1, 3 ], [ 1, 2 ],
  [ 1, 1 ], [ 1, 0 ], [ 1, 4 ], [ 0, 3 ], [ 0, 2 ], [ 0, 1 ], [ 4, 4 ], [ 4, 3 ], [ 4, 2 ], [ 4, 1 ], [ 4, 0 ],
  [ 3, 4 ], [ 3, 3 ], [ 3, 2 ], [ 3, 1 ], [ 3, 0 ], [ 2, 4 ], [ 2, 3 ], [ 2, 2 ], [ 2, 1 ], [ 2, 0 ], [ 1, 4 ],
  [ 1, 3 ], [ 1, 2 ], [ 1, 1 ], [ 1, 0 ], [ 1, 4 ], [ 1, 3 ], [ 1, 2 ], [ 1, 1 ], [ 0, 4 ], [ 0, 3 ], [ 0, 2 ],
  [ 0, 1 ], [ 4, 0 ], [ 4, 4 ], [ 4, 3 ], [ 4, 2 ], [ 4, 1 ], [ 3, 0 ], [ 3, 4 ], [ 3, 3 ], [ 3, 2 ], [ 3, 1 ],
  [ 2, 0 ], [ 2, 4 ], [ 2, 3 ], [ 2, 2 ], [ 2, 1 ], [ 1, 0 ], [ 1, 4 ], [ 1, 3 ], [ 1, 2 ], [ 0, 1 ], [ 0, 4 ],
  [ 0, 3 ], [ 0, 2 ], [ 4, 1 ], [ 4, 0 ], [ 4, 4 ], [ 4, 3 ], [ 4, 2 ], [ 3, 1 ], [ 3, 0 ], [ 3, 4 ], [ 3, 3 ],
  [ 3, 2 ], [ 2, 1 ], [ 2, 0 ], [ 2, 4 ], [ 2, 3 ], [ 2, 2 ], [ 1, 1 ], [ 1, 0 ], [ 1, 4 ], [ 1, 3 ], [ 0, 2 ],
  [ 0, 1 ], [ 0, 4 ], [ 0, 3 ], [ 4, 2 ], [ 4, 1 ], [ 4, 0 ], [ 4, 4 ], [ 4, 3 ], [ 3, 2 ], [ 3, 1 ], [ 3, 0 ],
  [ 3, 4 ], [ 3, 3 ], [ 2, 2 ], [ 2, 1 ], [ 2, 0 ], [ 2, 4 ], [ 2, 3 ], [ 1, 2 ], [ 1, 1 ], [ 1, 0 ], [ 1, 4 ],
  [ 0, 3 ], [ 0, 2 ], [ 0, 1 ], [ 0, 4 ], [ 4, 3 ], [ 4, 2 ], [ 4, 1 ], [ 4, 0 ], [ 4, 4 ], [ 3, 3 ], [ 3, 2 ],
  [ 3, 1 ], [ 3, 0 ], [ 3, 4 ], [ 2, 3 ], [ 2, 2 ], [ 2, 1 ], [ 2, 0 ], [ 2, 4 ], [ 1, 3 ], [ 1, 2 ], [ 1, 1 ],
  [ 1, 0 ], [ 0, 4 ], [ 0, 3 ], [ 0, 2 ], [ 0, 1 ], [ 4, 4 ], [ 4, 3 ], [ 4, 2 ], [ 4, 1 ], [ 4, 0 ], [ 3, 4 ],
  [ 3, 3 ], [ 3, 2 ], [ 3, 1 ], [ 3, 0 ], [ 2, 4 ], [ 2, 3 ], [ 2, 2 ], [ 2, 1 ], [ 2, 0 ], [ 2, 4 ], [ 2, 3 ],
  [ 2, 2 ], [ 2, 1 ], [ 1, 0 ], [ 1, 4 ], [ 1, 3 ], [ 1, 2 ], [ 1, 1 ], [ 0, 4 ], [ 0, 3 ], [ 0, 2 ], [ 0, 1 ],
  [ 4, 0 ], [ 4, 4 ], [ 4, 3 ], [ 4, 2 ], [ 4, 1 ], [ 3, 0 ], [ 3, 4 ], [ 3, 3 ], [ 3, 2 ], [ 3, 1 ], [ 2, 0 ],
  [ 2, 4 ], [ 2, 3 ], [ 2, 2 ], [ 1, 1 ], [ 1, 0 ], [ 1, 4 ], [ 1, 3 ], [ 1, 2 ], [ 0, 1 ], [ 0, 4 ], [ 0, 3 ],
  [ 0, 2 ], [ 4, 1 ], [ 4, 0 ], [ 4, 4 ], [ 4, 3 ], [ 4, 2 ], [ 4, 1 ], [ 4, 0 ], [ 4, 4 ], [ 3, 3 ], [ 3, 2 ],
  [ 2, 1 ], [ 2, 0 ], [ 2, 4 ], [ 2, 3 ], [ 1, 2 ], [ 1, 1 ], [ 1, 0 ], [ 1, 4 ], [ 1, 3 ], [ 0, 2 ], [ 0, 1 ],
  [ 0, 4 ], [ 0, 3 ], [ 4, 2 ], [ 4, 1 ], [ 4, 0 ], [ 4, 4 ], [ 4, 3 ], [ 3, 2 ], [ 3, 1 ], [ 3, 0 ], [ 3, 4 ],
  [ 3, 3 ], [ 2, 2 ], [ 2, 1 ], [ 2, 0 ], [ 2, 4 ], [ 1, 3 ], [ 1, 2 ], [ 1, 1 ], [ 1, 0 ], [ 1, 4 ], [ 1, 3 ],
  [ 0, 2 ], [ 0, 1 ], [ 0, 4 ], [ 4, 3 ], [ 4, 2 ], [ 4, 1 ], [ 4, 0 ], [ 4, 4 ], [ 3, 3 ], [ 3, 2 ], [ 3, 1 ],
  [ 3, 0 ], [ 3, 4 ], [ 2, 3 ], [ 2, 2 ], [ 2, 1 ], [ 2, 0 ], [ 1, 4 ], [ 1, 3 ], [ 1, 2 ], [ 1, 1 ], [ 1, 0 ],
  [ 0, 4 ], [ 0, 3 ], [ 0, 2 ], [ 0, 1 ], [ 4, 4 ], [ 4, 3 ], [ 4, 2 ], [ 4, 1 ], [ 4, 0 ], [ 3, 4 ], [ 3, 3 ],
  [ 3, 2 ], [ 2, 2 ], [ 1, 1 ], [ 1, 0 ], [ 1, 4 ], [ 1, 3 ], [ 1, 2 ], [ 0, 1 ], [ 0, 4 ], [ 0, 3 ], [ 0, 2 ],
  [ 4, 1 ], [ 4, 0 ], [ 4, 4 ], [ 4, 3 ], [ 4, 2 ], [ 3, 1 ], [ 3, 0 ], [ 3, 4 ], [ 3, 3 ], [ 2, 2 ], [ 2, 1 ],
  [ 2, 0 ], [ 2, 4 ], [ 2, 3 ], [ 1, 2 ], [ 1, 1 ], [ 1, 0 ], [ 1, 4 ], [ 1, 3 ], [ 0, 2 ], [ 0, 1 ], [ 0, 4 ],
  [ 0, 3 ], [ 4, 2 ], [ 4, 1 ], [ 4, 0 ], [ 4, 4 ], [ 4, 3 ], [ 3, 2 ], [ 3, 1 ], [ 3, 0 ], [ 3, 4 ], [ 2, 3 ],
  [ 2, 2 ], [ 2, 1 ], [ 2, 0 ], [ 2, 4 ], [ 1, 3 ], [ 1, 2 ], [ 1, 1 ], [ 1, 0 ], [ 1, 4 ], [ 0, 3 ], [ 0, 2 ],
  [ 0, 1 ], [ 0, 4 ], [ 4, 3 ], [ 4, 2 ], [ 4, 1 ], [ 4, 0 ], [ 4, 4 ], [ 3, 3 ], [ 3, 2 ], [ 3, 1 ], [ 3, 0 ],
  [ 2, 4 ], [ 2, 3 ], [ 2, 2 ], [ 2, 1 ], [ 2, 0 ], [ 1, 4 ], [ 1, 3 ], [ 1, 2 ], [ 1, 1 ], [ 1, 0 ], [ 0, 4 ],
  [ 0, 3 ], [ 0, 2 ], [ 0, 1 ], [ 4, 4 ], [ 4, 3 ], [ 4, 2 ], [ 4, 1 ], [ 4, 0 ], [ 4, 4 ], [ 4, 3 ], [ 4, 2 ],
  [ 4, 1 ], [ 3, 0 ], [ 3, 4 ], [ 3, 3 ], [ 3, 2 ], [ 3, 1 ], [ 2, 0 ], [ 2, 4 ], [ 2, 3 ], [ 2, 2 ], [ 2, 1 ],
  [ 1, 0 ], [ 1, 4 ], [ 1, 3 ], [ 1, 2 ], [ 1, 1 ], [ 0, 4 ], [ 0, 3 ], [ 0, 2 ], [ 0, 1 ], [ 4, 0 ], [ 4, 4 ],
  [ 4, 3 ], [ 4, 2 ], [ 3, 1 ], [ 3, 0 ], [ 3, 4 ], [ 3, 3 ], [ 3, 2 ], [ 2, 1 ], [ 2, 0 ], [ 2, 4 ], [ 2, 3 ],
  [ 2, 2 ], [ 1, 1 ], [ 1, 0 ], [ 1, 4 ], [ 1, 3 ], [ 1, 2 ], [ 0, 1 ], [ 0, 4 ], [ 0, 3 ], [ 0, 2 ], [ 4, 1 ],
  [ 4, 0 ], [ 4, 4 ], [ 4, 3 ], [ 3, 2 ], [ 3, 1 ], [ 3, 0 ], [ 3, 4 ], [ 3, 3 ], [ 2, 2 ], [ 2, 1 ], [ 2, 0 ],
  [ 2, 4 ], [ 2, 3 ], [ 1, 2 ], [ 1, 1 ], [ 1, 0 ], [ 1, 4 ], [ 1, 3 ], [ 0, 2 ], [ 0, 1 ], [ 0, 4 ], [ 0, 3 ],
  [ 4, 2 ], [ 4, 1 ], [ 4, 0 ], [ 4, 4 ], [ 3, 3 ], [ 3, 2 ], [ 3, 1 ], [ 3, 0 ], [ 3, 4 ], [ 2, 3 ], [ 2, 2 ],
  [ 2, 1 ], [ 2, 0 ], [ 2, 4 ], [ 1, 3 ], [ 1, 2 ], [ 1, 1 ], [ 1, 0 ], [ 1, 4 ], [ 0, 3 ], [ 0, 2 ], [ 0, 1 ],
  [ 0, 4 ], [ 4, 3 ], [ 4, 2 ], [ 4, 1 ], [ 4, 0 ], [ 3, 4 ], [ 3, 3 ], [ 3, 2 ], [ 3, 1 ], [ 3, 0 ], [ 2, 4 ],
  [ 2, 3 ], [ 2, 2 ], [ 2, 1 ], [ 2, 0 ], [ 1, 4 ], [ 1, 3 ], [ 1, 2 ], [ 1, 1 ], [ 1, 0 ], [ 0, 4 ], [ 0, 3 ],
  [ 0, 2 ], [ 0, 1 ] ]                                                                                          ,
```

el cual hemos generado en GAP con el código

```
C0:=[[1,1],[1,4],[2,2],[2,3],[3,3],[3,2],[4,4],[4,1]];
C1:=[[1,2],[1,3],[2,1],[2,4],[3,1],[3,4],[4,3],[4,2]];
F1:=[[1,0],[2,0],[3,0],[4,0]];
F2:=[[0,1],[0,2],[0,3],[0,4]];
D:=Union(C0,C1,F1,F2);
L:=[];
for i in [1..Size(D)] do
for j in [1..Size(D)] do
if j <> i then
        Add(L, (D[i]-D[j]) mod 5);
fi;
od;
od;
```

Usando el código

```
N:=[];
for i in [1..Size(D)] do
Add(N,Number(L,x->x=D[i]));
od;
```

Obtenemos que cada elemento no nulo aparece 23 veces en el multiconjunto, como vemos a continuación

```
gap> N;
[ 23, 23, 23, 23, 23, 23, 23, 23, 23, 23, 23, 23, 23, 23, 23, 23, 23, 23, 23, 23, 23, 23, 23 ]
```

Así, D se trata de un conjunto de diferencias parciales.

Por lo tanto, las construcciones en el teorema anterior están en la frontera de construcciones ciclotómicas y de "partial spread" de conjuntos de diferencias parciales.

En base a esto, nos podríamos preguntar si estos conjuntos de diferencias parciales tienen una estructura más rica con respecto a sus grupos de automorfismos.

Resulta que los conjuntos de diferencias parciales obtenidos con las construcciones del teorema anterior tienen un grupo de automorfismos mucho más grande que los grupos de automorfismos prescritos obtenidos de la acción multiplicativa del grupo H que origina la ciclotomía sobre el grupo aditivo de $F_q \times F_q$.

Se han realizado algunos cálculos numéricos utilizando el paquete matemático GAP ([**61**]) y, para $q = 3$, $e = 2$ el grupo de automorfismos esperado en general de la ciclotomía estándar es el producto $G = G_1G_2$, donde G_1 es el grupo de orden 9 derivado de la acción regular del grupo aditivo de $\mathbb{F}_3 \times \mathbb{F}_3$, G_2 es el grupo de orden 2 derivado del grupo H asociado a la ciclotomía. El producto es de orden 18, pero los grupos completos de automorfismos tienen órden 72, 1296 y 362880 dependiendo de las órbitas que se unen.

A pesar de solo exponer aquí un caso partícular bastante pequeño, con casos más grandes los resutados arrojados por el paquete GAP excedían la memoria del mismo, por lo que se obtenían grupos completos de automorfismos de órdenes muy superiores a los esperados.

Aún así, en la siguiente tabla veremos, para los casos $e = 2$, $q = 5$ y $e = 2$, $q = 7$, la cantidad de generadores de los grupos de automorfismos diferentes que se obtienen al unir de diversas maneras las órbitas

TABLA 4.1. Grupos de automorfismos obtenidos a partir de uniones de órbitas ciclotómicas

q	Órbitas Unidas	Número de generadores
5	$[\,]$	24
	$[C_0]$	5
	$[C_1]$	5
	$[(\mathbb{F}_5 \setminus \{0\}) \times \{0\}]$	20
	$[\{0\} \times (\mathbb{F}_5 \setminus \{0\})]$	4
	$[C_0, C_1]$	7
	$[C_0, (\mathbb{F}_5 \setminus \{0\}) \times \{0\}]$	3
	$[C_0, \{0\} \times (\mathbb{F}_5 \setminus \{0\})]$	4
	$[C_1, (\mathbb{F}_5 \setminus \{0\}) \times \{0\}]$	3
	$[C_1, \{0\} \times (\mathbb{F}_5 \setminus \{0\})]$	4
	$[(\mathbb{F}_5 \setminus \{0\}) \times \{0\}, \{0\} \times (\mathbb{F}_5 \setminus \{0\})]$	8
	$[C_0, C_1, (\mathbb{F}_5 \setminus \{0\}) \times \{0\}]$	24
	$[C_0, C_1, \{0\} \times (\mathbb{F}_5 \setminus \{0\})]$	20
	$[C_0, (\mathbb{F}_5 \setminus \{0\}) \times \{0\}, \{0\} \times (\mathbb{F}_5 \setminus \{0\})]$	5
	$[C_1, (\mathbb{F}_5 \setminus \{0\}) \times \{0\}, \{0\} \times (\mathbb{F}_5 \setminus \{0\})]$	5
	$[C_0, C_1, (\mathbb{F}_5 \setminus \{0\}) \times \{0\}, \{0\} \times (\mathbb{F}_5 \setminus \{0\})]$	24
7	$[\,]$	48
	$[C_0]$	4
	$[C_1]$	4
	$[(\mathbb{F}_7 \setminus \{0\}) \times \{0\}]$	42
	$[\{0\} \times (\mathbb{F}_7 \setminus \{0\})]$	48
	$[C_0, C_1]$	11
	$[C_0, (\mathbb{F}_7 \setminus \{0\}) \times \{0\}]$	3
	$[C_0, \{0\} \times (\mathbb{F}_7 \setminus \{0\})]$	4
	$[C_1, (\mathbb{F}_7 \setminus \{0\}) \times \{0\}]$	3
	$[C_1, \{0\} \times (\mathbb{F}_7 \setminus \{0\})]$	4
	$[(\mathbb{F}_7 \setminus \{0\}) \times \{0\}, \{0\} \times (\mathbb{F}_7 \setminus \{0\})]$	12
	$[C_0, C_1, (\mathbb{F}_7 \setminus \{0\}) \times \{0\}]$	48
	$[C_0, C_1, \{0\} \times (\mathbb{F}_7 \setminus \{0\})]$	42
	$[C_0, (\mathbb{F}_7 \setminus \{0\}) \times \{0\}, \{0\} \times (\mathbb{F}_7 \setminus \{0\})]$	4
	$[C_1, (\mathbb{F}_7 \setminus \{0\}) \times \{0\}, \{0\} \times (\mathbb{F}_7 \setminus \{0\})]$	4
	$[C_0, C_1, (\mathbb{F}_7 \setminus \{0\}) \times \{0\}, \{0\} \times (\mathbb{F}_7 \setminus \{0\})]$	48

Capítulo 5

CUASI MATRICES DE DIFERENCIAS CÍCLICAS

En este capítulo se abordarán y ampliarán los temas trabajados en el artículo [**90**].

En dicho artículo analizamos algunas ventajas prácticas de las cuasi matrices de diferencias sobre las matrices de diferencias para obtener arreglos ortogonales con parámetros dados. También analizamos la existencia de cuasi matrices de diferencias sobre grupos cíclicos que originan arreglos ortogonales con $t = 2$ y $\lambda = 1$, demostrando su existencia para algunos parámetros dados. Además, presentamos un modelo de programación entera para encontrar tales cuasi matrices de diferencias y también un algoritmo de búsqueda local bimodal para obtenerlos.

Damos una conjetura relacionada con las distribuciones de diferencias a lo largo de las filas y columnas de matrices cuadradas arbitrarias con entradas en un grupo cíclico en posiciones fuera de la diagonal principal que muestra una simetría especial, y la demostramos cuando la matriz es una cuasi matriz de diferencias.

La simetría es útil cuando se trata de resolver ciertos problemas matemáticos difíciles ([**25**], [**105**]). En el caso de arreglos ortogonales sus simetrías son permutaciones de símbolos o columnas (o combinaciones de ambos) que conservan su estructura, y constituyen sus grupos completos de automorfismos (más generalmente, estamos interesados en subgrupos de estos grupos completos de automorfismos, que llamamos grupos de automorfismos).

El estudio de los grupos de automorfismos de diferentes clases de estructuras combinatorias permite determinar ciertas propiedades y facilita el hallazgo de construcciones

para ciertos conjuntos de parámetros. Los casos en que la acción del grupo de automorfismos es regular o, más generalmente, semirregular, son especialmente interesantes. Esto es lo que sucede, por ejemplo, en el caso de diseños combinatorios ([**14**], [**20**], [**116**]), grafos no dirigidos fuertemente regulares ([**77**], [**79**]), o grafos dirigidos fuertemente regulares ([**2**], [**3**]).

En particular, Bose y Bush estudiaron en [**8**] los OAs que admiten un grupo de automorfismos de símbolos abeliano que actúa regularmente sobre el conjunto de símbolos. Estos tipos de OAs son generados por los llamados esquemas de diferencias. Se formalizan con más generalidad para grupos arbitrarios con el concepto de matriz de diferencias [**19**]. Usamos ambos términos indistintamente ya que solo consideramos grupos abelianos en este capítulo. Como se describe en [**53**], una matriz $r \times c$ con entradas en un grupo abeliano G de orden s se llama un esquema de diferencias basado en G si para todos i y j con $1 \leq i, j \leq c$ y $i \neq j$ el vector de diferencias entre las columnas i-ésima y j-ésima de la matriz contiene todos los elementos de G el mismo número de veces. Si usamos λ para denotar este número de veces, entonces $r = \lambda s$, y en este caso decimos que el esquema de diferencias es un $D(r, c, s)$. Obviamente, un $D(r, c, s)$ genera un $OA(rs, c, s, 2)$, tomando las traslaciones de las filas obtenidas al añadir el mismo elemento x de G a todas sus coordenadas para $x \in G$. Cuando el grupo en el que está basado un esquema de diferencia es cíclico, se dice que éste es cíclico. Cuando $\lambda = 1$, escribiremos $D(c, s)$ para denotar a un $D(s, c, s)$.

Los arreglos ortogonales que admiten un grupo de automorfismos de símbolos que fijan uno de los símbolos y actuan regularmente sobre los otros han sido estudiados en la literatura. Se pueden determinar por casos especiales de cuasi matrices de diferencias ([**1**], [**19**], [**114**]).

DEFINICIÓN 5.1. ***[19] Dado un grupo abeliano*** G ***de orden*** n***, una*** $(n, k; \lambda, \mu; u)$***-cuasi matriz de diferencias es una matriz*** $Q = (q_{ij})$ ***con k filas y*** $\lambda(n - 1 + 2u) + \mu$ ***columnas con entradas ya sean vacías (generalmente denotadas por −) o un elemento en*** G***, de modo que cada fila contiene exactamente*** λu ***entradas vacías, cada columna contiene como máximo una entrada vacía, y para cada*** $1 \leq i < j \leq k$ ***el multiconjunto***

$$\{q_{il} - q_{jl} \ : \ 1 \leq l \leq \lambda(n - 1 + 2u) + \mu, \text{ con } q_{il} \text{ y } q_{jl} \text{ no vacíos}\}$$

contiene cada elemento de G ***distinto de*** 0 ***exactamente*** λ ***veces y*** 0 ***exactamente*** μ ***veces.***

EJEMPLO 5.2. *Consideremos el grupo abeliano* $\mathbb{Z}_3$*. La siguiente matriz es una* $(3,3;1,1;1)$*-cuasi matriz de diferencias.*

$$\begin{pmatrix} 0 & 0 & 0 & 0 & - \\ 0 & 1 & 2 & - & 0 \\ 2 & 1 & - & 0 & 1 \end{pmatrix}.$$

En efecto, podemos ver que dicha matriz tiene entradas o bien vacías, o bien elementos de $\mathbb{Z}_3$*. La matriz tiene* $k = 3$ *filas y* $\lambda(n-1+2u)+\mu = 5$ *columnas. También podemos ver que cada fila contiene exactamente* $\lambda u = 1$ *entrada vacía y cada columna tiene a lo mucho una entrada vacía. Finalmente, no es difícil ver que los multiconjuntos de diferencias entre dos pares cualesquiera de filas (excluyendo aquellos elementos vacíos) será el conjunto* $\{0,1,2\}$ *y podemos ver que el elemento* 0 *aparece exactamente* $\mu = 1$ *veces y los elementos distintos de* 0 *aparecen* $\lambda = 1$ *veces.*

Las cuasi matrices de diferencias que vamos a analizar en este capítulo son las que originan OAs de fuerza 2 e índice unidad, que son los que tienen una relación directa con los grafos fuertemente regulares. También nos interesa el caso en que el grupo G es cíclico, porque es lo suficientemente potente como para garantizar la existencia de OAs para muchos de los parámetros actualmente conocidos a pesar de la sencillez de la estructura del grupo. Nos referiremos a tales matrices como cuasi matrices cíclicas de diferencias.

DEFINICIÓN 5.3. *Decimos que un arreglo ortogonal de fuerza* 2 *e índice unitario es un arreglo ortogonal cuasi cíclico si admite un grupo de automorfismos cíclico que fija uno de los símbolos y actúa regularmente en los otros.*

Este tipo de acciones que fijan un elemento y actuan regularmente (y, más generalmente, semirregularmente) en los otros elementos ha sido considerado en la literatura para otros tipos de estructuras combinatorias (normalmente se denominan 1-rotacionales), como por ejemplo en [**76**] para grafos fuertemente regulares y en [**14**] para diseños combinatorios.

A continuación daremos un ejemplo sencillo. Siguiendo la notación en los artículos antes mencionados [**14**] y [**76**]. Usaremos ∞ para denotar el símbolo fijado por el grupo y los otros símbolos por $0,\ldots,n-2$.

EJEMPLO 5.4. *El arreglo*

$$\begin{pmatrix} 0 & 0 & \infty & 1 \\ 0 & 1 & 1 & \infty \\ 0 & \infty & 0 & 0 \\ 1 & 0 & 0 & \infty \\ 1 & 1 & \infty & 0 \\ 1 & \infty & 1 & 1 \\ \infty & 0 & 1 & 0 \\ \infty & 1 & 0 & 1 \\ \infty & \infty & \infty & \infty \end{pmatrix}$$

es un $OA(4,3)$ *que admite el automorfismo que fija el símbolo* ∞ *y permuta cíclicamente los símbolos* 0 *y* 1*. Por supuesto es suficiente dar un solo representante para cada órbita de la acción del grupo en el conjunto de filas para determinarlo, y luego podemos ordenar lexicográficamente las filas con respecto al orden en que* $0 < 1 < \infty$*, obteniendo el subarreglo*

$$\begin{pmatrix} 0 & 0 & \infty & 1 \\ 0 & 1 & 1 & \infty \\ 0 & \infty & 0 & 0 \\ \infty & 0 & 1 & 0 \\ \infty & \infty & \infty & \infty \end{pmatrix}$$

Si eliminamos la última fila (la que tiene todas sus entradas iguales a ∞*), calculamos la transpuesta de la matriz y luego reemplazamos los infinitos con el símbolo "–" obtenemos la siguiente* $(2,4;1,1;1)$*-cuasi matriz de diferencias:*

$$\begin{pmatrix} 0 & 0 & 0 & - \\ 0 & 1 & - & 0 \\ - & 1 & 0 & 1 \\ 1 & - & 0 & 0 \end{pmatrix}$$

De forma más general, las matrices que estamos considerando son $(n-1,m;1,1;1)$-cuasi matrices cíclicas de diferencias. Denotaremos a tal matriz como $CMCD(m,n)$. Cuando se utilizado el citado orden lexicográfico diremos que la cuasi matriz de diferencias está en forma canónica.

Un problema importante en el estudio de arreglos ortogonales consiste en determinar el número mínimo de ejecuciones N en cualquier $OA(N, k, s, t)$, para valores dados de k, s y t. Denotamos este valor mínimo por $F(k, s, t)$.

Un problema relacionado, que aborda la cuestión de la existencia de arreglos ortogonales de una manera ligeramente diferente, se puede formular de la siguiente manera. Podemos observar que si eliminamos factores de un $OA(N, k, s, t)$ podemos obtener un $OA(N, k', s, t)$ para cualquier k' con $t \leq k' \leq k$. Entonces, para valores fijos de N, s y t se puede resolver el problema de determinar todos los valores de k para los cuales existe un $OA(N, k, s, t)$ siempre que conozcamos el número máximo de factores k en cualquier $OA(N, k, s, t)$. Denotamos este valor máximo por $f(N, s, t)$.

Podemos ver claramente que

$$\begin{aligned} F(k, s, t) &= \text{mín}\{N \ : \ f(N, s, t) \geq k\}, \\ f(N, s, t) &\leq \text{máx}\{k \ : \ F(k, s, t) \leq N\}. \end{aligned}$$

Por tanto, Los valores de $f(N, s, t)$ determinan completamente los de F(k, s, t), aunque lo contrario no es cierto. Los valores de $F(k, s, t)$ solo proporcionan cotas superiores en los valores de $f(N, s, t)$, por lo que determinar $f(N, s, t)$ es un problema más difícil que el problema de determinar $F(k, s, t)$.

Uno de las primeras cotas superiores en el número máximo de factores en un arreglo ortogonal fue obtenido por Rao [**102**]. Las cotas para el número de factores aparecen implícitamente. El resultado para $t = 2$ ya se conocía por el trabajo de Plackett y Burman [**99**].

TEOREMA 5.5 (Desigualdad de Rao). *[[53] Theorem 2.1] Los parámetros de un* $OA(N, k, s, t)$ *satisfacen las siguientes desigualdades:*

$$N \geq \sum_{i=0}^{u} \binom{k}{i} (s-1)^i, \textit{ si } t = 2u,$$

$$N \geq \sum_{i=0}^{u} \binom{k}{i} (s-1)^i + \binom{k-1}{u} (s-1)^{u+1}, \textit{ si } t = 2u+1,$$

para $u \geq 0$.

El siguiente teorema fue probado por Jungnickel en [**68**], pero yo hice una demostración alternativa que presentaré a continuación:

TEOREMA 5.6. *Si existe un* $D(r, c, s)$ *entonces* $c \leq r$.

DEMOSTRACIÓN. Es suficiente con probar que no existe un arreglo ortogonal $A = OA(n+1, n)$ tal que el ciclo $(0, 1, \ldots, n-1)$ es un automorfismo de A.

Por la desigualdad de Rao, un arreglo ortogonal $OA(m, n)$ satisface que $m \leq n+1$. Sea $A = (a_{ij})$ un arreglo ortogonal, con $a_{ij} \in \{0, 1, \ldots, n-1\}$ para todo $(i, j) \in \{1, \ldots, n^2\} \times \{1, \ldots, n+1\}$, el cual satisface que el ciclo $\gamma = (0, \ldots, n-1)$ es un automorfismo de A. Podemos escribir el arreglo ortogonal como $A = (B_i)_{i \in \{0,\ldots,n-1\}}$, con

$$B_0 = \begin{pmatrix} 0 & 0 & \\ 0 & 1 & \\ \vdots & \vdots & C \\ 0 & n-2 & \\ 0 & n-1 & \end{pmatrix} \quad \text{y} \quad B_{i+1} = \gamma(B_i) \quad \text{con } i \in \{0, 1, \ldots, n-2\},$$

donde C es una submatriz de A de tamaño $n \times (n-1)$. Debemos probar que no existe una tal matriz C.

En caso de existir, tendría la forma

$$C = \begin{pmatrix} c_{0,0} & c_{0,1} & \cdots & c_{0,n-2} \\ c_{1,0} & c_{1,1} & \cdots & c_{1,n-2} \\ \vdots & \vdots & \ddots & \vdots \\ c_{n-1,0} & c_{n-1,2} & \cdots & c_{n-1,n-2} \end{pmatrix}.$$

Podemos observar que, como γ es un automorfismo de A, la siguiente matriz H es una submatriz de A:

$$H = \begin{pmatrix} 0 & 0 & c_{0,0} & c_{0,1} & \cdots & c_{0,n-2} \\ 1 & 1 & \gamma(c_{0,0}) & \gamma(c_{0,1}) & \cdots & \gamma(c_{0,n-2}) \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ n-1 & n-1 & \gamma^{n-1}(c_{0,0}) & \gamma^{n-1}(c_{0,1}) & \cdots & \gamma^{n-1}(c_{0,n-2}) \\ 0 & n-1 & c_{n-1,0} & c_{n-1,1} & \cdots & c_{n-1,n-2} \\ 1 & 0 & \gamma(c_{n-1,0}) & \gamma(c_{n-1,1}) & \cdots & \gamma(c_{n-1,n-2}) \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ n-1 & n-2 & \gamma^{n-1}(c_{n-1,0}) & \gamma^{n-1}(c_{n-1,1}) & \cdots & \gamma^{n-1}(c_{n-1,n-2}) \end{pmatrix}.$$

En general, $c_{0,j} \in \{c_{n-1,j}, \gamma(c_{n-1,j}), \ldots, \gamma^{n-1}(c_{n-1,j})\}$ para $j \in \{0. \ldots, n-2\}$.

Nótese que $c_{0,0} \neq c_{n-1,0}$ y $c_{0,0} \neq \gamma(c_{n-1,0})$; así, $c_{0,0}$ tiene $n-2$ posibilidades ($c_{0,0} \in \{\gamma^2(c_{n-1,0}), \ldots, \gamma^{n-1}(c_{n-1,0})\}$). Por otro lado, podemos observar que $c_{0,1} \neq c_{n-1,1}$, $c_{0,1} \neq \gamma(c_{n-1,1})$ y, como $c_{0,0} = \gamma^k(c_{n-1,0})$ para algún $k \in \{2, \ldots, n-1\}$, entonces $c_{0,1}$ tiene $n-3$ posibilidades ($c_{0,1} \in \{\gamma^2(c_{n-1,1}), \ldots, \gamma^{n-1}(c_{n-1,1})\} \setminus \{\gamma^k(c_{n-1,1})\}$).

Siguiendo este procedimiento llegamos a que $c_{0,n-2}$ tiene 0 posibilidades, esto es, C no existe. ■

Una consecuencia del teorema anterior es que la cota de Rao nunca se alcanza para los arreglos ortogonales derivados de esquemas de diferencias, porque la cota de Rao establece que $m \leq n+1$ para un $OA(m,n)$. La situación es diferente para las $CMCD$ ya que, por ejemplo, el ejemplo dado anteriormente muestra que existe una $CMCD(4,3)$. Así, la simetría en los esquemas de diferencias se gana a costa de perder factores, es decir, el número de factores es menor que el máximo valor permitido por la cota de Rao, pero con una $CMCD$ todavía tenemos un grupo de simetría con una acción cerca de ser regular y al mismo tiempo se alcanza el número máximo de factores que aparecen en la cota de Rao.

Aunque el siguiente teorema fue probado, usando otra notación, por Ge en [**39**], Lemma 3.1; al igual que con el teorema anterior, yo hice de forma independiente una demostración alternativa que presentaré a continuación:

TEOREMA 5.7. *Si n es un número par, no existe un esquema de diferencias cíclico* $A = D(m,n)$ *para todo número entero* $m \geq 3$.

DEMOSTRACIÓN. Es suficiente con probar que no existe un esquema de diferencias cíclico $A = D(3,n)$ para todo n par.

Consideremos un arreglo ortogonal $A = (a_{ij})$ donde $a_{ij} \in \{0,1,\ldots,n-1\}$ para todo $(i,j) \in \{1,\ldots,n^2\} \times \{1,2,3\}$ de tal forma que el ciclo $\gamma = (0,1,\ldots,n-1)$ es un automorfismo de A. Podemos escribir el arreglo ortogonal como $A = (B_i)_{i \in \{0,\ldots,n-1\}}$ donde cada bloque B_i tiene la forma

$$B_1 = \begin{pmatrix} 0 & 0 & \\ 0 & 1 & \\ \vdots & \vdots & C \\ 0 & n-2 & \\ 0 & n-1 & \end{pmatrix}, \qquad B_{i+1} = \gamma(B_i),$$

donde $C = (c_i)_{i \in \{0,\ldots,n-1\}}$ es una matriz $n \times 1$ con $c_i \in \{0,\ldots,n-1\}$ y $c_i \neq c_j$ para todo $i \neq j$.

Nótese que podemos escribir cada fila de A como

$$a \qquad a+b \mod n \qquad \gamma^a(c_b)$$

para todos $a, b \in \{0, \dots n-1\}$.

Podemos observar que para todo $r \in \{1, \dots, n-1\}$, existe un $k_r \in \{1, \dots, n-1\}$ tal que $c_0 = \gamma^{k_r}(c_r)$. Por tanto, algunas filas de A son de la forma

$$\begin{array}{lll} 0 & 0 & c_0 \\ k_r & (k_r + r) \mod n & c_0 \end{array}$$

donde, para todo $r \in \{1, \dots, n-1\}$, k_r satisface

i. $k_i \neq k_j$ para todo $i \neq j$.

ii. $k_i + i \not\equiv (k_j + j) \mod n$ para todo $i \neq j$.

iii. $k_i + i \not\equiv 0 \mod n$ para todo $i \in \{1, \dots, n-1\}$.

Nótese que encontrar el vector $(c_i)_{i \in \{0,\dots,n-1\}}$ es equivalente a encontrar la familia $\{k_r\}_{r \in \{1,\dots,n-1\}}$, ya que, como $c_0 \in \{0, \dots, n-1\}$, $c_r = \gamma^{n-k_r}(c_0)$ para todo $r \in \{1, \dots, n-1\}$.

Por reducción al absurdo, vamos a suponer que existe tal familia $\{k_r\}_{r \in \{1,\dots,n-1\}}$.

Como $\{k_j\}_{j \in \{1,\dots,n-1\}} = \{1, \dots, n-1\}$, se tiene que

$$\sum_{j=1}^{n-1} k_j \equiv \frac{n(n-1)}{2} \mod n.$$

Nótese que

$$\sum_{j=1}^{n-1}(k_j + j) = \sum_{j=1}^{n-1} k_j + \sum_{j=1}^{n-1} j = \frac{n(n-1)}{2} + \frac{n(n-1)}{2} = n(n-1) \equiv 0 \mod n.$$

Además, como $\{(k_j + j) \mod n\}_{j \in \{1,\dots,n-1\}} = \{1, \dots, n-1\}$, se tiene que

$$\sum_{j=1}^{n-1}(k_j + j) = \frac{n(n-1)}{2}.$$

Esto es una contradicción, pues si n es par entonces $\dfrac{n(n-1)}{2} \not\equiv 0 \mod n$. ■

Como consecuencia del teorema, no existe un $D(3, 4)$. No obstante, el siguiente ejemplo muestra la existencia de una $CMCD(5, 4)$.

EJEMPLO 5.8. *El arreglo*

$$\begin{pmatrix} 0 & 0 & 0 & - & 2 \\ 0 & 1 & 2 & 1 & - \\ 0 & 2 & - & 0 & 0 \\ 0 & - & 1 & 2 & 1 \\ - & 0 & 2 & 2 & 0 \end{pmatrix}$$

es una $CMCD(5, 4)$.

Observemos que no podemos eliminar de las hipótesis del teorema la condición de que el arreglo ortogonal asociado sea de índice unitario. Por ejemplo, el arreglo ortogonal obtenido del siguiente esquema de diferencias tiene 4 símbolos, 3 factores y $\lambda = 2$, y admite al grupo cíclico C_4 como un grupo de automorfismos:

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 3 \\ 0 & 1 & 2 \\ 0 & 1 & 3 \\ 0 & 2 & 1 \\ 0 & 2 & 2 \\ 0 & 3 & 0 \\ 0 & 3 & 1 \end{pmatrix}.$$

A continuación, vamos a introducir algunas construcciones de $CMCD$s, y en particular proporcionamos un modelo de programación entera para encontrar $CMCD$s y un Algoritmo de búsqueda local bimodal que nos permite obtener ciertas $CMCD$s.

Primero, demostremos que para cualquier n y $m = 3$, existe una $CMCD$. En las siguientes dos proposiciones considereamos las $CMCD$s en forma canónica, es decir, si $Q = (q_{i,j})$ es la matriz, entonces

$$q_{1,j} = \begin{cases} 0, & \text{si} \quad 1 \leq j < n+1 \\ -, & \text{si} \quad\quad j = n+1 \end{cases},$$

$$q_{2,j} = \begin{cases} j-1, & \text{si} \quad 1 \leq j < n \\ -, & \text{si} \quad\quad j = n \\ 0, & \text{si} \quad j = n+1 \end{cases}$$

(asociando, por supuesto, la coclase correspondiente en el grupo cíclico $\mathbb{Z}/(n-1)\mathbb{Z}$ a un número natural). Por lo tanto, para obtener una $CMCD$ con $m = 3$ necesitamos dar solo los valores $q_{3,j}$. Para ello, damos las siguientes dos proposiciones.

PROPOSICIÓN 5.9. *Si n es par, entonces la matriz $Q = (q_{ij})$ con*

$$q_{3,j} = \begin{cases} n-j-2, & \textbf{\textit{si}} \quad 1 \leq j \leq n-2 \\ -, & \textbf{\textit{si}} \qquad j = n-1 \\ n-2, & \textbf{\textit{si}} \qquad j = n \\ 0, & \textbf{\textit{si}} \qquad j = n+1 \end{cases}$$

es una $CMCD(3, n)$.

DEMOSTRACIÓN. Si escribimos Q de forma matricial obtenemos

$$Q = \begin{pmatrix} 0 & 0 & \dots & 0 & 0 & 0 & 0 & - \\ 0 & 1 & \dots & n-4 & n-3 & n-2 & - & 0 \\ n-3 & n-4 & \dots & 1 & 0 & - & n-2 & 0 \end{pmatrix}$$

Lo primero que vemos claramente es que la matriz Q tiene $k = 3$ filas y $n+1$ columnas ($\lambda(n-2+2u)+\mu$, donde $\lambda = 1$, $u = 1$ y $\mu = 1$). Cada fila tiene exactamente $u = 1$ entrada vacía $-$. Vemos que las columnas $n-1$, n y $n+1$ contienen un único elemento vacío y las demás columnas no contienen elementos vacíos. Esto es, cada columna contiene como mucho un elemento vacío.

Finalmente, para todos $1 \leq i < j \leq 3$, el multiconjunto

$$\{q_{il} - q_{jl} \ : \ 1 \leq l \leq n+1 \text{ con } q_{il} \text{ y } q_{jl} \text{ no vacíos}\}$$

es, denotado por extensión:

- $i = 1, j = 2 : \{0, n-2, \dots, 3, 2, 1\}$.
- $i = 1, j = 3 : \{2, 3, \dots, n-2, 0\}$.
- $i = 2, j = 3 : \{2, 4, \dots, n-2, 1, 3, \dots n-5, n-3, 0\}$.

Podemos ver claramente que en cualquiera de los tres multiconjuntos, cada elemento de $\mathbb{Z}/(n-1)\mathbb{Z}$ está exactamente una vez ($\lambda = \mu = 1$). ■

PROPOSICIÓN 5.10. *Si n es impar, entonces la matriz $Q = (q_{ij})$ con*

$$q_{3,j} = \begin{cases} 2j-2, & \textbf{\textit{si}} \quad 1 \leq j \leq \frac{n-1}{2} \\ 2\left(j - \frac{n-1}{2}\right) - 1, & \textbf{\textit{si}} \quad \frac{n+1}{2} \leq j \leq n-2 \\ -, & \textbf{\textit{si}} \quad j = n-1 \\ n-2, & \textbf{\textit{si}} \quad j = n \\ \frac{n-1}{2}, & \textbf{\textit{si}} \quad j = n+1 \end{cases}$$

es una $CMCD(3, n)$.

DEMOSTRACIÓN. Si escribimos Q de forma matricial obtenemos

$$Q = \begin{pmatrix} 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 & 0 & - \\ 0 & 1 & \dots & \dots & \dots & \dots & \dots & n-3 & n-2 & - & 0 \\ 0 & 2 & \dots & n-3 & 1 & 3 & \dots & n-4 & - & n-2 & \frac{n-1}{2} \end{pmatrix}$$

Lo primero que vemos claramente es que la matriz Q tiene $k = 3$ filas y $n+1$ columnas ($\lambda(n-2+2u)+\mu$, donde $\lambda = 1$, $u = 1$ y $\mu = 1$). Cada fila tiene exactamente $u = 1$ entrada vacía $-$. Vemos que las columnas $n-1$, n y $n+1$ contienen un único elemento vacío y las demás columnas no contienen elementos vacíos. Esto es, cada columna contiene como mucho un elemento vacío.

Finalmente, para todos $1 \leq i < j \leq 3$, el multiconjunto

$$\{q_{il} - q_{jl} \ : \ 1 \leq l \leq n+1 \text{ con } q_{il} \text{ y } q_{jl} \text{ no vacíos}\}$$

es, denotado por extensión:

- $i = 1, j = 2 : \{0, n-2, \dots, 3, 2, 1\}$.
- $i = 1, j = 3 : \{0, n-3, n-1 \dots, 2, n-2, n-4, \dots, 5, 3, 1\}$.
- $i = 2, j = 3 : \{0, n-2, n-3, \dots, \frac{n+1}{2}, \frac{n-3}{2}, \frac{n-5}{2}, \dots, 2, 1, \frac{n-1}{2}\}$.

Podemos ver claramente que en cualquiera de los tres multiconjuntos, cada elemento de $\mathbb{Z}/(n-1)\mathbb{Z}$ está exactamente una vez ($\lambda = \mu = 1$). ■

A continuación mostraremos ejemplos de construcciones obtenidas con las dos proposiciones anteriores:

EJEMPLO 5.11. *Para $n = 10$ y $n = 12$, obtenemos de la Proposición 5.9 las $CMCDs$*

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & - \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & - & 0 \\ 7 & 6 & 5 & 4 & 3 & 2 & 1 & 0 & - & 8 & 0 \end{pmatrix}$$

y

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & - \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & - & 0 \\ 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 & 0 & - & 8 & 0 \end{pmatrix},$$

respectivamente.

Por otro lado, para $n = 11$ y $n = 13$ obtenemos de la Proposición 5.10 las $CMCDs$

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & - \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & - & 0 \\ 0 & 2 & 4 & 6 & 8 & 1 & 3 & 5 & 7 & - & 9 & 5 \end{pmatrix}$$

y

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & - \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & - & 0 \\ 0 & 2 & 4 & 6 & 8 & 10 & 1 & 3 & 5 & 7 & - & 11 & 9 & 5 \end{pmatrix},$$

respectivamente.

Ahora mostraremos que, si n es una potencia de un primo, siempre podemos encontrar una $CMCD$.

TEOREMA 5.12. *Si $n = p^r$ con p un número primo y $r \in \mathbb{N}$ entonces existe una $CMCD(n+1, n)$.*

DEMOSTRACIÓN. Sea $\mathbb{F}_n$ el cuerpo de Galois de orden n, y sea $\mathbb{F}_n^*$ el conjunto de elementos no nulos de $\mathbb{F}_n$. Consideramos el plano proyectivo $PG(n, 2)$ cuyo conjunto de puntos es el conjunto X de subespacios unidimensionales de $\mathbb{F}_n^3$ y cuyas rectas son los subespacios bidimensionales. Para cualquier $s \in \mathbb{F}_n^*$, la función $f_s : X \longrightarrow X$ con $f_s(< v >) =< sv >$ es un automorfismo del plano, y el grupo de automorfismos $G = \{f_s \ : \ s \in \mathbb{F}_n^*\}$ es isomorfo al grupo multiplicativo de los elementos no nulos de $\mathbb{F}_n$ y, por lo tanto, es cíclico. Ahora tenemos que, bajo la bien conocida biyección entre planos proyectivos de orden n y arreglos ortogonales de $OA(n+1, n)$ mencionada en

la introducción de esta tesis, el $OA(n+1,n)$ asociado al $PG(n,2)$ admite un grupo de automorfismos isomorfo a G que fija el 0 y actúa regularmente sobre los elementos no nulos de $\mathbb{F}_n$. ■

Se debe tener en cuenta que la cota de Rao se alcanza en los arreglos ortogonales asociados a las $CMCD$s del teorema anterior, y este es el único caso en que esto podría suceder si la Conjetura de la Potencia de Primo para planos proyectivos resulta cierta.

A continuación presentamos un modelo de Programación Entera que nos permite obtener $CMCD$s arbitrarios, y en particular, podemos considerar valores de n que no son potencias de primos.

Vamos a introducir el modelo matemático cuya solución óptima es un $OA(m,n)$ con $N = n^2$ ejecuciones, m factores, n niveles, fuerza $t = 2$ e índice $\lambda = 1$, que se puede reformular como una $CMCD(m,n)$. Sin pérdida de generalidad, supongamos que el arreglo contiene las n^2 combinaciones en las primeras dos columnas de forma ordenada. Ahora, si denotamos por $[n]$ al conjunto $\{0,1,\ldots,n-1\}$, definamos las siguientes variables, donde i denota la ejecución (o fila), $i \in [N]$; $\sigma(i)$, la siguiente fila a la i-ésima fila, relacionada con el automorfismo que fija el símbolo 1 y permuta cíclicamente (alfabéticamente) los símbolos en $[n] \setminus \{1\}$; s, el nivel (o símbolo), $s \in [n]$; l, la posición de la combinación (x_1, x_2), $l \in [|S^2|]$; j, el factor (o columna) y (j_1, j_2) un par de columnas, $j, j_1, j_2 \in \{3,\ldots,m\}$ tales que $3 \leq j_1 < j_2 \leq m$:

$$x_{i,j}^{s} = \begin{cases} 1 & \text{si el elemento de la fila } i \text{ y la columna } j \text{ vale } s \\ 0 & \text{en otro caso} \end{cases}$$

$$z_{i,j_1,j_2}^{l} = \begin{cases} 1 & \text{si el par de la fila } i \text{ y el par de columnas } (j_1,j_2) \text{ contiene la } l\text{-ésima combinación} \\ 0 & \text{en otro caso} \end{cases}$$

Entonces, el modelo matemático para $CMCD$, con $\mathcal{O}(m^2n^4)$ variables, es como sigue:

$$\sum_{i} x^s_{i,j} = n, \qquad \forall j, s \qquad (1a)$$

$$\sum_{s} x^s_{i,j} = 1, \qquad \forall i, j \qquad (1b)$$

$$\sum_{i=(q-1)n+1}^{qn} x^s_{i,j} = 1, \qquad \forall q \in [n], j, s \qquad (1c)$$

$$\sum_{i : i \equiv q \mod n} x^s_{i,j} = 1, \qquad \forall q \in [n], j, s \qquad (1d)$$

$$x^1_{i,j} = x^1_{\sigma(i),j}, \qquad \forall i, j \qquad (1e)$$

$$x^s_{i,j} = x^{s+1}_{\sigma(i),j}, \qquad \forall i, j, \forall s \in [n] \setminus \{1, n\} \qquad (1f)$$

$$x^n_{i,j} = x^2_{\sigma(i),j}, \qquad \forall i, j \qquad (1g)$$

$$\sum_{l} l \; z^l_{i,j_1,j_2} = n \sum_{s} s \; x^s_{i,j_1} + \sum_{s} s \; x^s_{i,j_2} - n, \qquad \forall i, j_1, j_2 \qquad (1h)$$

$$\sum_{l} z^l_{i,j_1,j_2} = 1, \qquad \forall i, j_1, j_2 \qquad (1i)$$

$$\sum_{i} z^l_{i,j_1,j_2} = 1, \qquad \forall l, j_1, j_2 \qquad (1j)$$

$$x^s_{i,j},\ z^l_{i,j_2,j_2} \in \{0, 1\}, \qquad \forall i, j, j_1, j_2, l, s. \qquad (1k)$$

Las restricciones (1a) garantizan que cada nivel aparece una vez a lo largo de todas las ejecuciones para cada columna. Las restricciones (1b) aseguran que cada celda tenga exactamente un nivel asociado. Las restricciones (1c) y (1d) imponen que el par de columnas $(1, j)$ y $(2, j)$, respectivamente, contienen todas las n^t combinaciones. Las restricciones (1e)–(1g) garantizan que la aplicación que fija el símbolo 1 y permuta cíclicamente (alfabéticamente) los símbolos $[n] \setminus \{1\}$, donde los símbolos $\{1, 2, \ldots, n\}$ se pueden volver a etiquetar como $\{-, 0, \ldots, n-2\}$, es un automorfismo. Las restricciones (1h) determinan que, para cada fila, cualquier par de columnas (j_1, j_2) se corresponde con una combinación de elementos de S^t. Las restricciones (1i) establecen que para cada ejecución, hay exactamente una combinación asociada a cada par de columnas (j_1, j_2). Las restricciones (1j) aseguran que para cada par de columnas (j_1, j_2), cada posible combinación aparece exactamente una vez. Y (1k) son las restricciones de integralidad.

Nótese que una vez resuelto el modelo de Programación Entera, la celda (i, j) de la $CMCD$ contiene el símbolo determinado por la variable no nula del vector $(x^1_{i,j}, \ldots, x^m_{i,j})$, es decir, $a_{i,j} = \sum_s s x^s_{i,j}$. Además, si la función objetivo es nula, el resultado es una $CMCD(m, n)$; de lo contrario, no existe una $CMCD$ con esos parámetros.

También implementamos un algoritmo de búsqueda local bimodal para encontrar una $CMCD(m,n)$ para valores dados de m y n. Tomamos como espacio de búsqueda el conjunto X de matrices $A=(a_{i,j})$ de tamaño $m\times(n+1)$ con entradas en $C_{n-1}\cup\{-\}$ donde C_{n-1} es el grupo cíclico de orden $n-1$, que satisface las siguientes condiciones:

(i) $a_{i,i}=-$, para todo $i\in\{1,\ldots,m\}$

(ii) $a_{i,j}\in C_{n-1}$, para todo $i\in\{1,\ldots,m\}$, $j\in\{1,\ldots,n+1\}$ con $i\neq j$

(iii) $a_{2,1}=0$

(iv) $a_{1,j}=0$, para todo $j\in\{2,\ldots,n+1\}$.

Consideramos la siguiente función de desadecuación U a minimizar: Si $A\in X$, entonces

$$U(A)=\sum_{i=1}^{m}\sum_{j=i+1}^{m}\sum_{a\in C_{n-1}}(|\{k\in\{1,\ldots,n+1\}\setminus\{i,j\}\ :\ a_{j,k}-a_{i,k}=a\}|-1)^2.$$

Primero consideramos una matriz aleatoria en X y realizamos el primer modo de búsqueda local, probando todas las modificaciones en uno de sus elementos. Cuando el valor de U se reduce estrictamente, el candidato se reemplaza por el modificado. Una vez realizadas todas las modificaciones probadas sin que se haya conseguido una reducción, se realiza una búsqueda local del segundo modo, probando todas las modificaciones en dos elementos arbitrarios. Cuando se obtiene una reducción en U, el algoritmo vuelve a entrar en una búsqueda local de primer modo. Si no ocurre ninguna reducción, entonces se genera un nuevo candidato inicial y se repite todo el proceso, hasta que se alcance un tiempo de umbral prefijado. Cuando obtenemos un valor de U igual a 0, entonces el candidato es una verdadera $CMCD(m,n)$ y si esto sucede el algoritmo termina.

Después de encontrar una solución, la convertimos a forma canónica.

Por supuesto, una versión alternativa del algoritmo podría ser tomar matrices en las que las dos primeras filas estén en la forma canónica como matrices candidatas en el espacio de búsqueda, y donde las posibles posiciones para el símbolo $-$ y los símbolos en C_{n-1} se modifican durante el proceso. Probamos también esta variación, pero la eficiencia del algoritmo fue similar, y no obtuvimos solución para los parámetros no encontrados con el algoritmo de la forma anterior. Además, la forma anteriormente descrita de las matrices encaja mejor con el enunciado de la conjetura que trataremos posteriormente.

Hemos obtenido ciertas $CMCD$s con n que no es una potencia de un primo usando los dos métodos computacionales descritos anteriormente. El algoritmo de búsqueda local bimodal no pudo encontrar soluciones para $n>15$ en menos de 48 horas, pero

el algoritmo de programación entera tuvo éxito en esta tarea. No obstante, mantenemos la exposición de lo anterior para ofrecer una comparación entre los dos algoritmos y también porque establece la base en el enunciado de la conjetura que trataremos más adelante. A continuación mostramos las $CMCD$s obtenidos con el algoritmo de búsqueda local bimodal para $n \leq 15$ y usando el modelo de programación entera para $n \geq 18$. Los resultados se han obtenido implementando el modelo de programación entera con el software de optimización IBM ILOG CPLEX v20.1 usando hasta 8 hilos [**63**]. Los experimentos computacionales se llevaron a cabo en el clúster computacional ARINA de SGI/IZO-SGIker en la UPV/EHU [**4**]:

Para $n = 10$, $m = 4$:

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & - \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & - & 0 \\ 6 & 2 & 0 & 7 & 4 & 8 & 5 & - & 1 & 3 & 5 \\ 4 & 7 & 2 & 8 & - & 3 & 5 & 1 & 0 & 6 & 2 \end{pmatrix}$$

Para $n = 12$, $m = 4$:

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & - \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & - & 0 \\ 3 & 10 & 6 & 9 & 1 & 4 & 8 & 7 & 2 & 5 & - & 0 & 1 \\ 9 & 6 & 5 & - & 4 & 1 & 8 & 0 & 3 & 10 & 7 & 2 & 10 \end{pmatrix}$$

Para $n = 14$, $m = 4$:

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & - \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & - & 0 \\ 8 & 11 & 5 & 7 & 0 & 3 & 6 & - & 10 & 2 & 9 & 12 & 14 & 1 & 7 \\ 11 & 8 & - & 9 & 6 & 2 & 7 & 10 & 4 & 0 & 5 & 3 & 12 & 1 & 12 \end{pmatrix}$$

Para $n = 15$, $m = 4$:

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & - \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & - & 0 \\ 11 & 13 & 0 & 8 & 12 & 5 & 10 & 6 & 1 & 4 & 2 & - & 13 & 9 & 7 & 3 \\ 2 & 1 & 13 & 11 & 7 & 6 & - & 0 & 12 & 4 & 8 & 10 & 3 & 5 & 9 & 10 \end{pmatrix}$$

Para $n = 18$, $m = 4$:

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & - \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & - & 0 \\ 10 & - & 8 & 0 & 7 & 13 & 1 & 16 & 2 & 5 & 11 & 9 & 12 & 15 & 4 & 14 & 3 & 6 & 5 \\ 10 & 4 & 16 & 7 & 2 & 0 & 15 & 1 & 13 & 11 & 9 & 12 & 8 & 3 & 14 & 6 & - & 5 & 6 \end{pmatrix}$$

Para $n = 20$, $m = 4$:

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & - \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & - & 0 \\ 16 & 15 & 4 & 7 & 5 & 13 & 12 & 17 & 6 & - & 2 & 10 & 8 & 1 & 14 & 9 & 0 & 3 & 11 & 18 & 9 \\ 16 & 12 & 5 & 3 & 13 & 0 & 7 & 15 & 18 & 11 & - & 17 & 10 & 6 & 8 & 1 & 4 & 2 & 14 & 9 & 18 \end{pmatrix}$$

Comparamos la estructura de los grafos fuertemente regulares correspondientes a los arreglos ortogonales asociados a las $CMCD$s obtenidos con el algoritmo de búsqueda local bimodal y el modelo de programación entera con los correspondientes a los arreglos ortogonales con los mismos parámetros obtenidos con el paquete 'Orthogonal Arrays' en el software matemático SageMath ([**108**]), y encontramos que no son isomorfos. De hecho, en todos los casos, incluso los grupos de automorfismos de los grafos no eran isomorfos.

Sea $n \geq 3$. Si definimos

$$\alpha(n) := \text{máx}\{m \in \mathbb{N} \ : \ \textbf{existe un } OA(m, n)\}$$

y

$$\beta(n) := \text{máx}\{m \in \mathbb{N} \ : \ \textbf{existe una } CMCD(m, n)\},$$

entonces podemos preguntarnos cuándo $\alpha(n)$ y $\beta(n)$ son iguales. Deducimos de la Proposición 5.9, el Teorema 5.12 y las $CMCD$s obtenidas con el algoritmo de búsqueda local bimodal que $\alpha(n) = \beta(n)$ para n hasta 9. Aunque el valor $\alpha(10)$ no se conoce, se sabe que $\alpha(10) \geq 4$. La $CMCD(10, 4)$ obtenida anteriormente abre la posibilidad, hasta el estado actual de conocimiento sobre las cotas de $\alpha(10)$, de que $\alpha(10) = \beta(10)$. Además, el Teorema 5.12 muestra que $\alpha(n) = \beta(n)$ cuando n es una potencia de un primo.

En lo que sigue, dada una matriz cuadrada de orden n con entradas en el grupo cíclico C_n y definida excepto en la diagonal principal, $U(A)$ denotará la función de desadecuación definida previamente.

TEOREMA 5.13. *Si A es una cuasi matriz cíclica de diferencias y A^t es su transpuesta, entonces se tiene que $U(A) = U(A^t) = 0$.*

DEMOSTRACIÓN. Bajo la biyección ya mencionada entre el conjunto de arreglos $OA(n+1, n)$ y los planos proyectivos de orden n, la forma de construir el plano afín del correspondiente conjunto de cuadrados latinos mutuamente ortogonales es simétrica con respecto a la operación de transponer los cuadrados latinos asociados. Por lo tanto, si A es una cuasi matriz cíclica de diferencias, obtenemos el mismo plano proyectivo cuando repetimos formalmente la construcción con su transpuesta A^t. ■

A pesar de la sencillez del argumento anterior, llama la atención que la igualdad $U(A) = U(A^t)$ parece cumplirse para matrices arbitrarias en las que no tenemos estructura combinatoria o algebraica, aunque, por supuesto, este valor común no necesariamente es 0.

EJEMPLO 5.14. *Sea*

$$A = \begin{pmatrix} - & 2 & 1 & 1 \\ 1 & - & 0 & 2 \\ 2 & 1 & - & 1 \\ 2 & 2 & 0 & - \end{pmatrix}$$

Para calcular $U(A)$, debemos analizar las frecuencias de las diferencias a lo largo de las filas:

- ***Filas 1 y 2:*** $1 - 0 \equiv 1 \mod 3$, $1 - 2 \equiv 2 \mod 3$. ***El 0 aparece cero veces, el 1 aparece una vez y el 2 aparece una vez.***
- ***Filas 1 y 3:*** $2 - 1 \equiv 1 \mod 3$, $1 - 1 \equiv 0 \mod 3$. ***El 0 aparece una vez, el 1 aparece una vez y el 2 aparece cero veces.***
- ***Filas 1 y 4:*** $2 - 2 \equiv 0 \mod 3$, $1 - 0 \equiv 1 \mod 3$. ***El 0 aparece una vez, el 1 aparece una vez y el 2 aparece cero veces.***
- ***Filas 2 y 3:*** $1 - 2 \equiv 2 \mod 3$, $2 - 1 \equiv 1 \mod 3$. ***El 0 aparece cero veces, el 1 aparece una vez y el 2 aparece una vez.***
- ***Filas 2 y 4:*** $1 - 2 \equiv 2 \mod 3$, $0 - 0 \equiv 0 \mod 3$. ***El 0 aparece una vez, el 1 aparece cero veces y el 2 aparece una vez.***
- ***Filas 3 y 4:*** $2 - 2 \equiv 0 \mod 3$, $1 - 2 \equiv 2 \mod 3$. ***El 0 aparece una vez, el 1 aparece cero veces y el 2 aparece una vez.***

Por tanto, la cantidad de veces que hay un elemento que aparece cero veces es 6, la cantidad de veces que hay un elemento que aparece una vez es 12 y la cantidad de vecez que hay un elemento que aparece dos veces es 0. Por tanto

$$U(A) = 6 \cdot 1^2 + 12 \cdot 0^2 + 0 \cdot 1^2 = 6.$$

De manera similar, podemos calcular $U(A^t)$ *haciendo el mismo análisis pero por columnas:*

- ***Columnas 1 y 2:*** $2 - 1 \equiv 1 \mod 3$, $2 - 2 \equiv 2 \mod 3$. ***El 0 aparece una vez, el 1 aparece una vez y el 2 aparece cero veces.***
- ***Columnas 1 y 3:*** $1 - 0 \equiv 1 \mod 3$, $2 - 0 \equiv 2 \mod 3$. ***El 0 aparece cero veces, el 1 aparece una vez y el 2 aparece una vez.***
- ***Columnas 1 y 4:*** $1 - 2 \equiv 2 \mod 3$, $2 - 1 \equiv 1 \mod 3$. ***El 0 aparece cero veces, el 1 aparece una vez y el 2 aparece una vez.***
- ***Columnas 2 y 3:*** $2 - 1 \equiv 1 \mod 3$, $2 - 0 \equiv 2 \mod 3$. ***El 0 aparece cero veces, el 1 aparece una vez y el 2 aparece una vez.***
- ***Columnas 2 y 4:*** $2 - 1 \equiv 1 \mod 3$, $1 - 1 \equiv 0 \mod 3$. ***El 0 aparece una vez, el 1 aparece una vez y el 2 aparece cero veces.***
- ***Columnas 3 y 4:*** $1 - 1 \equiv 0 \mod 3$, $0 - 2 \equiv 1 \mod 3$. ***El 0 aparece una vez, el 1 aparece una vez y el 2 aparece cero veces.***

Por tanto, la cantidad de veces que hay un elemento que aparece cero veces es 6, la cantidad de veces que hay un elemento que aparece una vez es 12 y la cantidad de vecez que hay un elemento que aparece dos veces es 0. Por tanto

$$U(A^t) = 6 \cdot 1^2 + 12 \cdot 0^2 + 0 \cdot 1^2 = 6.$$

Conjeturamos que la igualdad $U(A) = U(A^t)$ siempre se cumple. Hay evidencias numéricas muy fuertes a favor de la conjetura. Tenemos demostrado mediante la realización de un análisis numérico exhaustivo que es cierta para todas las matrices de órdenes hasta 5, y hemos generado aleatoriamente 10^9 matrices para cada orden de 6 a 15, y la conjetura se cumple en todos estos casos.

Curiosamente, si cambiamos el exponente 2, el resultado no es cierto.

Por ejemplo, si

$$A = \begin{pmatrix} - & 4 & 2 & 4 & 3 & 1 & 2 \\ 0 & - & 0 & 1 & 1 & 1 & 0 \\ 4 & 1 & - & 2 & 3 & 0 & 3 \\ 3 & 1 & 4 & - & 2 & 1 & 4 \\ 2 & 3 & 2 & 1 & - & 0 & 3 \\ 3 & 3 & 4 & 3 & 0 & - & 3 \\ 4 & 4 & 1 & 2 & 3 & 2 & - \end{pmatrix},$$

entonces la distribución de frecuencias de las diferencias a lo largo de las filas para los valores 0, 1, 2, 3, 4 y 5 es: 31, 49, 19, 6, 0 y 0, respectivamente, y por lo tanto $U(A) = 31 \cdot 1^2 + 49 \cdot 0^2 + 19 \cdot 1^2 + 6 \cdot 2^2 + 0 \cdot 3^2 + 0 \cdot 4^2 = 74$.

De manera similar, la distribución de frecuencias de las diferencias a lo largo de las columnas para los valores 0, 1, 2, 3, 4 y 5 es: 32, 46, 22, 5, 0 y 0, respectivamente, y $U(A^t) = 32 \cdot 1^2 + 46 \cdot 0^2 + 22 \cdot 1^2 + 5 \cdot 2^2 + 0 \cdot 3^2 + 0 \cdot 4^2 = 74$.

Pero ahora, si por ejemplo tomamos el exponente 4 en este ejemplo dado el valor para la matriz A es $31 \cdot 1^4 + 49 \cdot 0^4 + 19 \cdot 1^4 + 6 \cdot 2^4 + 0 \cdot 3^4 + 0 \cdot 4^4 = 146$, y para A^t es $32 \cdot 1^4 + 46 \cdot 0^4 + 22 \cdot 1^4 + 5 \cdot 2^4 + 0 \cdot 3^4 + 0 \cdot 4^4 = 134$.

Capítulo 6

CUASI ARREGLOS ORTOGONALES CON UNA TOLERANCIA DADA Y UN GRUPO DE AUTOMORFISMOS

En este capítulo mencionamos lo difícil que es obtener arreglos ortogonales y la necesidad de relajar la definición. Algunos ejemplos de esto los vemos en [**80**] para fMRI (imagen por resonancia magnética funcional).

En las referencias [**84**] - [**87**] se demostró que todas las clases de isomorfía de arreglos ortogonales son equivalentes a encontrar todas las clases de isomorfía de soluciones enteras no negativas de un sistema de ecuaciones lineales bajo el grupo de simetría del sistema de ecuaciones. En [**16**] se utiliza un problema de programación entera que involucra conos convexos racionales para generar todos los arreglos ortogonales de 2 niveles de dimensión y fuerza dadas. En [**13**], se muestra una clasificación de arreglos ortogonales mediante programación entera. En [**113**], se describe un método de programación entera mixta, que es útil para construir diseños ortogonales, o mejorar los existentes.

Los principales conceptos que estaremos tratando en el capítulo son los siguientes: Primero, presentamos las simetrías y automorfismos de un arreglo; segundo, tratamos arreglos ortogonales y consideramos algunos ejemplos donde hay simetrías; tercero, introducimos la noción de cuasi arreglos ortogonales con simetrías y consideramos sus simetrías como en el caso de arreglos ortogonales; y cuarto y último, introducimos el problema de minimización que vamos a considerar.

Se puede observar que en el estudio de arreglos ortogonales, no estamos interesados en el orden de las filas de la matriz. En nuestro caso, se trata del mismo arreglo si se hace permutaciones de sus filas. Esto sugiere la siguiente definición.

DEFINICIÓN 6.1. *Dados dos arreglos $A, \tilde{A} \in S^{N\times k}$ con entradas en S, decimos que A* y *$\tilde{A}$* son equivalentes*, $A \cong \tilde{A}$, si hay una permutación de filas P tal que*

$$\tilde{A} = PA.$$

En otras palabras, $A \cong \tilde{A}$ si y solo si los multiconjuntos de sus filas son iguales.

El siguiente ejemplo muestro dos arreglos equivalentes.

EJEMPLO 6.2. *Los arreglos*

$$A = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 2 & 2 & 2 \\ 1 & 0 & 1 & 2 \\ 1 & 1 & 2 & 0 \\ 1 & 2 & 0 & 1 \\ 2 & 0 & 2 & 1 \\ 2 & 1 & 0 & 2 \\ 2 & 2 & 1 & 0 \end{pmatrix} \quad \textbf{y} \quad \tilde{A} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 2 & 0 & 2 & 1 \\ 1 & 0 & 1 & 2 \\ 1 & 1 & 2 & 0 \\ 1 & 2 & 0 & 1 \\ 0 & 2 & 2 & 2 \\ 2 & 1 & 0 & 2 \\ 2 & 2 & 1 & 0 \end{pmatrix}$$

son equivalentes, pues al permutar la tercera fila de A con la séptima fila se obtiene el arreglo $\tilde{A}$.

Sea

$$\Sigma(S, k) := \Sigma(S) \times \Sigma_k$$

el producto del grupo de permutaciones de S, $\Sigma(S)$, y el grupo de permutaciones de $[k] := \{1, \ldots, k\}$, Σ_k. Denotaremos sus elementos por

$$[g|\sigma] \tag{6.1}$$

donde $g \in \Sigma(S)$ y $\sigma \in \Sigma_k$. De esta forma, escribiremos una expresión como $[(1,2,3)|(1,2)(3,4)]$ en lugar de $((1,2,3),(1,2)(3,4))$ para un elemento de $\Sigma(\{1,2,3\},4)$. Ahora, $\Sigma(S,k)$ actúa naturalmente sobre $S^{N\times k}$ de la siguiente manera: dado $[g|\sigma] \in$

$\Sigma(S,k)$ y $A \in S^{N\times k}$,

$$[g|\sigma]A := \left(gA_{i,\sigma(j)}\right)_{\substack{i\in[N]\\ j\in[k]}}, \tag{6.2}$$

esto es, g permuta los símbolos del arreglo y σ permuta las columnas.

Una vez introducida la equivalencia de arreglos y la acción de grupo sobre arreglos, estamos listos para definir lo que es un automorfismo (o simetría) de un arreglo.

DEFINICIÓN 6.3. *Dado un arreglo $A \in S^{N\times k}$ con entradas en S, un automorfismo (o simetría) de A es un elemento $[g|\sigma] \in \Sigma(S,k)$ tal que*

$$[g|\sigma]A \cong A.$$

*El grupo de automorfismos de A, **Aut**(A), es el conjunto*

$$\textbf{\textit{Aut}}(A) := \{[g|\sigma] \in \Sigma(S,k) \ : \ [g|\sigma]A \cong A\}. \tag{6.3}$$

Nótese que *un grupo de automorfismos* de A significa un subgrupo de Aut(A). Por lo tanto, debe quedar claro que cuando decimos que A tiene a $G \leq \Sigma(S,k)$ como un grupo de automorfismos, queremos decir que $G \leq$ Aut(A) permite que la inclusión sea estricta.

EJEMPLO 6.4. *Consideremos los arreglos*

$$A = \begin{pmatrix} a & b & c \\ b & c & a \\ c & a & b \end{pmatrix} \text{ y } B = \begin{pmatrix} a & b & c & a \\ b & a & b & a \end{pmatrix}.$$

Con respecto a A, podemos ver que tanto $[(a,b,c)|id]$ como $[id|(1,2,3)]$ son automorfismos de A. En efecto,

$$[(a,b,c)|id]A = \begin{pmatrix} b & c & a \\ c & a & b \\ a & b & c \end{pmatrix} \cong A$$

y

$$[id|(1,2,3)]A = \begin{pmatrix} c & a & b \\ a & b & c \\ b & c & a \end{pmatrix} \cong A$$

Sin embargo, nótese que hay más automorfismos, como $[(a,b)|(1,2)]$, aunque ni $[(a,b)|id]$ ni $[id|(1,2)]$ son así.

Con respecto a B*, podemos demostrar que* $Aut(B) = [id|id]$*, por lo que* B *no tiene simetrías no triviales. Esto es claro, ya que en caso de haber alguna permutación no trivial de símbolos, tendría que haber al menos dos símbolos que estuvieran la misma cantidad de veces en el arreglo y vemos claramente que el símbolo* a *aparece cuatro veces, el símbolo* b *aparece tres veces y el símbolo* c *aparece una vez. Si hubiese alguna permutación de símbolos, esta frecuencia se vería alterada. Por otro lado, en caso de haber una permutación de columnas, no podría involucrar la tercera columna, ya que no habría ninguna fila cuya tercera componente fuese* c*. Por lo que la permutación es un ciclo de tamaño dos, tres o un producto de dos ciclos de longitud 2. Si fuese un ciclo de tamaño tres, sería* $(1,2,4)$ *o* $(1,4,2)$*. Al aplicarle el ciclo* $(1,2,4)$*, obtenemos el arreglo*

$$\begin{pmatrix} a & a & c & b \\ a & b & b & a \end{pmatrix}$$

y al aplicarle el ciclo $(1,4,2)$ *obtenemos el arreglo*

$$\begin{pmatrix} b & a & c & a \\ a & a & b & b \end{pmatrix},$$

los cuales vemos claramente que no son equivalentes a B*. Los posibles ciclos de tamaño dos serían* $(1,2)$*,* $(1,4)$ *y* $(2,4)$*, las cuales darían los arreglos*

$$\begin{pmatrix} b & a & c & a \\ a & b & b & a \end{pmatrix}, \quad \begin{pmatrix} a & b & c & a \\ a & a & b & b \end{pmatrix} \quad y \quad \begin{pmatrix} a & a & c & b \\ b & a & b & a \end{pmatrix}$$

respectivamente. Vemos también que ninguno es equivalente a B*.*

Finalmente, los productos de ciclos posibles son $(1,2)(3,4)$*,* $(1,3)(2,4)$ *y* $(1,4)(2,3)$*, los cuales darían los arreglos*

$$\begin{pmatrix} b & a & a & c \\ a & b & a & b \end{pmatrix}, \quad \begin{pmatrix} c & a & a & b \\ b & a & b & a \end{pmatrix} \quad y \quad \begin{pmatrix} a & c & b & a \\ a & b & b & a \end{pmatrix},$$

respectivamente. Vemos que, en este caso, también se tiene que ninguno es equivalente a B*.*

Antes de pasar a los arreglos ortogonales, podemos definir de una manera más sencilla el concepto de arreglo ortogonal utilizando una notación más simple.

DEFINICIÓN 6.5. *Un arreglo ortogonal de fuerza t sobre S es un arreglo $A \in S^{N\times k}$ con entradas en S tal que siempre que eliminemos $k-t$ columnas de A, cada t-tupla con entradas en S aparece el mismo número de veces, N/s^t. El índice de dicho arreglo ortogonal, denotado por $\lambda(A)$ o simplemente λ, es este último número.*

Diremos que A es un $OA(N,k,s,t)$ si para algún conjunto S de tamaño s, $A \in S^{N\times k}$ es un arreglo ortogonal de fuerza t sobre S.

Ahora, presentaremos un enfoque más formal que será útil para nuestra generalización a cuasi arreglos ortogonales.

Primero, indicamos una forma de seleccionar t columnas de un arreglo de tamaño $N \times k$, que es lo mismo que eliminar $k-t$ columnas. Para ello, sean $t, k \in \mathbb{N}$, con $t \leq k$, y consideramos el conjunto

$$T_{t,k} := \{(j_1, \ldots, j_t) \in [k]^t \,:\, 1 \leq j_1 < \ldots < j_t \leq k\}. \tag{6.4}$$

Nótese que $T_{t,k}$ está en biyección con $\binom{[k]}{t}$, el conjunto de subconjuntos de tamaño t de $[k]$. Por tanto, se tiene que $\#T_{t,k} = \binom{k}{t}$.

En segundo lugar, presentamos las funciones de conteo, que cuentan cuántas veces aparece una fila en el subarreglo de tamaño $N \times t$ seleccionado. Para un arreglo A de tamaño $N \times k$ con entradas en S, $j \in T_{t,k}$ y $x \in S^t$, definimos

$$n(A, x, j) := \left|\{i \in [N] \,:\, \forall r \in [t],\, a_{i,j_r} = x_r\}\right|. \tag{6.5}$$

En otras palabras, $n(A,x,j)$ cuenta el número de veces que aparece cada t-tupla x como una fila en el subarreglo

$$A[j_1, \ldots, j_t] := \begin{pmatrix} A_{1,j_1} & \cdots & A_{1,j_t} \\ \vdots & \ddots & \vdots \\ A_{N,j_1} & \cdots & A_{N,j_t} \end{pmatrix}$$

de A, obtenido tras seleccionar las columnas $j_1, \ldots, j_t$ de A.

Se tiene la siguiente proposición.

PROPOSICIÓN 6.6. *Para un arreglo $A \in S^{N\times k}$ con entradas en un conjunto S de cardinal s, A es un arreglo ortogonal con fuerza t si y solo si para todo $x \in S^t$ y todo $j \in T_{t,k}$,*

$$n(A, x, j) = N/s^t.$$

DEMOSTRACIÓN. Sean $A \in S^{N\times k}$ un arreglo ortogonal con fuerza t, $x = (x_1, \ldots, x_t) \in S^t$ y $j = (j_1, \ldots, j_t) \in T_{t,k}$. Tenemos que ver cuántas veces aparece x como una fila en

$$A[j_1, \ldots, j_t] = \begin{pmatrix} A_{1,j_1} & \cdots & A_{1,j_t} \\ \vdots & \ddots & \vdots \\ A_{N,j_1} & \cdots & A_{N,j_t} \end{pmatrix}$$

Nótese que $A[j_1, \ldots, j_t]$ es una submatriz de A que se obtiene eliminando $k - t$ columnas de A. Como A es un arreglo ortogonal con fuerza t, por definición se tiene que cada t-túpla con entradas en S (en particular x es una de ellas) aparece exactamente N/s^t veces en dicha submatriz, lo que demuestra que $n(A, x, j) = N/s^t$.

Recíprocamente, supongamos que $n(A, x, j) = N/s^t$. Esto implica que la t-túpla x aparece N/s^t veces en un subarreglo de A obtenido al eliminar $k - t$ columnas. Por tanto, A es un arreglo ortogonal con fuerza t. ■

Con respecto a las simetrías, podemos ver que para $A \in S^{N\times k}$, $x \in S^t$, $j \in T_{t,k}$ y $[g|\sigma] \in \Sigma(S, k)$,

$$n([g|\sigma]A, x, j) = n(A, g^{-1}x, \sigma^{-1}j) \tag{6.6}$$

donde $g^{-1}x := (g^{-1}x_1, \ldots, g^{-1}x_t)$ y $\sigma^{-1}j$ es igual a $(\sigma^{-1}j_1, \ldots, \sigma^{-1}j_t)$ salvo un reordenamiento de las entradas (la permutación podría no dar una tupla en $T_{t,k}$). En efecto, $n([g|\sigma]A, x, j)$ cuenta el número de veces que aparece cada t-túpla x como una fila en el subarreglo

$$\begin{pmatrix} [g|\sigma]A_{1,j_1} & \cdots & [g|\sigma]A_{1,j_t} \\ \vdots & \ddots & \vdots \\ [g|\sigma]A_{N,j_1} & \cdots & [g|\sigma]A_{N,j_t} \end{pmatrix},$$

donde $[g|\sigma]A_{i,j_k}$ indica el elemento A_{i,j_k} después de haber aplicado la permutación $[g|\sigma]$. Es claro que este subarreglo tiene N filas, cada entrada es un elemento de S y además $[g|\sigma]A \cong A$, luego $[g|\sigma]A$ es un arreglo ortogonal con fuerza t. Así, por la Proposición 6.6, $n([g|\sigma]A, x, j) = N/s^t$.

Por otro lado, está claro que $g^{-1}x \in S^t$ y $\sigma^{-1}j \in T_{t,k}$. Por tanto, por la Proposición 6.6, $n(A, g^{-1}x, \sigma^{-1}j) = N/s^t$.

Concluimos entonces que $n([g|\sigma]A, x, j) = n(A, g^{-1}x, \sigma^{-1}j)$.

Por lo anterior, tenemos que la acción de $\Sigma(S,k)$ sobre $S^{N\times k}$ conserva los arreglos ortogonales, por lo que tiene sentido hablar de los automorfismos de un arreglo ortogonal.

EJEMPLO 6.7. *Considérese el siguiente arreglo ortogonal de fuerza* 2 *sobre* $\{0,1\}$

$$A = \begin{pmatrix} 0 & 0 \\ 0 & 1 \\ 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Nótese que el automorfismo $[(0,1)|(1,4)(2,3)]$ es una simetría no trivial de A. Además, es el generador del grupo de automorfismos de A.

No siempre podemos obtener un $OA(N,k,s,t)$. Por lo tanto, podríamos contentarnos con un arreglo en la que cada t-tupla con entradas en S aparezca "más o menos" el mismo número de veces. ¿A qué nos referimos con "más o menos" ? Definimos el "desequilibrio" para medir esto.

DEFINICIÓN 6.8. *Sea* $A \in S^{N\times k}$ *un arreglo. Dado* $p \in [1,\infty)$*, el* p*-desequilibrio de fuerza* t *de* A *es*

$$\mathrm{U}_{p,t}(A) := \sum_{x\in S^t} \sum_{j\in T_{t,k}} |n(A,x,j) - N/s^t|^p, \tag{6.7}$$

y la tolerancia de fuerza t *de* A *es*

$$\mathrm{Tol}_t(A) := \max\left\{|n(A,x,j) - N/s^t| \,:\, x\in S^t,\, j\in T_{t,k}\right\}. \tag{6.8}$$

Cuando p *y/o* t *se sobreentiendan por el contexto, los omitiremos de la notación.*

En el caso especial en el que A es un $OA(N,k,s,t)$, podemos ver que $\mathrm{U}_{p,t}(A) = \mathrm{Tol}(A) = 0$, ya que para todos $x\in S^t$ y $j\in T_{t,k}$ se tiene $n(A,x,j) = N/s^t$. Ahora, para un arreglo arbitrario $A\in S^{N\times k}$, este no es el caso, ya que no todos los $n(A,x,j)$ son iguales. Por lo tanto, considerar diferentes desequilibrios significa considerar diferentes sentidos en los que un arreglo es casi ortogonal.

Ahora, una desventaja de la definición anterior de desequilibrio es que no permite comparaciones entre arreglos de diferentes tamaños y diferentes valores de p. Nótese que $\mathrm{U}_{1,t}$ es lineal y $\mathrm{U}_{2,t}$ es cuadrático. Para resolver este problema, presentamos versiones normalizadas.

DEFINICIÓN 6.9. *Sea $A \in S^{N\times k}$ un arreglo. Para $p \in [1,\infty]$, el p-desequilibrio normalizado de fuerza t de A es*

$$\widehat{\mathrm{U}}_{p,t}(A) := \begin{cases} \left(s^{-t}\binom{k}{t}^{-1} \sum\limits_{x\in S^t,\, j\in T_{t,k}} |n(A,x,j) - N/s^t|^p \right)^{\frac{1}{p}}, & \textit{si } p\in[1,\infty) \\ \max\limits_{x\in S^t,\, j\in T_{t,k}} \left\{ |n(A,x,j) - N/s^t| \right\}, & \textit{si } p=\infty. \end{cases} \tag{6.9}$$

Cuando p y/o t estén claros por el contexto, los omitiremos de la notación.

Sabemos de (6.7) que

$$\sum_{x\in S^t, j\in T_{t,k}} |n(A,x,j) - N/s^t|^p = \mathrm{U}_{p,t}$$

y por (6.8) se tiene que

$$\max_{x\in S^t, j\in T_{t,k}} \left\{ |n(A,x,j) - N/s^t| \right\} = \mathrm{Tol}_t(A),$$

por lo que podemos deducir que

$$\widehat{\mathrm{U}}_{p,t}(A) = \begin{cases} \left(s^{-t}\binom{k}{t}^{-1} \mathrm{U}_{p,t}(A) \right)^{\frac{1}{p}}, & \text{si } p\in[1,\infty) \\ \mathrm{Tol}_t(A), & \text{si } p=\infty. \end{cases}$$

Se tiene la siguiente proposición.

PROPOSICIÓN 6.10. *Sea $A\in S^{N\times k}$ un arreglo y $p,q\in[1,\infty]$ tales que $p\le q$. Entonces*

$$\frac{1}{\left(s^t\binom{k}{t}\right)^{\frac{q-p}{pq}}}\, \widehat{\mathrm{U}}_{q,t}(A) \le \widehat{\mathrm{U}}_{p,t}(A) \le \widehat{\mathrm{U}}_{q,t}(A).$$

En particular, si $p<q<\infty$,

$$\mathrm{U}_{q,t}(A) \le \mathrm{U}_{p,t}(A)^{\frac{q}{p}} \le \frac{1}{\left(s^t\binom{k}{t}\right)^{\frac{q}{p}-1}}\, \mathrm{U}_{q,t}(A),$$

y

$$\mathrm{Tol}_t(A)^p \le \mathrm{U}_{p,t}(A) \le s^t\binom{k}{t}\, \mathrm{Tol}_t(A)^p.$$

DEMOSTRACIÓN. Supongamos que $p\le q<\infty$.

Analicemos la desigualdad de la izquierda. Se tiene que

$$\frac{1}{\left(s^t\binom{k}{t}\right)^{\frac{q-p}{pq}}}\,\widehat{\mathrm{U}}_{q,t}(A) = \frac{1}{\left(s^t\binom{k}{t}\right)^{\frac{1}{p}-\frac{1}{q}}}\,s^{-\frac{t}{q}}\binom{k}{t}^{-\frac{1}{q}}\,\mathrm{U}_{q,t}(A)^{\frac{1}{q}} = \frac{1}{\left(s^t\binom{k}{t}\right)^{\frac{1}{p}}}\,\mathrm{U}_{q,t}(A)^{\frac{1}{q}}$$

$$\leq \frac{1}{\left(s^t\binom{k}{t}\right)^{\frac{1}{p}}}\,\mathrm{U}_{p,t}(A)^{\frac{1}{p}} = \widehat{\mathrm{U}}_{p,t}(A)$$

.

Esta última desigualdad se sigue de que $\mathrm{U}_{p,t}$ es monótona decreciente respecto a p.

Utilizando el hecho conocido de que la p-norma cumple la desigualdad

$$||x||_p \leq n^{\frac{1}{p}-\frac{1}{q}}||x||_q$$

siempre que $p \leq q$, donde n es el número de sumandos de la definición de la p-norma, podemos ver que la desigualdad de la derecha satisface

$$\widehat{\mathrm{U}}_{p,t}(A) = \frac{1}{\left(s^t\binom{k}{t}\right)^{\frac{1}{p}}}\,\mathrm{U}_{p,t}(A)^{\frac{1}{p}} \leq \frac{1}{\left(s^t\binom{k}{t}\right)^{\frac{1}{p}}}\left(s^t\binom{k}{s}\right)^{\frac{1}{p}-\frac{1}{q}}\mathrm{U}_{q,t}(A)^{\frac{1}{q}}$$
$$= \frac{1}{\left(s^t\binom{k}{t}\right)^{\frac{1}{q}}}\,\mathrm{U}_{q,t}(A)^{\frac{1}{q}} = \widehat{\mathrm{U}}_{q,t}(A).$$

Supongamos ahora que $p < q = \infty$.

Se tiene que

$$\frac{1}{\left(s^t\binom{k}{t}\right)^{\frac{q-p}{pq}}}\,\widehat{\mathrm{U}}_{q,t}(A) = \frac{1}{\left(s^t\binom{k}{t}\right)^{\frac{1}{p}-\frac{1}{q}}}\,\mathrm{Tol}_t(A) = \frac{1}{\left(s^t\binom{k}{t}\right)^{\frac{1}{p}}}\,\mathrm{Tol}_t(A) \leq \frac{1}{\left(s^t\binom{k}{t}\right)^{\frac{1}{p}}}\,\mathrm{U}_{p,t}(A)^{\frac{1}{p}} = \widehat{\mathrm{U}}_{p,t}(A).$$

Dicha desigualdad se tiene debido a que la norma infinito es menor o igual que la p-norma.

Por otro lado,

$$\widehat{\mathrm{U}}_{p,t}(A) = \frac{1}{\left(s^t\binom{k}{t}\right)^{\frac{1}{p}}}\,\mathrm{U}_{p,t}(A)^{\frac{1}{p}} \leq \mathrm{Tol}_t(A) = \widehat{\mathrm{U}}_{q,t}(A)$$

.

Esta desigualdad se obtiene por la conocida relación entre la norma infinito y la p-norma:

$$||x||_p \leq n^{\frac{1}{p}}||x||_\infty,$$

donde n es el número de sumandos de la p-norma. ■

Usando la notación de tolerancia, definimos el concepto de *cuasi arreglo ortogonal.*

DEFINICIÓN 6.11. *Un* $AOA(N, k, s, t, \epsilon)$ *es un arreglo* $A \in M_{N\times k}(S)$ *que satisface que*

$$\mathrm{Tol}_t(A) \leq \epsilon.$$

$AOA(N, k, s, t, \epsilon)$ significa "almost-orthogonal array", el cual traduciremos como **"cuasi arreglo ortogonal"** con N ejecuciones, k factores, s niveles, fuerza t y tolerancia ϵ, donde, por abuso de lenguaje, decimos "con tolerancia ϵ" para indicar que la tolerancia, $\mathrm{Tol}_t(A)$, es como mucho ϵ. Como $\mathrm{Tol}_t(A)$ es una medida de cómo de lejos está A de ser un $OA(N, k, s, t)$, es razonable este abuso ya que estamos interesados en medir errores desde arriba.

EJEMPLO 6.12. *El arreglo*

$$\begin{pmatrix}
0 & 0 & 0 & 2 & 0\\
0 & 1 & 2 & 0 & 1\\
0 & 2 & 1 & 1 & 2\\
1 & 0 & 2 & 1 & 0\\
1 & 1 & 1 & 2 & 1\\
1 & 2 & 0 & 0 & 2\\
2 & 0 & 1 & 0 & 0\\
2 & 1 & 0 & 1 & 1\\
2 & 2 & 2 & 2 & 2
\end{pmatrix}$$

es un $AOA(9, 5, 3, 2, 2)$.

La definición anterior está muy relacionada con la de $OA(n, k, s, t, b)$ dada por Lin, Phao y Kao en [**80**], aunque ellos impusieron la condición adicional de que el arreglo sea circulante y no pidieron que el número de apariciones de las t-tuplas x estuvieran en un intervalo centrado en un valor dado λ, y en consecuencia no requirieron que el número de ejecuciones fuera λs^t. No obstante, mantenemos la terminología "cuasi arreglo ortogonal" utilizada en este capítulo.

Cada arreglo con λs^t filas y k columnas con entradas en S es un $AOA(N, k, s, t, \epsilon)$ siempre que la tolerancia sea lo suficientemente alta; por ejemplo, este es el caso cuando $\epsilon = \lambda(s^t - 1)$. Lo interesante y difícil es obtener cuasi arreglos ortogonales para los cuales ϵ sea lo más bajo posible. Esto nos lleva a la siguiente definición.

DEFINICIÓN 6.13. *Diremos que un* $AOA(N, k, s, t, \epsilon)$ *es ajustado si no existe un* $AOA(N, k, s, t, \epsilon')$ *con* $\epsilon' < \epsilon$.

EJEMPLO 6.14. *El arreglo*

$$\begin{pmatrix} 0 & 0 & 2 & 1 & 1 \\ 0 & 1 & 1 & 0 & 2 \\ 0 & 2 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 2 \\ 1 & 1 & 2 & 0 & 0 \\ 1 & 2 & 1 & 0 & 1 \\ 2 & 0 & 0 & 0 & 1 \\ 2 & 1 & 1 & 1 & 0 \\ 2 & 2 & 2 & 2 & 2 \end{pmatrix}$$

es un $AOA(9, 5, 3, 2, 1)$ *ajustado.*

Sin embargo, no estamos interesados en minimizar necesariamente la tolerancia. Queremos encontrar arreglos con un desequilibrio mínimo después de fijar un grupo de automorfismos (que no tiene que ser el grupo completo de automorfismos) y una tolerancia máxima.

Formulemos entonces el siguiente problema de optimización:

Problema del mínimo desequilibrio (PMD): Fijamos un conjunto S de cardinal s. Dado un grupo $G \subset \Sigma(S, k)$ y una tolerancia ϵ, encontrar el $AOA(N, k, s, t, \epsilon)$ con mínimo $\mathrm{U}_{p,t}$ tal que A está fijado por G. En otras palabras,

$$\text{mín}\{\mathrm{U}_{p,t}(A) \ : \ A \in \mathfrak{U}\}$$

donde

$$\mathfrak{U} = \{A \in S^{N \times k} \ : \ A \text{ es un } AOA(N, k, s, t, \epsilon) \text{ y } G \subset \mathbf{Aut}(A)\}.$$

Teniendo en cuenta este problema de optimización, tenemos la siguiente definición:

DEFINICIÓN 6.15. *Diremos que un* $AOA(N, k, s, t, \epsilon)$ *es* (G, ϵ)*-óptimo si satisface el PMD.*

Notación: El desequilibrio de un cuasi arreglo ortogonal (G, ϵ)-óptimo lo denotamos por $\mathfrak{u}(N, k, t, p, G, \epsilon)$.

Se tiene la siguiente proposición trivial:

PROPOSICIÓN 6.16. *Si* $\epsilon_1 \leq \epsilon_2$ *entonces* $\mathfrak{u}(N,k,t,p,G,\epsilon_1) \geq \mathfrak{u}(N,k,t,p,G,\epsilon_2)$.

Se deduce de la proposición anterior que existe $\epsilon_0 \in \mathbb{N}$ tal que para todo $\epsilon > \epsilon_0$, $\mathfrak{u}(N,k,t,p,G,\epsilon) = \mathfrak{u}(N,k,t,p,G,\epsilon_0)$. Si $\epsilon \to \infty$, denotaremos a $\mathfrak{u}(N,k,t,p,G,\epsilon)$ por

$$\mathfrak{u}(N,k,t,p,G).$$

EJEMPLO 6.17. *Consideremos el grupo trivial* $G = \{[id|id]\}$. *En la Figura 6.1, dibujamos* $\mathfrak{u}(25,7,2,1,G,\epsilon)$ *con respecto a* ϵ. *Podemos ver que*

$$\mathfrak{u}(25,7,2,1,G,1) = 180 > \mathfrak{u}(25,7,2,1,G,2) = 80 > \mathfrak{u}(25,7,2,1,G,3) = 70 > \mathfrak{u}(25,7,2,1,G,\epsilon) = 40$$

para $\epsilon \geq 4$. *Por lo tanto,* $\mathfrak{u}(25,7,2,1,G) = 40$.

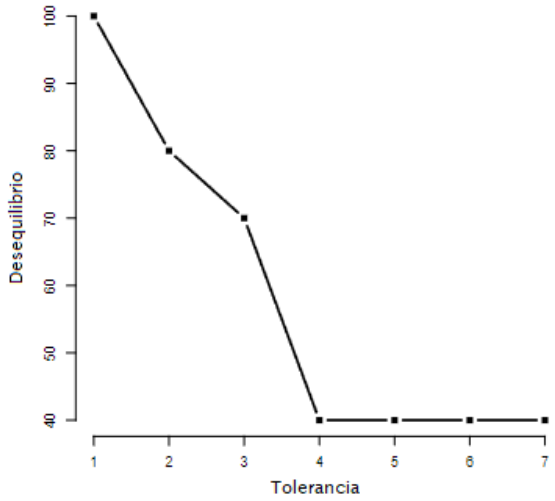

FIGURA 6.1. $\mathfrak{u}(25,7,2,1,G,\epsilon)$ y $G = \{[id|id]\}$

En general, el problema de optimización planteado en PMD es muy difícil de resolver, por lo que es conveniente introducir un nuevo tipo de AOAs que siguen estando muy cerca del concepto de arreglos ortogonales y también pueden usarse en aplicaciones de estadística cuando no existe un OA:

DEFINICIÓN 6.18. *Llamaremos cuasi arreglo ortogonal semi-extremo a un* $AOA(N,k,s,t,1)$ *en el que las primeras* $k-1$ *columnas forman un arreglo ortogonal.*

EJEMPLO 6.19. *El arreglo*

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 2 & 2 & 2 & 2 \\ 1 & 0 & 1 & 2 & 2 \\ 1 & 1 & 2 & 0 & 1 \\ 1 & 2 & 0 & 1 & 0 \\ 2 & 0 & 2 & 1 & 1 \\ 2 & 1 & 0 & 2 & 2 \\ 2 & 2 & 1 & 0 & 2 \end{pmatrix}$$

es un $AOA(9, 5, 3, 2, 1)$ *semi-extremo, ya que las primeras 4 columnas forman un* $OA(9, 4, 3, 2)$.

Dado un número impar q potencia de un primo, denotamos por R y NR a los conjuntos de cuadrados y no cuadrados en el cuerpo finito $\mathbb{F}_q$. Esto es, $R = \{x^2 \ : \ x \in \mathbb{F}_q \setminus \{0\}\}$ y $NR = \mathbb{F}_q \setminus (R \cup \{0\})$.

TEOREMA 6.20. *Sea* $\mathbb{F}_q$ *un cuerpo finito de orden impar. Tomamos un elemento* x *que estará en* R *si* $q \equiv 3 \mod 4$ *o estará en* NR *si* $q \equiv 1 \mod 4$ *y sean* a, b *dos elementos distintos que no están en* $\mathbb{F}_q$. *Considérese la matriz* $A^{[q,x]} = (a^{[q,x]}_{(i,j),k}) \in M_{q^2 \times (q+2)}(\mathbb{F}_q)$, *cuyas filas están indexadas por elementos en* $\mathbb{F}_q^2$ *y cuyas filas están indexadas por elementos de* $\mathbb{F}_q \cup \{a, b\}$, *donde*

$$a^{[q,x]}_{(i,j),k} = \begin{cases} ik + j, & \textbf{\textit{si}} \quad k \in \mathbb{F}_q \\ -i, & \textbf{\textit{si}} \quad k = a \\ (j - i)^2 + x \cdot i^2, & \textbf{\textit{si}} \quad k = b \end{cases}$$

Entonces $A^{[q,x]}$ *es un cuasi arreglo ortogonal semi-extremo, y para todo* p,

$$\mathrm{U}_{p,t}(A) = (q^2 - 1)q.$$

DEMOSTRACIÓN. En primer lugar, consideremos cualesquiera dos columnas indexadas por $k_1, k_2 \in \mathbb{F}_q$ y sea $(u, v) \in \mathbb{F}_q^2$. Veamos que existe una única fila indexada por (i, j) que tiene a los elementos u y v en las columnas k_1 y k_2, respectivamente. Para obtener i y j, nótese que

$$u = ik_1 + j \quad \text{y} \quad v = ik_2 + j,$$

de donde obtenemos que $u - v = i(k_1 - k_2)$, esto es

$$i = \frac{u - v}{k_1 - k_2}.$$

Por otro lado, podemos multiplicar u por k_2 (obteniendo $k_2 u = ik_1k_2 + jk_2$), v por k_1 (obteniendo $k_1 v = ik_1k_2 + jk_1$) y restamos las dos expresiones obtenidas para obtener que $k_1 v - k_2 u = j(k_1 - k_2)$, esto es,

$$j = \frac{k_1 v - k_2 u}{k_1 - k_2}.$$

En segundo lugar, consideremos una columna indexada por $k \in \mathbb{F}_q$ y la columna indexada por a (la columna $(q+1)$-ésima). Sea $(u, v) \in \mathbb{F}_q^2$. Veamos que existe una única fila indexada por (i, j) que tiene a los elementos u y v en las columnas k y a, respectivamente. Para obtener i y j, nótese que

$$u = ik + j \quad \text{y} \quad v = -i.$$

Se tiene entonces que

$$i = -v$$

y, despejando j de la expresión para u, se tiene que $j = u - ik$, esto es,

$$j = u + vk.$$

Ahora, tomemos una columna indexada por $k \in \mathbb{F}_q$ y la columna indexada por b (la columna $(q + 2)$-ésima). Sea $(u, v) \in \mathbb{F}_q^2$. Una única fila indexada por (i, j) que tiene a los elementos u y v en las columnas k y b satisface que

$$u = ik + j \quad \text{y} \quad v = (j - i)^2 + xi^2.$$

Trivialmente, se tiene que

$$j = u - ik.$$

Vamos a desarrollar la expresión para v:

$$\begin{aligned} v &= j^2 - 2ji + i^2 + xi^2 \\ &= (u - ik)^2 - 2(u - ik)i + i^2 + xi^2 \\ &= u^2 - 2uik + i^2k^2 - 2ui + 2i^2k + i^2 + xi^2 \\ &= (k^2 + 2k + 1 + x)i^2 - 2u(k + 1)i + u^2. \end{aligned}$$

De aquí se obtiene la ecuación cuadrática $((k+1)^2+x)i^2 - 2u(k+1)i + u^2 - v = 0$, cuya solución en $\mathbb{F}_q$ es

$$i = \frac{(k+1)u + \sqrt{(k+1)^2 v + x(v-u^2)}}{(k+1)^2 + x}$$

Nótese que la manera de escoger a x garantiza que el denominador sea distinto de cero. Para ver esto, consideremos la ecuación $(k+1)^2 + x = 0$, esto es, $x = -(k+1)^2 = (-1)(k+1)^2$. Demostremos que $-1 \in R$ si $q \equiv 1 \mod 4$ y $-1 \in NR$ si $q \equiv 3 \mod 4$.

Sea θ una raiz primitiva de $\mathbb{F}_q$, entonces $1 = \theta^{q-1}$, lo cual implica que $-1 = \theta^{(q-1)/2}$. Si $q \equiv 1 \mod 4$ entonces existe $r \in \mathbb{Z}$ tal que $q = 4r+1$. Por tanto, $-1 = \theta^{2r}$, es decir, $-1 \in R$. Por otro lado, si $q \equiv 3 \mod 4$ entonces existe $r \in \mathbb{Z}$ tal que $q = 4r+3$. Por tanto, $-1 = \theta^{2r+1}$, es decir, $-1 \in NR$.

Por lo tanto, si $q \equiv 1 \mod 4$, $x \in R$, lo cual contradice la elección de x para este caso. De igual forma, si $q \equiv 3 \mod 4$, $x \in NR$ y se obtiene la misma contradicción.

El número de filas que contienen a u y a v es 2, 1 o 0, dependiendo de si $(k+1)^2 v + x(v-u^2)$ está en R, es 0 o está en NR.

Finalmente, tomemos la columna indexada por a y la columna indexada por b. Sea $(u,v) \in \mathbb{F}_q^2$. Una única fila indexada por (i,j) que tiene a los elementos u y v en las columnas a y b satisface que

$$u = -i \quad \text{y} \quad v = (j-i)^2 + xi^2.$$

Trivialmente, se tiene que

$$i = -u$$

y veamos el desarrollo de v :

$$\begin{aligned} v &= (j+u)^2 + xu^2 \\ &= j^2 + 2ju + u^2 + xu^2, \end{aligned}$$

de donde se tiene la ecuación $j^2 + 2uj + u^2 + xu^2 - v = 0$, la cual tiene por solución

$$j = -u + \sqrt{v - xu^2}$$

y por tanto el número de filas que contienen a u y v es 2, 1 o 0 dependiendo de si $v - xu^2$ está en R, es 0 o está en NR. Así, $A^{[q,x]}$ es un cuasi arreglo ortogonal semi-extremo. Nos queda solo calcular el p-desequilibrio. Como A se trata de un cuasi arreglo ortogonal

semi-extremo, las primeras $q+1$ columnas tienen un desequilibrio nulo, por lo que solo hay que hacer el cálculo de la última columna con cada una de las demás.

Sabemos que la columna $(q+2)$-ésima (que es la etiquetada por b) está dada por

$$a^{[q,x]}_{(i,j),b} = (j-i)^2 + x \cdot i^2.$$

Por el análisis anterior, cada par $(i,j) \in \mathbb{F}_q^2$ aparece en el par de columnas (h,b), con $h \in \mathbb{F}_q \cup \{a\}$, ninguna vez, una vez o dos veces dependiendo de si ciertas expresiones pertenecen a R, son nulas o pertenecen a NR. El caso en el que (i,j) aparece una vez no lo tenemos en cuenta, ya que este término no suma nada en el cálculo del desequilibrio. Sabemos que R y NR tienen $(q-1)/2$ elementos, por lo que hay $(q-1)/2$ parejas que no aparecen ninguna vez, y hay $(q-1)/2$ parejas que aparecen dos veces. Las parejas que no aparecen y las que aparecen dos veces, suman un 1 en el cálculo del desequilibrio. Como hay q bloques de q filas en el arreglo, y hay $q+1$ columnas (distintas de la indexada por b), se tiene que $\mathrm{U}_{p,t}(A) = (q-1)q(q+1) = (q^2-1)q$ ■

EJEMPLO 6.21. *Para $q = 3$ y $x = 1$,*

$$A = \begin{pmatrix}
0 & 0 & 0 & 0 & 0 \\
0 & 1 & 2 & 1 & 2 \\
0 & 2 & 1 & 2 & 2 \\
1 & 1 & 1 & 0 & 1 \\
1 & 2 & 0 & 1 & 1 \\
1 & 0 & 2 & 2 & 2 \\
2 & 2 & 2 & 0 & 1 \\
2 & 0 & 1 & 1 & 2 \\
2 & 1 & 0 & 2 & 1
\end{pmatrix}$$

es un $AOA(9,5,3,1,1)$ semi-extremo y $\mathrm{U}_{p,2}(A) = 24$.

En efecto, si indexamos las tres primeras columnas por los elementos de $\mathbb{Z}_3$, que por simplicidad podemos denotarlos por $0,1,2$, la cuarta columna por 3 y la quinta columna por 4; y también denotamos cada fila por los elementos de $\mathbb{Z}_3 \times \mathbb{Z}_3$; se tiene del Teorema 6.20 el arreglo dado. El desequilibrio debe ser $\mathrm{U}_{p,2} = (3^2-1)\cdot 3 = 24$.

De forma similar podemos construir el siguiente cuasi arreglo ortogonal

EJEMPLO 6.22. *Para* $q = 5$ *y* $x = 2$*,*

$$A = \begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 2 & 3 & 4 & 1 & 3 \\
0 & 2 & 4 & 1 & 3 & 2 & 2 \\
0 & 3 & 1 & 4 & 2 & 3 & 2 \\
0 & 4 & 3 & 2 & 1 & 4 & 3 \\
1 & 1 & 1 & 1 & 1 & 0 & 1 \\
1 & 2 & 3 & 4 & 0 & 1 & 2 \\
1 & 3 & 0 & 2 & 4 & 2 & 4 \\
1 & 4 & 2 & 0 & 3 & 3 & 2 \\
1 & 0 & 4 & 3 & 2 & 4 & 1 \\
2 & 2 & 2 & 2 & 2 & 0 & 4 \\
2 & 3 & 4 & 0 & 1 & 1 & 3 \\
2 & 4 & 1 & 3 & 0 & 2 & 3 \\
2 & 0 & 3 & 1 & 4 & 3 & 4 \\
2 & 1 & 0 & 4 & 3 & 4 & 1 \\
3 & 3 & 3 & 3 & 3 & 0 & 4 \\
3 & 4 & 0 & 1 & 2 & 1 & 1 \\
3 & 0 & 2 & 4 & 1 & 2 & 4 \\
3 & 1 & 4 & 2 & 0 & 3 & 3 \\
3 & 2 & 1 & 0 & 4 & 4 & 3 \\
4 & 4 & 4 & 4 & 4 & 0 & 1 \\
4 & 0 & 1 & 2 & 3 & 1 & 1 \\
4 & 1 & 3 & 0 & 2 & 2 & 2 \\
4 & 2 & 0 & 3 & 1 & 3 & 4 \\
4 & 3 & 2 & 1 & 0 & 4 & 2
\end{pmatrix}$$

es un $AOA(25, 7, 5, 1, 1)$ *semi-extremo y* $\mathrm{U}_{p,2}(A) = 120$*.*

PROPOSICIÓN 6.23. *Sea* $p \in [1, \infty)$*,* $N, k, t \in \mathbb{N}$ *con* $t \leq k$*,* $\lambda \in \mathbb{R}$*,* S *un conjunto finito de tamaño* s *y* k *el número natural más grande para el que existe un* $OA(N, k-1, s, t)$ *con* $N = \lambda s^t$ *ejecuciones y fuerza* $t = 2$*. Se cumple la siguiente desigualdad:*

$$\mathfrak{u}(N, k, t, p) \leq s\lambda^p[(s-1)^p + (s-1)] =: \overline{U} \tag{6.10}$$

DEMOSTRACIÓN. Sea B un $OA(N, k-1, s, t)$ y A el $AOA(N, k, s, t)$ generado con las primeras $k-1$ columnas B y cuya última columna es cualquier columna de B. Sin pérdida de generalidad, podemos asumir que la columna k-ésima de A coincide con la primera columna de A.

Tenemos entonces que

$$\mathfrak{u}(N,k,t,p) = \sum_{x\in S^t}\sum_{j\in T_{t,k}} |n(A,x,j)-\lambda|^p \leq \sum_{\substack{x\in S^t\\ x_1=x_2}}\sum_{j\in T_{t,k}} |n(A,x,j)-\lambda|^p + \sum_{\substack{x\in S^t\\ x_1\neq x_2}}\sum_{j\in T_{t,k}} |n(A,x,j)-\lambda|^p$$

$$\leq s|\lambda s-\lambda|^p + s(s-1)|0-\lambda|^p = s|\lambda(s-1)|^p + s(s-1)|-\lambda|^p$$

$$= s\lambda^p[(s-1)^p + (s-1)]$$

Nótese que la tolerancia satisface que $\epsilon \leq \lambda(s-1)$

■

Podemos observar que para $\lambda = 1$ la cota superior $\overline{U} = 2s(s-1)$ para $p = 1$ y $\overline{U} = s^2(s-1)$ para $p = 2$ se alcanza para s igual a una potencia de un primo. Sin embargo, para $\lambda = 2$ la cota superior $\overline{U} = 4s(s-1)$ para $p = 1$ y $\overline{U} = 4s^2(s-1)$ para $p = 2$ no se alcanza para $s = 2$. Esto lo podemos resumir en la siguiente proposición.

PROPOSICIÓN 6.24. *Sea q una potencia de un primo y A un $AOA(q^2, q+2, q, 2, \epsilon)$, con $\epsilon \geq 1$. Entonces, $\mathrm{U}_{p,2}(A) \geq q((q-1)^p + (q-1))$ para $p = 1$ y $p = 2$.*

A continuación, se darán los principales resultados de los cálculos computacionales obtenidos al resolver el problema del mínimo desesequilibrio. Veremos primero los resultados para el mínimo desequilibrio, y después los resultados para la mínima tolerancia.

Para la búsqueda de cuasi arreglos ortogonales se implentaron los siguientes algoritmos.

Algoritmo 1: Modelo de Programación Entera.

En primer lugar se introdujo un modelo de **programación entera** del Problema del Mínimo Desequilibrio (PMD), cuya solución óptima es un cuasi arreglo ortogonal $AOA(N, k, s, t, \epsilon)$ con $N = \lambda s^t$ ejecuciones, k factores, s niveles, fuerza $t = 2$, índice λ y tolerancia ϵ. Sin pérdida de generalidad, consideramos que el arreglo contiene las λs^t combinaciones ordenadas en las primeras t columnas. Definamos los siguientes índices y conjuntos:

- i, denota la ejecución (o fila), donde $i \in \mathcal{I} = \{1 \ldots, N\}$;
- j, denota el factor (o columna), donde $j \in \mathcal{J} = \{t+1, \ldots, k\}$;
- c, denota la columna t-tupla, donde $c \in \mathcal{C} = \{1, \ldots, \binom{k-t}{t}\}$;
- m, denota el nivel (o símbolo), donde $m \in \mathcal{M} = \{1, \ldots, s\}$;
- l, denota la posición lexicográfica de la combinación $(x_1, \ldots, x_t)$, donde $l \in \mathcal{L} = \{1, \ldots, s^t\}$.

Ahora, considérese las siguientes variables:

- $x_{i,j}^m$ es una variable binaria, que toma el valor 1 si el elemento de la la fila i y columna j toma el valor m;
- $z_{i,c}^l$ es una variable binaria, que toma el valor 1 si la fila i y la t-tupla de columnas c contienen la combinación l-ésima;
- $\delta_c^{0,l}$ es una variable entera, tal que la t-tupla de columnas c contiene la combinación l-ésima exactamente $\lambda + \delta_c^{0,l}$ veces. En otras palabras, es la diferencia (positiva o negativa) entre la frecuencia de la combinación l-ésima y el índice λ. Por ejemplo, cuando el índice λ es 1 y la tolerancia ϵ es 1, entonces, $\delta_c^{0,l} = -1$ si la t-tupla c no contienen la combinación l-ésima, $\delta_c^{0,l} = 0$ si la t-tupla c contiene exactamente una vez la combinación l-ésima y $\delta_c^{0,l} = 1$ si la t-tupla c contiene exactamente el doble de la combinación l-ésima.
- $\delta^{1,m}$ es una variable entera, que toma un valor no nulo si se relaja la condición de que cada nivel aparezca λs veces a lo largo de las ejecuciones.
- $\delta_{m',j}^{2,m}$ es una variable entera, que toma un valor no nulo si se relaja la condición de que cada par de columnas $(1, j)$ contenga todas las s^t combinaciones λ veces.
- $\delta_{m',j}^{3,m}$ es una variable entera, que toma un valor no nulo si se relaja la condición de que cada par de columnas $(2, j)$ contenga todas las s^t combinaciones λ veces.

Con estas notaciones, el modelo matemático del PMD es el siguiente:

$$\text{mín} \sum_{c\in\mathcal{C},l\in\mathcal{L}} |\delta_c^{0,l}|^p + \sum_{m\in M} |\delta^{1,m}|^p + \sum_{m,m'\in\mathcal{M},j\in\mathcal{J}} |\delta_{m',j}^{2,m}|^p + |\delta_{m',j}^{3,m}|^p \tag{6.11a}$$

$$s.a. \sum_{i\in\mathcal{I}} x_{i,j}^m = \lambda\, s, \quad \forall j \in \mathcal{J}\setminus\{|\mathcal{J}|\},\ m\in\mathcal{M} \tag{6.11b}$$

$$\sum_{i\in\mathcal{I}} x_{i,|\mathcal{J}|}^m = \lambda\, s + \delta^{1,m}, \quad \forall m\in\mathcal{M} \tag{6.11c}$$

$$\sum_{m\in\mathcal{M}} x_{i,j}^m = 1, \quad \forall i\in\mathcal{I},\ j\in\mathcal{J} \tag{6.11d}$$

$$\sum_{l=1}^{\lambda} \sum_{i=(l-1)s^2+(m'-1)s+1}^{(l-1)s^2+m's} x_{i,j}^m = \lambda + \delta_{m',j}^{2,m}, \quad \forall j\in\mathcal{J},\ m,m'\in\mathcal{M} \tag{6.11e}$$

$$\sum_{l=1}^{\lambda} \sum_{i\in\mathcal{I}:i\equiv(l-1)s^2+m' \pmod s} x_{i,j}^m = \lambda + \delta_{m',j}^{3,m}, \quad \forall j\in\mathcal{J},\ m,m'\in\mathcal{M} \tag{6.11f}$$

$$\sum_{l\in\mathcal{L}} l\, z_{i,c}^l = s\sum_{m\in\mathcal{M}} m\, x_{i,j_1}^m + \sum_{m\in\mathcal{M}} m\, x_{i,j_2}^m - s, \quad \forall i\in\mathcal{I},\ c=(j_1,j_2)\in\mathcal{C} \tag{6.11g}$$

$$\sum_{l\in\mathcal{L}} z_{i,c}^l = 1, \quad \forall i\in\mathcal{I},\ c\in\mathcal{C} \tag{6.11h}$$

$$\sum_{i\in\mathcal{I}} z_{i,c}^l = \lambda + \delta_c^{0,l}, \quad \forall l\in\mathcal{L},\ c\in\mathcal{C} \tag{6.11i}$$

$$x_{i,j}^m,\ z_{i,c}^l \in \{0,1\}, \quad \forall i\in\mathcal{I},\ j\in\mathcal{J},\ c\in\mathcal{C},\ l\in\mathcal{L},\ m\in\mathcal{M} \tag{6.11j}$$

$$\delta_c^{0,l}, \delta_{m',j}^{2,m}, \delta_{m',j}^{3,m} \in \{-\lambda,\dots,\epsilon\}, \quad \forall j\in\mathcal{J},\ c\in\mathcal{C},\ l\in\mathcal{L},\ m,m'\in\mathcal{M} \tag{6.11k}$$

$$\delta^{1,m} \in \{-\lambda s,\dots,\lambda s^t - \lambda s\}, \quad \forall m\in\mathcal{M}. \tag{6.11l}$$

La función objetivo (6.11a) minimiza el p-desequilibrio de A, donde

$$\mathrm{U}_{p,2}(A) = \sum_{c\in\mathcal{C},l\in\mathcal{L}} |\delta_c^{0,l}|^p + \sum_{m,m'\in\mathcal{M},j\in\mathcal{J}} |\delta_{m',j}^{2,m}|^p + |\delta_{m',j}^{3,m}|^p.$$

Podemos observar que $\delta_c^{0,l}$, $\delta_{m',j}^{2,m}$ y $\delta_{m',j}^{e,m}$ corresponden a $n(A,x,c)-\lambda$, donde x es la l-ésima combinación y c es la t-tupla, para $c=(j_1,j_2)$, $c=(1,j_2)$ y $c=(2,j_2)$, respectivamente, $j_1,j_2\in\mathcal{J}$. Las restricciones (6.11b) garantizan que, para toda columna, cada nivel aparece λs veces a lo largo de todas las ejecuciones, salvo quizás, para la última columna, cuya condición se relaja como se indica en (6.11c), donde cada nivel puede aparecer $\lambda s+\delta^{1,m}$ veces. Las restricciones (6.11d) aseguran que cada celda tenga asociado exactamente un nivel. Las restricciones (6.11e) y (6.11f) obligan a que el par de columnas

$(1, j)$ y $(2, j)$ contengan las s^t combinaciones $\lambda+\delta^{2,m}_{m',j}$ o $\lambda+\delta^{3,m}_{m',j}$ veces, respectivamente, con $j \in \mathcal{J}$. Las restricciones (6.11g) determinan que para cada fila, cualquier par de columnas (j_1, j_2) corresponde a una combinación de S^t. Las restricciones (6.11h) establecen que para cada ejecución, hay exactamente una combinación asociada a cada par de columnas (j_1, j_2). Las restricciones (6.11i) aseguran que para cada par de columnas (j_1, j_2), cada posible combinación puede aparecer ninguna vez, una, dos, ..., o como máximo $\epsilon+\lambda$ veces. (6.11j) contiene las restricciones 0-1 y (6.11k)-(6.11l) las restricciones de integralidad.

Podemos adaptar el modelo anterior (6.11) para introducir simetrías en la matriz resultante de la manera que describiremos a continuación. Las restricciones (6.12a)-(6.12c) aseguran la existencia del automorfismo $[(r, \ldots, s)|id]$ que fija los símbolos $\{1, \ldots, r-1\}$ y permuta cíclicamente los símbolos $\{r, \ldots, s\}$, donde $r \in [s]$. Para cada ejecución $i \in [N]$, $\sigma_r(i)$ es la siguiente fila correspondiente, que prefija los automorfismos siguientes.

Nótese que para $r = 1$, se considera el ciclo más largo; para $r = 2$, se puede obtener una matriz de diferencias ([**90**]); para $r = s-1$, se considera el ciclo más pequeño; y para $r = s$, no se considera simetría.

(6.12a) $$x^m_{i,j} = x^m_{\sigma_r(i),j}, \qquad \forall i, j,\ \forall m \in \{1, \ldots, r-1\}$$

(6.12b) $$x^m_{i,j} = x^{m+1}_{\sigma_r(i),j}, \qquad \forall i, j,\ \forall m \in \{r, \ldots, s-1\}$$

(6.12c) $$x^s_{i,j} = x^r_{\sigma_r(i),j}, \qquad \forall i, j$$

Adicionalmente, para los casos con más de tres factores, $k \geq 4$, podemos considerar, simultáneamente o no, el automorfismo $[id|(1, 2)(3, 4)]$, esto es, la simetría que permuta el par de columnas $(1, 2)$ y $(3, 4)$. Las restricciones (6.13a)-(6.13b) aseguran la existencia de esa simetría. Para cada ejecución $i \in [N]$, $\sigma_0(i)$ es la siguiente fila correspondiente, que sigue de la simetría anterior.

(6.13a) $$x^m_{i,3} = x^m_{\sigma_0(i),4}, \qquad \forall i, m$$

(6.13b) $$x^m_{i,4} = x^m_{\sigma_0(i),3}, \qquad \forall i, m$$

(6.13c) $$x^m_{i,k} = x^m_{\sigma_0(i),k}, \qquad \forall i, m,\ \forall k > 4$$

Nótese que una vez que resolvemos el PMD, la posición (i, j) de A contiene el símbolo determinado por la variable no nula del vector $(x_{i,j}^1, \ldots, x_{i,j}^k)$, es decir, $a_{i,j} = \sum_m m\, x_{i,j}^m - 1$. Además, si la función objetivo es igual a 0, el PMD obtiene un OA; de lo contrario, puede obtener un AOA cuando el problema se resuelve hasta la optimización o, por el contrario, una cota superior en el valor de $\mathfrak{u}(\lambda s^2, k, 2, p)$.

Se puede observar que el PMD es un problema de Programación Lineal Entera (PLE) para $p = 1$ y es un problema de Programación Cuadrática Entera (PCE) para $p = 2$.

Los siguientes arreglos fueron obtenidos con el modelo de programación entera lineal y cuadrática respectivamente.

EJEMPLO 6.25. *El arreglo*

$$\begin{pmatrix} 0 & 0 & 2 & 2 & 2 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 2 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 2 & 2 & 1 \\ 1 & 2 & 0 & 1 & 2 \\ 2 & 0 & 0 & 1 & 1 \\ 2 & 1 & 1 & 0 & 2 \\ 2 & 2 & 2 & 2 & 0 \end{pmatrix}$$

es un AOA con $s = 3$*,* $k = 5$*,* $\lambda = 1$*. Su desequilibrio para* $p = 1$ *es* $\mathfrak{u} = 12$ *y su tolerancia es* $\epsilon = 2$*.*

EJEMPLO 6.26. *El arreglo*

$$\begin{pmatrix} 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 2 & 0 & 0 \\ 0 & 2 & 0 & 2 & 2 \\ 1 & 0 & 0 & 2 & 0 \\ 1 & 1 & 1 & 1 & 2 \\ 1 & 2 & 2 & 0 & 1 \\ 2 & 0 & 2 & 0 & 2 \\ 2 & 1 & 0 & 2 & 1 \\ 2 & 2 & 1 & 1 & 0 \end{pmatrix}$$

es un AOA con $s = 3$*,* $k = 5$*,* $\lambda = 1$*. Su desequilibrio para* $p = 2$ *es* $\mathfrak{u} = 18$ *y su tolerancia es* $\epsilon = 2$*.*

Algoritmo 2: Modelos Heurísticos.

Dado un grupo de automorfismos G que fijamos, utilizamos dos tipos de algoritmos de búsqueda metaheurística para obtener soluciones subóptimas del problema del mínimo desequilibrio: búsqueda local y búsqueda local bimodal, respectivamente. Lo resolvimos como un problema de optimización multiobjetivo en el que, si $\mathrm{U}_{p,t}(A)$ y $\mathrm{Tol}_t(A)$ son como en la Definición 6.8, los pares $(\mathrm{U}_{p,t}(A), \mathrm{Tol}_t(A))$ forman el conjunto de soluciones factibles, y un par $(\mathrm{U}_{p,t}(A), \mathrm{Tol}_t(A))$ domina a otro par $(\mathrm{U}_{p,t}(A'), \mathrm{Tol}_t(A'))$ si $\mathrm{U}_{p,t}(A) < \mathrm{U}_{p,t}(A')$ y $\mathrm{Tol}_t(A) \leq \mathrm{Tol}_t(A')$ o $\mathrm{U}_{p,t}(A) \leq \mathrm{U}_{p,t}(A')$ y $\mathrm{Tol}_t(A) < \mathrm{Tol}_t(A')$. Los algoritmos buscan aproximaciones al frente de Pareto correspondiente. Cuando terminan los algoritmos, tomamos como solución subóptima del PMD para G y ϵ el arreglo A con $(\mathrm{U}_{p,t}(A'), \epsilon)$ en la aproximación del frente de Pareto en caso de que exista dicha matriz A.

Construimos AOAs con dos diferentes tipos de grupos de automorfismos prescritos que se describirán más adelante. En todos los casos los AOAs pueden describirse a partir de un arreglo menor T cuyas filas corresponden a los representantes de las órbitas de la acción determinada por el grupo de automorfismos. Llamaremos a este arreglo la *plantilla* de todo el AOA A cuyas filas son las órbitas correspondientes, y diremos que $A = D(T)$ es el desarrollo de T.

Tanto en la búsqueda local como en la búsqueda local bimodal, tomamos el conjunto $\mathfrak{T}$ de todas las plantillas posibles como espacio de búsqueda.

En el **algoritmo de búsqueda local**, primero tomamos una plantilla aleatoria $T \in \mathfrak{T}$ y evaluamos el desequilibrio $\mathrm{U}_{p,t}(D(T))$ y la tolerancia $\mathrm{Tol}_t(D(T))$ de su desarrollo. Tomamos $\mathfrak{P} = \{(\mathrm{U}_{p,t}(D(T)), \mathrm{Tol}_t(D(T)))\}$ como estimación inicial del frente de Pareto y $\mathfrak{A} = \{D(T)\}$ como el conjunto de matrices asociadas a los elementos de la estimación del frente de Pareto. Luego probamos secuencialmente todas las plantillas obtenidas de T cambiando una de sus entradas. Si para uno de los cambios obtenemos una nueva plantilla $T' \in \mathfrak{T}$ tal que el par asociado no está dominado por ningún par en $\mathfrak{P}$, entonces agregamos $(\mathrm{U}_{p,t}(D(T')), \mathrm{Tol}_t(D(T')))$ a $\mathfrak{P}$ y sumamos $D(T')$ a $\mathfrak{A}$, y eliminamos (si los hay) los pares dominados por $(\mathrm{U}_{p,t}(D(T')), \mathrm{Tol}_t(D(T')))$ y sus desarrollos asociados de $\mathfrak{P}$ y $\mathfrak{A}$, respectivamente. A continuación, reemplazamos T por T' y comenzamos el proceso de cambios nuevamente. Si, por el contrario ningún cambio mejora la estimación del frente

de Pareto, entonces elegimos una nueva plantilla aleatoria y volvemos a repetir todo el proceso. Esto lo hacemos por un periodo de tiempo limitado a 72 horas, y finalmente fusionamos de la forma obvia los conjuntos $\mathfrak{P}$ y $\mathfrak{A}$ obtenidos en cada repetición del proceso, eliminando los pares dominados y sus correspondientes desarrollos.

En el **algoritmo de búsqueda local bi-modal**, como en el anterior, comenzamos eligiendo aleatoriamente una plantilla y evaluando su desequilibrio y tolerancia, y tomando el par como estimación inicial del frente de Pareto e iniciando con la plantilla el conjunto de arreglos asociado. A diferencia del algoritmo anterior, en este caso existen dos modos de funcionamiento para la búsqueda. En el primer modo, al que se ingresa inicialmente, las modificaciones son como en el algoritmo anterior, es decir, se intentan secuencialmente todos los cambios posibles en las entradas de una plantilla, y en caso de encontrar un par no dominado se siguen los mismos pasos que en el algoritmo de búsqueda local. Si ninguno de los cambios produce una mejora del frente de Pareto entonces, a diferencia de lo que se hizo en el algoritmo de búsqueda local, se ingresa a un segundo modo de operación y se realiza una búsqueda más fina haciendo modificaciones simultáneamente en dos posiciones de la plantilla. Al igual que en la búsqueda local, si obtenemos con alguna de las dobles modificaciones una plantilla no dominada, entonces sumamos el par (desequilibrio, tolerancia) a $\mathfrak{P}$ y la nueva plantilla a $\mathfrak{A}$ y eliminamos los posibles pares dominados y los arreglos asociados y volvemos a repetir el proceso, comenzando con la nueva plantilla en el primer modo. Al igual que en el algoritmo de búsqueda local, cuando no se alcanza ninguna mejora en el frente de Pareto se repite todo el proceso con una nueva plantilla aleatoria, y esto se hace por un tiempo límite de 72 horas, haciendo finalmente una fusión de las estimaciones del frente de Pareto.

Diremos que un AOA es *bi-cíclico* si para algún entero positivo r con $r|s$ y $r \leq k$ existe un automorfismo que permuta cíclicamente los primeros r símbolos y las primeras r columnas. Si etiquetamos los símbolos con $0, 1, \ldots s-1$ y las columnas con $1, 2, \ldots, k$, entonces la permutación es $[(0, 1, \ldots, r-1)|(1, 2, \ldots, r)]$. En los algoritmos hemos tomado r como el mayor divisor de s que satisface $r \leq k$.

Todas las órbitas en un cuasi arreglo ortogonal bi-cíclico tienen tamaño r y por lo tanto para determinarlo es suficiente dar $\frac{\lambda n^2}{r}$ k-tuplas. Llamaremos plantilla del AOA a tal familia de $\frac{\lambda n^2}{r}$ representantes de las órbitas, y dispondremos estos representantes en un arreglo de tamaño $\frac{\lambda n^2}{r} \times k$.

EJEMPLO 6.27. *El arreglo*

$$\begin{pmatrix} 1 & 1 & 1 & 2 & 1 \\ 0 & 1 & 2 & 0 & 2 \\ 2 & 1 & 0 & 1 & 0 \end{pmatrix}$$

es una plantilla de un AOA bi-cíclico con $s = 3, k = 5$ *y* $\lambda = 1$*. El AOA que se origina, ordenado con respecto a las dos primeras columnas, es*

$$\begin{pmatrix} 0 & 0 & 0 & 2 & 0 \\ 0 & 1 & 2 & 0 & 2 \\ 0 & 2 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 2 \\ 1 & 1 & 1 & 2 & 1 \\ 1 & 2 & 2 & 1 & 0 \\ 2 & 0 & 2 & 0 & 1 \\ 2 & 1 & 0 & 1 & 0 \\ 2 & 2 & 1 & 2 & 2 \end{pmatrix}$$

Su desequilibrio para $p = 2$ *es* $\mathfrak{u} = 20$*, y su tolerancia es* $\epsilon = 1$*.*

Se ha implementado tanto una búsqueda local simple como una búsqueda local de dos etapas de AOAs bi-cíclicos. Denotamos por BLBC y DEBC a los algoritmos de búsqueda local y de búsqueda local de dos etapas, respectivamente.

DEFINICIÓN 6.28. *Diremos que un AOA con conjunto de símbolos* $0, 1, \ldots, s-1$ *es cuasi cíclico si existe un automorfismo que fija el símbolo* 0 *y permuta cíclicamente los otros* $s-1$ *símbolos.*

Una de las órbitas es de tamaño 1 y es la k-túpla de todo ceros, y todas las demás órbitas tienen tamaño $s-1$. Las plantillas, en este caso, están formadas por $\lambda(s+1)$ filas, que representan a las órbitas no triviales, y el desarrollo de una plantilla tiene λ filas de ceros y las otras $\lambda(s+1)(s-1)$ son las órbitas completas representadas por las $\lambda(s+1)$ filas en la plantilla.

Los siguientes ejemplos muestran AOAs obtenidos con el algoritmo de búsqueda local de dos etapas.

EJEMPLO 6.29. *El arreglo*

$$\begin{pmatrix} 1 & 0 & 1 & 2 & 2 \\ 2 & 1 & 2 & 2 & 2 \\ 0 & 2 & 0 & 2 & 2 \end{pmatrix}$$

es una plantilla de un AOA bi-cíclico con $s = 3$, $k = 5$ *y* $\lambda = 1$. *El AOA que origina, ordenado con respecto a las primeras dos columnas, es*

$$\begin{pmatrix} 0 & 0 & 2 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 2 & 0 & 2 & 2 \\ 1 & 0 & 1 & 2 & 2 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 2 & 2 & 0 & 0 \\ 2 & 0 & 0 & 0 & 0 \\ 2 & 1 & 2 & 2 & 2 \\ 2 & 2 & 1 & 1 & 1 \end{pmatrix}$$

Su desequilibrio para $p = 1$ *es* $\mathfrak{u} = 12$, *y su tolerancia es* $\epsilon = 2$.

EJEMPLO 6.30. *El arreglo*

$$\begin{pmatrix} 1 & 0 & 1 & 0 & 2 \\ 2 & 1 & 2 & 1 & 2 \\ 0 & 2 & 0 & 2 & 2 \end{pmatrix}$$

es una plantilla de un AOA bi-cíclico con $s = 3$, $k = 5$ *y* $\lambda = 1$. *El AOA que origina, ordenado con respecto a las primeras dos columnas, es*

$$\begin{pmatrix} 0 & 0 & 2 & 2 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 2 & 0 & 2 & 2 \\ 1 & 0 & 1 & 0 & 2 \\ 1 & 1 & 0 & 0 & 1 \\ 1 & 2 & 2 & 1 & 0 \\ 2 & 0 & 0 & 2 & 0 \\ 2 & 1 & 2 & 1 & 2 \\ 2 & 2 & 1 & 1 & 1 \end{pmatrix}$$

Su desequilibrio para $p = 2$ *es* $\mathfrak{u} = 18$*, y su tolerancia es* $\epsilon = 1$.

Se ha implementado, de la misma manera que antes, una búsqueda local simple y una búsqueda local en dos etapas de AOAs cuasi cíclicos. Denotamos BLCC y DECC a los algoritmos de búsqueda local y búsqueda local en dos etapas, respectivamente.

EJEMPLO 6.31. *El arreglo*

$$\begin{pmatrix} 1 & 0 & 2 & 3 & 0 & 1 \\ 0 & 0 & 3 & 1 & 1 & 0 \\ 0 & 1 & 2 & 0 & 3 & 0 \\ 3 & 0 & 0 & 0 & 2 & 3 \\ 0 & 3 & 0 & 2 & 0 & 0 \end{pmatrix}$$

es una plantilla de un AOA cuasi cíclico con $s = 4$*,* $k = 6$ *y* $\lambda = 1$*. El AOA que origina, ordenado con respecto a las primeras dos columnas, es*

$$\begin{pmatrix} 0 & 0 & 3 & 1 & 1 & 0 \\ 0 & 1 & 2 & 0 & 3 & 0 \\ 0 & 2 & 1 & 3 & 2 & 0 \\ 0 & 3 & 0 & 2 & 0 & 0 \\ 1 & 0 & 2 & 3 & 0 & 1 \\ 1 & 1 & 3 & 2 & 2 & 1 \\ 1 & 2 & 0 & 1 & 3 & 1 \\ 1 & 3 & 1 & 0 & 1 & 1 \\ 2 & 0 & 1 & 2 & 3 & 2 \\ 2 & 1 & 0 & 3 & 1 & 2 \\ 2 & 2 & 3 & 0 & 0 & 2 \\ 2 & 3 & 2 & 1 & 2 & 2 \\ 3 & 0 & 0 & 0 & 2 & 3 \\ 3 & 1 & 1 & 1 & 0 & 3 \\ 3 & 2 & 2 & 2 & 1 & 3 \\ 3 & 3 & 3 & 3 & 3 & 3 \end{pmatrix}$$

Su desequilibrio para $p = 1$ es $\mathfrak{u} = 24$, y su tolerancia es $\epsilon = 3$.

EJEMPLO 6.32. *El arreglo*

$$\begin{pmatrix} 2 & 1 & 2 & 2 & 0 & 3 \\ 3 & 2 & 1 & 2 & 2 & 0 \\ 1 & 1 & 3 & 0 & 2 & 0 \\ 2 & 3 & 1 & 0 & 2 & 2 \\ 1 & 2 & 2 & 3 & 3 & 2 \end{pmatrix}$$

es una plantilla de un AOA cuasi cíclico con $s = 4$*,* $k = 6$ *y* $\lambda = 1$*. El AOA que origina, ordenado con respecto a las primeras dos columnas, es*

$$\begin{pmatrix} 0 & 0 & 3 & 2 & 1 & 2 \\ 0 & 1 & 1 & 3 & 3 & 1 \\ 0 & 2 & 0 & 0 & 1 & 3 \\ 0 & 3 & 2 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 2 & 3 \\ 1 & 1 & 3 & 0 & 2 & 0 \\ 1 & 2 & 2 & 3 & 3 & 2 \\ 1 & 3 & 0 & 2 & 1 & 1 \\ 2 & 0 & 0 & 3 & 3 & 0 \\ 2 & 1 & 2 & 2 & 0 & 3 \\ 2 & 2 & 3 & 1 & 0 & 1 \\ 2 & 3 & 1 & 0 & 2 & 2 \\ 3 & 0 & 2 & 0 & 0 & 1 \\ 3 & 1 & 0 & 1 & 1 & 2 \\ 3 & 2 & 1 & 2 & 2 & 0 \\ 3 & 3 & 3 & 3 & 3 & 3 \end{pmatrix}$$

Su desequilibrio para $p = 2$ *es* $\mathfrak{u} = 48$*, y su tolerancia es* $\epsilon = 3$*.*

Soluciones optimales y suboptimales del problema del mínimo desequilibrio.

A continuación se mostrarán los principales resultados de los experimentos computacionales al resolver el problema de mínimo desequilibrio, según la metodología explicada

anteriormente. Las Tablas de la 6.1 a la 6.4 muestran los resultados para el desequilibrio mínimo, mientras que las Tablas de la 6.5 a la 6.6 muestran los resultados para la tolerancia mínima.

Los resultados numéricos se detallan para arreglos con hasta $s = 10$ símbolos, k factores, fuerza $t = 2$, índice $\lambda \in \{1, 2\}$, $p \in \{1, 2\}$, $N = \lambda s^t$ ejecuciones y tolerancia $\epsilon \leq 10$. Nótese que k es el siguiente número de factores con respecto al arreglo ortogonal más grande conocido ([**19**], Capítulo 6, III). La metodología MP ha sido ejecutada bajo el software de optimización IBM ILOG CPLEX v20.1 ([**63**]) utilizando hasta 8 subprocesos. Los experimentos computacionales se realizaron en el clúster computacional ARINA de SGI/IZO-SGIker en la UPV/EHU ([**4**]).

La Tabla 6.1 muestra los resultados del 1-desequilibrio para el índice $\lambda = 1$, la Tabla 6.2 muestra los resultados del 2-desequilibrio para el índice $\lambda = 1$, la Tabla 6.3 muestra los resultados del 1-desequilibrio para el índice $\lambda = 2$ y la Tabla 6.4 muestra los resultados del 2-desequilibrio para el índice $\lambda = 2$. La primera columna indica los parámetros del caso, la segunda columna indica la cota superior $\overline{U}$, las siguientes cuatro columnas muestran los resultados de la programación entera y las últimas cuatro columnas para el heurístico. Los encabezados son los siguientes: (s, k), número de símbolos y factores; $\overline{U}$, cota superior para el valor del desequilibrio, ver fórmula en (6.10); $\mathfrak{u}$, valor de desequilibrio obtenido; $estado$, estado de resolución, donde OP significa que se ha encontrado la solución óptima, ML significa que se ha excedido el límite de memoria de 100 Gb y TL que se ha superado el límite de tiempo de 3 días, ^{i} significa que se ha considerado como entrada un arreglo ortogonal con menos de k factores, el diseño se ha obtenido con el paquete DoE.base ([**45**]) del software R ([**101**]); ^{j}, significa que se ha considerado, total o parcialmente, la solución para la alternativa p; ϵ, la tolerancia; G, la simetría utilizada, donde $[(k \dots s)|(1, 2)(3, 4)]$ denota el automorfismo relacionado con la permutación de símbolos $(k, \dots, s)$, donde $k \in [s]$ (ver modelo en ecuaciones (6.12)) y la permutación de la primera y segunda columnas y la tercera y cuarta columnas (ver modelo en ecuaciones (6.13)), y por último, $met.$, la metodología utilizada para la obtención de los resultados.

TABLA 6.1. Resultados del desequilibrio para $\lambda = 1$ y $p = 1$

Caso	Cota	Programación Entera				Heurísticos			
(s,k)	$\overline{U}$	u	estado	ϵ	G	u	ϵ	G	met.
$(2,4)$	4	4	OP	1	$[id\|(1,2)(3,4)]$	4	1		DEBC
$(3,5)$	12	12	OP	2	$[id\|(1,2)(3,4)]$	12	2		DEBC
$(4,6)$	24	24	OP	3	$[id\|(1,2)(3,4)]$	24	3		DECC
$(5,7)$	40	40	OP	4	$[(1,\ldots,4)\|id]$	40	4		DEBC
$(6,4)$	60	4	OP	1	$[(2,\ldots,5)\|id]$	12	1		DEBC
$(7,9)$	84	84	TL	6	$[(1,\ldots,6)\|id]$	84	6		DECC
$(8,10)$	112	112	OP	7	$[(1,\ldots,7)\|id]$	112	7		DECC
$(9,11)$	144	144	OP^i	8	$[id\|id]$	976	8		DECC
$(10,5)$	180	36	TL	1	$[(1,\ldots,9)\|(1,2)(3,4)]$	36	1		DECC

TABLA 6.2. Resultados del desequilibrio para $\lambda = 1$ y $p = 2$

Caso	Cota	Programación Entera				Heurísticos			
(s,k)	$\overline{U}$	u	estado	ϵ	G	u	ϵ	G	met.
$(2,4)$	4	4	OP	1	$[id\|(1,2)(3,4)]$	4	1		DEBC
$(3,5)$	18	18	OP	2	$[id\|(1,2)(3,4)]$	18	1		DEBC
$(4,6)$	48	48	OP	3	$[(1,2,3)\|id]$	48	3		DECC
$(5,7)$	100	100	OP	4	$[1,\ldots,4)\|id]$	100	1		DEBC
$(6,4)$	180	4	OP	1	$[(2,\ldots,5)\|id]$	12	1		DEBC
$(7,9)$	294	294	OP^j	6	$[(1,\ldots,6)\|id]$	294	6		DECC
$(8,10)$	448	448	OP^j	7	$[(1,\ldots,7)\|id]$	448	7		DECC
$(9,11)$	648	648	ML^i	4	$[id\|id]$	1144	8		DECC
$(10,5)$	900	36	OP^i	1	$[(1,\ldots,9)\|(1,2)(3,4)]$	36	1		DECC

TABLA 6.3. Resultados del desequilibrio para $\lambda = 2$ y $p = 1$

Caso	Cota	Programación Entera				Heurísticos			
(s,k)	$\overline{U}$	u	estado	ϵ	G	u	ϵ	G	met.
$(2,8)$	8	8	OP	2	$[id\|(1,2)(3,4)]$	24	2		DEBC
$(3,8)$	24	18	OP	1	$[id\|id]$	24	4		DEBC
$(4,10)$	48	32	OP^i	2	$[id\|id]$	156	3		DECC
$(5,12)$	80	60	OP^i	3	$[id\|id]$	472	8		DECC
$(6,8)$	120	48	OP^j	1	$[id\|id]$	140	5		DECC
$(7,16)$	168	140	ML^i	5	$[id\|id]$	2232	6		DECC
$(8,18)$	224	192	TL^i	6	$[id\|id]$	4102	7		DECC
$(9,20)$	288	1244	TL^i	10	$[id\|id]$	6896	8		DECC
$(10,11)$	360	3564	TL^j	9	$[(1,\ldots,9)\|(1,2)(3,4)]$	1386	2		DECC

TABLA 6.4. Resultado del desequilibrio para $\lambda = 2$ and $p = 2$

Caso	Cota	Programación Entera				Heurísticos			
(s,k)	$\overline{U}$	u	estado	ϵ	G	u	ϵ	G	met.
$(2,8)$	16	16	OP	1	$[id\|id]$	48	1		DEBC
$(3,8)$	72	18	TL	1	$[id\|id]$	54	2		DEBC
$(4,10)$	192	64	TL^i	2	$[id\|id]$	208	2		DEBC
$(5,12)$	400	150	ML^i	3	$[id\|id]$	640	1		DEBC
$(6,8)$	720	48	TL^i	1	$[id\|id]$	144	1		DEBC
$(7,16)$	1176	490	OP^j	5	$[id\|id]$	2958	6		DECC
$(8,18)$	1792	768	OP^j	6	$[id\|id]$	5362	7		DECC
$(9,20)$	2592	2456	TL^i	6	$[id\|id]$	9072	8		DECC
$(10,11)$	3600	7920	OP^j	9	$[(1,\ldots,9)\|(1,2)(3,4)]$	1458	1		DECC

A continuación, veamos los resultados para la tolerancia mínima $\epsilon = 1$ en la Tabla 6.5 para el índice $\lambda = 1$ y en la Tabla 6.6 para el índice $\lambda = 2$. La primera columna denota el caso; las columnas segunda a cuarta corresponden a la solución MP y denotan el desequilibrio, el estado final de la implementación y la simetría utilizada, respectivamente; las columnas quinta a séptima corresponden a las soluciones heurísticas y denotan el desequilibrio, la simetría y la metodología, respectivamente.

TABLA 6.5. Resultados del desequilibrio para $\lambda = 1$ y mínima tolerancia ($\epsilon = 1$)

Caso	Programación Entera			Heurísticos	
(s,k)	u	estado	G	u	met.
$(2,4)$	4	OP	$[id\|(1,2)(3,4)]$	4	DEBC
$(3,5)$	18	OP	$[id\|id]$	18	DEBC
$(4,6)$	48	TL	$[id\|id]$	60	DECC
$(5,7)$	128	TL	$[id\|id]$	100	DEBC
$(6,4)$	4	OP	$[(2,\ldots,5)\|id]$	12	DEBC
$(7,9)$	576	TL	$[(1,\ldots,6)\|id]$	336	DECC
$(8,10)$	1022	TL	$[(1,\ldots,7)\|id]$	504	DECC
$(9,11)$	2272	TL	$[(1,\ldots,8)\|id]$	1216	DECC
$(10,5)$	36	TL	$[(1,\ldots,9)\|(1,2)(3,4)]$	36	DECC

TABLA 6.6. Resultados del desequilibrio para $\lambda = 2$ y tolerancia mínima

Caso	Programación entera					Heurísticos			
(s,k)	$\mathfrak{u}$	estado	ϵ	G	met.	$\mathfrak{u}$	ϵ	G	met.
$(2,8)$	16	OP	1	$[id\|id]$	MP	48	1	$[(0,1)\|(1,2)]$	DEBC
$(3,8)$	18	OP	1	$[id\|id]$	MP	66	1	$[(0,1,2)\|(1,2,3)]$	DEBC
$(4,10)$	410	TL	1	$[(0,\ldots,3)\|id]$	MP	224	1	$[(0,\ldots,3)\|(1,\ldots,4)]$	DEBC
$(5,12)$	-	TL	1	$[(0,\ldots,4)\|id]$	MP	640	1	$[(0,\ldots,4)\|(1,\ldots,5)]$	DEBC
$(6,8)$	48	TL	1	$[id\|id]$	MP	144	1	$[(0,\ldots,5)\|(1,\ldots,6)]$	DEBC
$(7,16)$	-	TL	1	$[id\|id]$	MP	2716	2	$[(0,\ldots,6)\|(1,\ldots,7)]$	DEBC
$(8,18)$	-	TL	1	$[id\|id]$	MP	4864	2	$[(0,\ldots,7)\|(1,\ldots,8)]$	DEBC
$(9,20)$	-	TL	1	$[id\|id]$	MP	8226	2	$[(0,\ldots,8)\|(1,\ldots,9)]$	DEBC
$(10,11)$	-	TL	1	$[id\|id]$	MP	1458	1	$[(1,\ldots,9)\|id]$	DECC

En la Tabla 6.6 vemos que hay algunos casos de la programación entera que aparece "-" y algunos casos de heurísticos con $\epsilon = 2$. Esto es debido a que los algoritmos no fueron capaces de encontrar un AOA con tolerancia $\epsilon = 1$.

A continuación introducimos algunas comparaciones con los resultados publicados en la literatura científica. Por un lado, en la Tabla 6.7, mostramos la comparación de los nuevos resultados para los arreglos $AOA(36, 7, 6, 2, \epsilon)$ en **[81]** y $AOA(9, 8, 3, 2, \epsilon)$ en **[70]**. Por otra parte, en la Tabla 6.8 para n^2 ejecuciones y en la Tabla 6.9 para $2n^2$ ejecuciones, comparamos todos los resultados comunes presentados en las tablas anteriores para el desequilibrio mínimo con los diseños uniformes disponibles en **[72]**. Hemos considerado $D_p = \mathfrak{u}/\binom{k}{2}$ con $p \in \{1, 2\}$ como en **[81]**. La medida de discrepancia centrada de L_2 (DC), la medida de discrepancia envolvente de L_2 (DE), **[?, 55]** y la medida de discrepancia de mezcla de L_2 (DM) **[120]** se calcula con el paquete DiceDesign **[34]** del software R **[101]**, donde se ha aplicado la función

$$\begin{array}{rccc} f: & \{0,1,\ldots,s-1\} & \to & (0,1) \\ & x & \to & \frac{2x+1}{2s} \end{array}$$

TABLA 6.7. Comparación de los resultados para los casos en [**81**] y [**70**]

s	k	λ	p	$\mathfrak{u}_1$	ϵ	$\mathfrak{u}_2$	ϵ	D_1	D_2	DC	DE	DM	$OA(1)$	Met.
3	8	1	1	68	2	72	2	2.4286	2.5714	0.2242	1.5638	4.2253	0	Ke [**70**]
3	8	1	1	66	2	72	2	2.3571	2.5714	0.2351	1.5638	4.2667	0	DC [**55**]
3	8	1	1	66	2	72	2	2.3571	2.5714	0.2351	1.5638	4.2667	0	DE [**55**]
3	8	1	1	48	2	72	2	1.7143	2.5714	0.2443	1.5638	4.2936	0	DECC
3	8	1	1	72	1	72	1	2.5714	2.5714	0.2392	1.5638	4.2908	0	PE
3	8	1	1	48	2	72	2	1.7143	2.5714	0.2266	1.5638	4.2282	0	PE
6	7	1	1	140	2	144	2	6.6667	6.8571	0.0419	0.2206	0.4674	0	Ma [**81**]
6	7	1	1	276	2	286	2	13.1429	13.6190	0.0359	0.2247	0.4548	0	DC [**55**]
6	7	1	1	100	1	100	1	4.7619	4.7619	0.0402	0.2209	0.4612	0	DECC
6	7	1	1	100	1	100	1	4.7619	4.7619	0.0391	0.2154	0.4507	0	PE

Para el caso $(s,k) = (6,7)$, tanto con el PE como con los heurísticos, se obtiene un desequilibrio de $\mathfrak{u} = 100$ para $p = 1,2$ con la mínima tolerancia $\epsilon = 1$. La matriz del PE se ha obtenido con el automorfismo $[(2,\ldots,5)|id]$ y la matriz del heurístico DECC, con el automorfismo $[(1,\ldots,5)|id]$.

Para el caso $(s,k) = (3,8)$ tanto con el PE como con los heurísticos se obtiene un desequilibrio de $\mathfrak{u} = 48$ para $p = 1,2$ con la tolerancia $\epsilon = 2$. Ambas matrices se han obtenido con el automorfismo $[(1,2)|id]$. Además, la matriz del PE obtuvo la tolerancia mínima con $\mathfrak{u} = 72$ y sin simetrías.

TABLA 6.8. Comparación de los resultados para la web de diseños uniformes [**55**] y $\lambda = 1$

s	k	λ	p	$\mathfrak{u}_1$	ϵ	$\mathfrak{u}_2$	ϵ	D_1	D_2	DC	DE	DM	$OA(1)$	Met.
3	5	1	1	20	1	20	1	2.0000	2.0000	0.0773	0.3412	0.5246	0	DC
3	5	1	1	16	2	18	2	1.6000	1.8000	0.0841	0.3386	0.5323	0	DE
3	5	1	1	18	1	18	1	1.8000	1.8000	0.0814	0.3386	0.5298	0	PE
3	5	1	1	12	2	18	2	1.2000	1.8000	0.0817	0.3386	0.5316	0	PE
4	6	1	1	48	1	48	1	3.2000	3.2000	0.0603	0.3243	0.5439	0	DC
4	6	1	1	48	1	48	1	3.2000	3.2000	0.0652	0.3021	0.5371	0	DE
4	6	1	1	48	1	48	1	3.2000	3.2000	0.0703	0.3129	0.5599	0	PE
4	6	1	1	24	3	48	3	1.6000	3.2000	0.0697	0.3145	0.5602	0	PE
5	7	1	1	180	2	186	2	8.5714	8.8571	0.0516	0.3293	0.6845	0	DC
5	7	1	1	128	1	128	1	6.0952	6.0952	0.0703	0.3605	0.8546	8	PE
5	7	1	1	40	4	100	4	1.9048	4.7619	0.0583	0.3217	0.6952	0	PE
6	4	1	1	16	1	16	1	2.6667	2.6667	0.0124	0.0454	0.0567	0	DC
6	4	1	1	4	1	4	1	0.6667	0.6667	0.0135	0.0452	0.0571	0	PE

TABLA 6.9. Comparación de los resultados para la web de diseños uniformes [**55**] y $\lambda = 2$

s	k	λ	p	$\mathfrak{u}_1$	ϵ	$\mathfrak{u}_2$	ϵ	D_1	D_2	DC	DE	DM	$OA(1)$	Met.
3	8	2	1	16	2	18	2	0.5714	0.6429	0.1492	1.2517	3.3878	0	DC
3	8	2	1	16	2	18	2	0.5714	0.6429	0.1522	1.2517	3.3936	0	DE
3	8	2	1	18	1	18	1	0.6429	0.6429	0.1545	1.2517	3.4052	0	PE
3	8	2	1	24	2	26	2	0.8571	0.9286	0.1537	1.2580	3.4088	0	PE
4	10	2	1	272	2	310	2	6.0444	6.8889	0.1588	1.7177	5.8851	0	DC
4	10	2	1	206	2	210	2	4.5778	4.6667	0.1693	1.6747	5.8821	0	DE
4	10	2	1	410	1	410	1	9.1111	9.1111	0.1907	1.7750	6.3064	0	PE
4	10	2	1	424	2	520	2	9.4222	11.5556	0.1936	1.8202	6.4585	0	PE
5	12	2	1	944	3	1166	3	14.3030	17.6667	0.1516	2.5771	12.6809	0	DC
5	12	2	1	60	3	150	3	0.9091	2.2727	0.1621	2.3661	12.1654	0	PE
7	16	2	1	4268	4	5786	4	35.5667	48.2167	0.2008	6.7195	62.7258	0	DC
7	16	2	1	140	5	490	5	1.1667	4.0833	0.2433	6.1279	59.9444	0	PE

El enfoque del PE explicado en este capítulo supera notablemente los resultados del desequilibrio. Según la medida DC, como se esperaba, es ligeramente mejor para las matrices DC que para las matrices PE, pero ligeramente peor para las matrices DE que para las matrices PE. Además, las medidas DE y DM son ligeramente mejores para las matrices PE.

En la comparativa de las Tablas 6.1-6.6, podemos observar que hay 16 casos en los que ambos criterios coinciden, es decir, se obtiene el mínimo desequilibrio para la mínima tolerancia $\epsilon = 1$. Resumiendo, el enfoque de programación entera obtuvo mejores resultados en más casos que el que el enfoque heurístico para el desequilibrio mínimo, mientras que el heurístico se comporta mejor para la tolerancia mínima. Se obtuvieron empates entre ambas metodologías en un tercio de los casos, ver Tabla 6.10 con el número de mejores desequilibrios encontrados por metodología y objetivo. En cambio, la construcción algebraica obtuvo peor desequilibrio para $s = 3$, igual para $s \in \{5, 7\}$ y mejor desequilibrio para $s = 9$. Por lo tanto, consideramos que la construcción algebraica es una construcción prometedora para una cantidad de símbolos grande.

TABLA 6.10. Comparación en términos del número de mejores desequilibrios por objetivo y algoritmo

Objetivo	PE	Empates	Heurístico
mínimo desequilibrio	20	14	2
mínima tolerancia	5	3	10

En la Figura 6.2 mostramos los mejores resultados obtenidos con la programación entera o con los heurísticos para el desequilibrio normalizado para $p = 1$ en rojo y $p = 2$ en azul, cuando $\lambda = 1$ a la izquierda y $\lambda = 2$ a la derecha. Podemos observar que el mejor desquilibrio normalizado se obtiene para $p = 1$ en ambos casos.

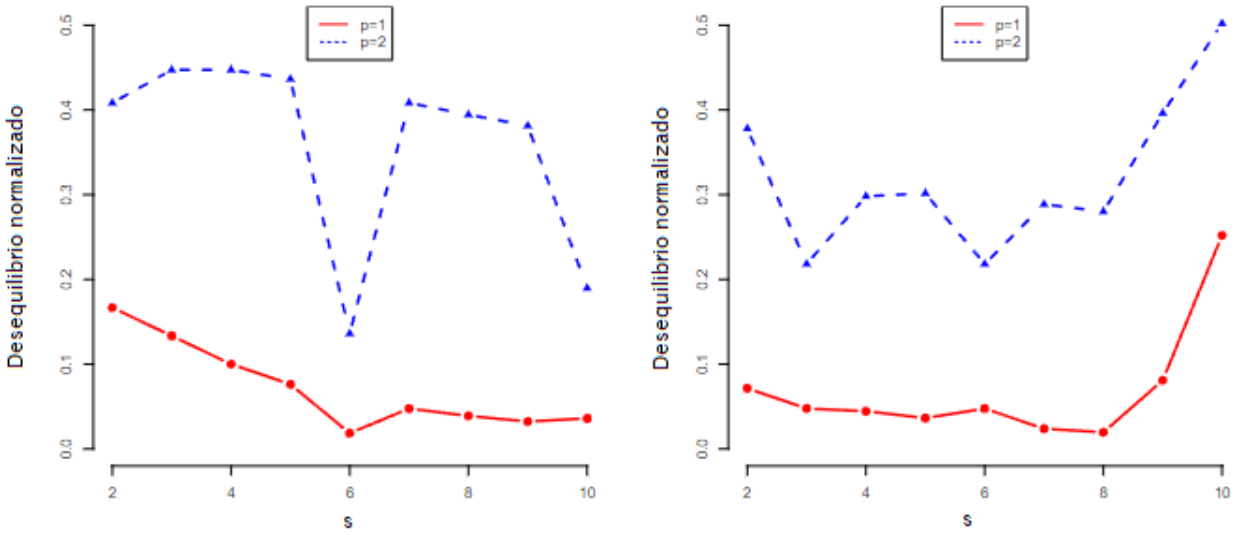

FIGURA 6.2. Mejores resultados para el desequilibrio normalizado cuando $\lambda = 1$ (izquierda) y $\lambda = 2$ (derecha)

Capítulo 7

TRABAJO A FUTURO: ARREGLOS ORTOGONALES INFINITOS

Como trabajo a futuro, pretendemos generalizar el concepto de arreglo ortogonal al caso en que el número de símbolos sea infinito (numerable), y estudiamos la existencia de tales arreglos ortogonales infinitos que admiten al grupo $\mathbb{Z}$ como un grupo de automorfismos que actúa regularmente sobre el conjunto de símbolos y también cuando fija un símbolo y actúa regularmente sobre los demás.

Vamos a centrarnos en el caso de fuerza 2 e índice unidad, aunque puede ampliarse fácilmente a diferentes valores de la fuerza y del índice.

Análogamente al caso finito, si S es un alfabeto infinito de cardinalidad numerable y $m \in \mathbb{N}$, un $OA(m, \infty)$ será un arreglo con sus filas indexadas por S^2 y con m columnas, con entradas en S, en el que cada subarreglo con todas las filas y dos columnas diferentes contiene cada par de S^2 exactamente una vez en una fila. De forma más general, si la matriz tiene una cantidad numerable de columnas diremos que es un $OA(\infty, \infty)$. Por supuesto, en esta situación, si tomamos las primera m columnas con $m \in \mathbb{N}$, obtendremos un $OA(m, \infty)$.

Los automorfismos de arreglos ortogonales infinitos dados por permutaciones de símbolos y permutaciones de columnas se pueden definir de manera análoga al caso finito. En capítulos anteriores se analizaron los arreglos ortogonales que admiten grupos cíclicos finitos que fijan un símbolo y actúan regularmente sobre los otros. En la teoría de grupos, hay dos clases de grupos cíclicos: los finitos y los infinitos, siendo estos últimos

isomorfos al grupo aditivo de los números enteros. Por lo tanto, es natural considerar una generalización de los conceptos de matrices de diferencias y cuasi matrices de diferencias al caso infinito en el que el grupo es $\mathbb{Z}$.

DEFINICIÓN 7.1. *Si $m \in \mathbb{N}$, una matriz de diferencias cíclica infinita $MDCI(m)$ es una matriz $Q = (q_{ij})$ con $i \in \{1, \ldots, m\}$ y $j \in \mathbb{N}$, con entradas en $\mathbb{Z}^+$, donde $\mathbb{Z}^+$ denota el conjunto de enteros no negativos, tal que para cada $1 \leq i < j \leq m$ el multiconjunto*

$$\{q_{il} - q_{jl} \ : \ l \in \mathbb{Z}^+\}$$

contiene todos los números enteros exactamente una vez.

DEFINICIÓN 7.2. *Una matriz de diferencias cíclica infinita $MDCI(\infty)$ es una matriz $Q = (q_{ij})$ con $i, j \in \mathbb{N}$, con entradas en $\mathbb{Z}^+$, donde $\mathbb{Z}^+$ denota el conjunto de enteros no negativos, tal que para cada $i, j \in \mathbb{N}$ el multiconjunto*

$$\{q_{il} - q_{jl} \ : \ l \in \mathbb{Z}^+\}$$

contiene todos los números enteros exactamente una vez.

Claramente, para todo $m \in \mathbb{N}$, las primeras m columnas de una $MDCI(\infty)$ es una $MDCI(m)$.

DEFINICIÓN 7.3. *Si $m \in \mathbb{N}$, una cuasi matriz de diferencias cíclica infinita $MCDCI(m)$ es una matriz $Q = (q_{ij})$ con $i \in \{1, \ldots, m\}$ y $j \in \mathbb{N}$, con entradas en $\mathbb{Z}^+ \cup \{-\}$, tal que cada fila contiene exactamente una entrada vacía (es decir, –), cada columna contiene como máximo una entrada vacía, y para cada $1 \leq i < j \leq m$ el multiconjunto*

$$\{q_{il} - q_{jl} \ : l \in \mathbb{Z}^+, \text{ con } q_{il} \text{ y } q_{jl} \text{ no vacíos}\}$$

contiene todos los números enteros exactamente una vez.

DEFINICIÓN 7.4. *Una cuasi matriz de diferencias cíclica infinita $MCDCI(\infty)$ es una matriz $Q = (q_{ij})$ con $i, j \in \mathbb{N}$, con entradas en $\mathbb{Z}^+ \cup \{-\}$, tal que cada fila contiene exactamente una entrada vacía, cada columna contiene como máximo una entrada vacía, y para cada $1 \leq i < j \leq m$ el multiconjunto*

$$\{q_{il} - q_{jl} \ : l \in \mathbb{Z}^+, \text{ con } q_{il} \text{ y } q_{jl} \text{ no vacíos}\}$$

contiene todos los números enteros exactamente una vez.

Tenemos de nuevo que para cualquier $m \in \mathbb{N}$ las primeras m columnas de una $MCDCI(\infty)$ es una $MCDCI(m)$.

Daremos una construcción, que conjeturamos que es una $MDCI(m)$ para cualquier $m \in \mathbb{N}$. Primero introduciremos alguna notación. Si $m \in \mathbb{N}$ y, para todo $n \in \mathbb{N}$, $Q^{[m,n]} = (q_{r,s}^{[m,n]}) \in M_{m\times n}(\mathbb{Z})$, diremos que la sucesión $\{Q^{[m,n]}\}_{n\in\mathbb{N}}$ es una sucesión de matrices compatible si $q_{r,s}^{[m,n_1]} = q_{r,s}^{[m,n_2]}$ siempre que $n_1 < n_2$ y $1 \leq r \leq m, 1 \leq s \leq n_1$. En este caso llamaremos $\sum_{n\in\mathbb{N}} Q^{[m,n]}$ a la matriz $Q^{[m]} = (Q_{r,s}^{[m]})$ con m filas y un número infinito de columnas indexadas por $\mathbb{N}$ con $Q_{r,s}^{[m]} = Q_{r,s}^{[m,s]}\ \forall r \in \{1,\ldots,m\}, \forall s \in \mathbb{N}$.

Ahora daremos un algoritmo codicioso que, para cualesquiera $m, n \in \mathbb{N}$, produce una matriz $Q^{[m,n]}$ tal que la sucesión $\{Q^{[m,n]}\}_{n\in\mathbb{N}}$ es compatible y su suma es la $MDCI(m)$ conjeturada deseada.

Algoritmo 1

Entrada: $n, m \in \mathbb{N}$

Salida $Q^{[m,n]} \in M_{m\times n}(\mathbb{Z})$

Para $i \in \{0,\ldots,m\}$ hacer lo siguiente

  Para $j \in \{1,\ldots,n\}$ hacer lo siguiente

    $D = \{q_{i,k}^{[m,n]} + q_{l,j}^{[m,n]} - q_{l,k}^{[m,n]} \mid 0 \leq l < i, 1 \leq k < j\}$

    $q_{i,j}^{[m,n]} = \text{mín}\{\mathbb{Z}^+ - D\}$

Eliminar la fila correspondiente a $i = 0$

Veamos un ejemplo para $m = 3, n = 4$. Obviamente, $D = \emptyset$ cuando $i = 0$ y también cuando $j = 1$.

Mostraremos a continuación D en los demás casos:

i/j	2	3	4
1	{0}	{0,1}	{0,1,2}
2	{0,1}	{0,2,3}	{0,1,2,3,4}
3	{0,1,2}	{0,1,2,3,4}	{0,3,5,6,9}

Por lo tanto, la matriz extendida es

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 3 \\ 0 & 2 & 1 & 5 \\ 0 & 3 & 5 & 1 \end{pmatrix},$$

y cuando ignoramos la primera fila obtenemos

$$Q^{[3,4]} = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 0 & 2 & 1 & 5 \\ 0 & 3 & 5 & 1 \end{pmatrix}.$$

CONJETURA 7.5. *Si* $m \in \mathbb{N}$*, entonces* $Q^{[m]} = \sum_{n\in\mathbb{N}} Q^{[m,n]}$ *es una* $MDCI(m)$.

Es importante en el Algoritmo 1 eliminar al final la primera fila de la matriz, porque si no hacemos esto no obtenemos un arreglo de diferencias infinito, porque entonces la diferencia entre una fila y la primera fila no tomaría valores negativos.

La suma vertical de $Q^{[m]}$ en el siguiente corolario se toma de la manera obvia similar a lo que hicimos antes para las sumas horizontales. En el caso de que la conjetura fuera cierta obtendríamos lo siguiente:

COROLARIO 7.6. $Q = \sum_{m\in\mathbb{N}} Q^{[m]}$ *es una* $MDCI(\infty)$.

Una consecuencia del Corolario anterior es que existe una matriz de diferencias cíclica infinita MDCI(∞).

A continuación mostraremos la primera matriz cuadrada de orden 20 obtenida a partir de Q. Agregaremos nuevamente la primera fila de ceros para mantener la simetría de la matriz:

$$\begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 \\
0 & 2 & 1 & 5 & 7 & 3 & 10 & 4 & 13 & 15 & 6 & 18 & 20 & 8 & 23 & 9 & 26 & 28 & 11 & 31 \\
0 & 3 & 5 & 1 & 9 & 2 & 7 & 11 & 4 & 8 & 16 & 6 & 23 & 20 & 28 & 24 & 10 & 34 & 30 & 12 \\
0 & 4 & 7 & 9 & 1 & 6 & 2 & 5 & 3 & 11 & 14 & 23 & 19 & 26 & 8 & 29 & 24 & 10 & 27 & 38 \\
0 & 5 & 3 & 2 & 6 & 1 & 11 & 16 & 18 & 21 & 26 & 9 & 4 & 32 & 34 & 42 & 40 & 7 & 15 & 8 \\
0 & 6 & 10 & 7 & 2 & 11 & 1 & 9 & 20 & 3 & 23 & 8 & 13 & 4 & 29 & 36 & 38 & 26 & 45 & 44 \\
0 & 7 & 4 & 11 & 5 & 16 & 9 & 1 & 15 & 2 & 29 & 28 & 32 & 25 & 3 & 13 & 45 & 42 & 6 & 24 \\
0 & 8 & 13 & 4 & 3 & 18 & 20 & 15 & 1 & 7 & 33 & 2 & 9 & 40 & 16 & 34 & 5 & 11 & 44 & 49 \\
0 & 9 & 15 & 8 & 11 & 21 & 3 & 2 & 7 & 1 & 42 & 26 & 5 & 35 & 33 & 4 & 54 & 50 & 22 & 6 \\
0 & 10 & 6 & 16 & 14 & 26 & 23 & 29 & 33 & 42 & 1 & 3 & 36 & 2 & 11 & 8 & 12 & 5 & 4 & 35 \\
0 & 11 & 18 & 6 & 23 & 9 & 8 & 28 & 2 & 26 & 3 & 1 & 39 & 22 & 25 & 14 & 51 & 40 & 55 & 15 \\
0 & 12 & 20 & 23 & 19 & 4 & 13 & 32 & 9 & 5 & 36 & 39 & 1 & 3 & 54 & 60 & 28 & 22 & 2 & 58 \\
0 & 13 & 8 & 20 & 26 & 32 & 4 & 25 & 40 & 35 & 2 & 22 & 3 & 1 & 57 & 45 & 6 & 41 & 17 & 66 \\
0 & 14 & 23 & 28 & 8 & 34 & 29 & 3 & 16 & 33 & 11 & 25 & 54 & 57 & 1 & 6 & 13 & 36 & 64 & 2 \\
0 & 15 & 9 & 24 & 29 & 42 & 36 & 13 & 34 & 4 & 8 & 14 & 60 & 45 & 6 & 1 & 49 & 2 & 57 & 80 \\
0 & 16 & 26 & 10 & 24 & 40 & 38 & 45 & 5 & 54 & 12 & 51 & 28 & 6 & 13 & 49 & 1 & 74 & 69 & 9 \\
0 & 17 & 28 & 34 & 10 & 7 & 26 & 42 & 11 & 50 & 5 & 40 & 22 & 41 & 36 & 2 & 74 & 6 & 68 & 18 \\
0 & 18 & 11 & 30 & 27 & 15 & 45 & 6 & 44 & 22 & 4 & 55 & 2 & 17 & 64 & 57 & 69 & 68 & 1 & 95 \\
0 & 19 & 31 & 12 & 38 & 8 & 44 & 24 & 49 & 6 & 35 & 15 & 58 & 66 & 2 & 80 & 9 & 18 & 95 & 1
\end{pmatrix}$$

Nótese que la tercera fila corresponde a la sucesión A002251 en la enciclopedia online de sucesiones enteras de Sloane ([**60**]), y que sumando 1 a todos sus términos se obtiene la sucesión A019444 de la misma enciclopedia online.

Ahora daremos, de manera similar, una construcción de una cuasi matriz de diferencias cíclica infinita.

Algoritmo 2

Entrada: $n, m \in \mathbb{N}$

Salida: $Q^{[m,n]} \in M_{m\times n}(\mathbb{Z})$

Para $i \in \{0, \ldots, m\}$ hacer lo siguiente

  Para $j \in \{1, \ldots, n\}$ hacer lo siguiente

    Si $j = i + 1$ entonces

      $q_{i,j}^{[m,n]} = -$

    En caso contrario

      $D = \{q_{i,k}^{[m,n]} + q_{l,j}^{[m,n]} - q_{l,k}^{[m,n]} \mid 0 \leq l < i, 1 \leq k < j, k \neq i + 1, j \neq l + 1, k \neq l + 1\}$

      $q_{i,j}^{[m,n]} = \text{mín}\{\mathbb{Z}^+ - D\}$

    Terminar condicional.

Eliminar la fila correspondiente a $i = 0$

CONJETURA 7.7. *Si* $m \in \mathbb{N}$*, entonces* $Q^{[m]} = \sum_{n\in\mathbb{N}} Q^{[m,n]}$ *es una* $MCDCI(m)$.

De nuevo, en el caso en que esta conjetura fuera cierta, se tiene el siguiente corolario

COROLARIO 7.8. $Q = \sum_{m\in\mathbb{N}} Q^{[m]}$ *es una* $MCDCI(\infty)$.

Agregando la fila correspondiente a $i = 0$ para mantener la simetría, tenemos la siguiente matriz de orden 20 obtenida con el Algoritmo 2:

$$\begin{pmatrix}
- & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & - & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 \\
0 & 0 & - & 2 & 1 & 5 & 7 & 3 & 10 & 4 & 13 & 15 & 6 & 18 & 20 & 8 & 23 & 9 & 26 & 28 \\
0 & 1 & 2 & - & 0 & 7 & 3 & 6 & 14 & 10 & 4 & 20 & 15 & 5 & 9 & 19 & 21 & 24 & 8 & 12 \\
0 & 2 & 1 & 0 & - & 9 & 6 & 10 & 3 & 5 & 16 & 4 & 20 & 14 & 25 & 17 & 7 & 30 & 23 & 8 \\
0 & 3 & 5 & 7 & 9 & - & 0 & 2 & 1 & 8 & 11 & 21 & 19 & 4 & 14 & 27 & 12 & 6 & 35 & 30 \\
0 & 4 & 7 & 3 & 6 & 0 & - & 14 & 12 & 1 & 21 & 2 & 5 & 9 & 8 & 30 & 33 & 37 & 15 & 22 \\
0 & 5 & 3 & 6 & 10 & 2 & 14 & - & 4 & 16 & 0 & 11 & 24 & 8 & 1 & 7 & 38 & 22 & 28 & 36 \\
0 & 6 & 10 & 14 & 3 & 1 & 12 & 4 & - & 21 & 17 & 0 & 27 & 26 & 15 & 2 & 9 & 41 & 44 & 11 \\
0 & 7 & 4 & 10 & 5 & 8 & 1 & 16 & 21 & - & 3 & 29 & 31 & 2 & 0 & 36 & 46 & 11 & 50 & 6 \\
0 & 8 & 13 & 4 & 16 & 11 & 21 & 0 & 17 & 3 & - & 1 & 38 & 30 & 36 & 18 & 26 & 2 & 6 & 48 \\
0 & 9 & 15 & 20 & 4 & 21 & 2 & 11 & 0 & 29 & 1 & - & 7 & 23 & 3 & 42 & 55 & 40 & 39 & 13 \\
0 & 10 & 6 & 15 & 20 & 19 & 5 & 24 & 27 & 31 & 38 & 7 & - & 0 & 17 & 1 & 18 & 55 & 11 & 2 \\
0 & 11 & 18 & 5 & 14 & 4 & 9 & 8 & 26 & 2 & 30 & 23 & 0 & - & 40 & 43 & 1 & 57 & 62 & 60 \\
0 & 12 & 20 & 9 & 25 & 14 & 8 & 1 & 15 & 0 & 36 & 3 & 17 & 40 & - & 11 & 54 & 28 & 52 & 63 \\
0 & 13 & 8 & 19 & 17 & 27 & 30 & 7 & 2 & 36 & 18 & 42 & 1 & 43 & 11 & - & 66 & 5 & 0 & 3 \\
0 & 14 & 23 & 21 & 7 & 12 & 33 & 38 & 9 & 46 & 26 & 55 & 18 & 1 & 54 & 66 & - & 0 & 41 & 31 \\
0 & 15 & 9 & 24 & 30 & 6 & 37 & 22 & 41 & 11 & 2 & 40 & 55 & 57 & 28 & 5 & 0 & - & 12 & 27 \\
0 & 16 & 26 & 8 & 23 & 35 & 15 & 28 & 44 & 50 & 6 & 39 & 11 & 62 & 52 & 0 & 41 & 12 & - & 77 \\
0 & 17 & 28 & 12 & 8 & 30 & 22 & 36 & 11 & 6 & 48 & 13 & 2 & 60 & 63 & 3 & 31 & 27 & 77 & -
\end{pmatrix}$$

Nótese que la parte de la tercera fila que omite el primer 0 y el símbolo $-$ es la sucesión A002251 en [**60**].

Vamos a analizar el caso $m = 2$. En la siguiente proposición, $\lfloor\ \rfloor$ denota la parte entera.

PROPOSICIÓN 7.9. *$Q^{[2]}$ es una $MDCI(2)$.*

DEMOSTRACIÓN. Sea $Q^{[2]} = Q^{[2]}_{i,j}$. Es obvio que $Q^{[2]}_{0,j} = 0\ \forall j \in \mathbb{Z}^+$ y que $Q^{[2]}_{1,j} = j\ \forall j \in \mathbb{Z}^+$. Probaremos que, si $j \in \mathbb{Z}^+$, entonces

$$Q^{[2]}_{2,j} = \begin{cases} 0, & \textbf{si} \quad n = 0 \\ \lfloor \varphi n \rfloor + 1, & \textbf{si} \quad n \in A \\ \lfloor (\varphi - 1)n \rfloor, & \textbf{si} \quad n \in B \end{cases} \tag{7.1}$$

donde $\varphi = \frac{1+\sqrt{5}}{2}$ es la proporción áurea, $A = \{1, 3, 4, 6, 8, 9, \cdots\} = \{\lfloor \varphi n \rfloor \ : \ n \in \mathbb{N}\}$ es el conjunto correspondiente a la secuencia de Wythoff inferior, y $B = \{2, 5, 7, 10, 13, 15, \cdots\} = \{\lfloor \varphi^2 n \rfloor \ : \ n \in \mathbb{N}\}$ es el conjunto correspondiente a la secuencia superior de Wythoff. La igualdad (7.1) es una consecuencia directa del hecho de que tanto la sucesión $Q^{[2]}_{2,j} + 1$ como la sucesión $a_j + 1$, donde a_j es el número en el lado derecho en (7.1) satisface la recurrencia establecida en [**112**] para la sucesión que estamos estudiando.

La identidad

$$\lfloor \varphi \lfloor \varphi k \rfloor \rfloor + 1 - \lfloor \varphi k \rfloor = k \ \forall k \in \mathbb{N} \tag{7.2}$$

se puede deducir del caso $j = 0$ en el Corolario 2 en ([**44**]) (de hecho, el corolario mencionado se establece para $j \in \mathbb{N}$, pero la demostración se puede adaptar para cubrir también el caso $j = 0$).

De manera similar, es fácil probar la siguiente identidad:

$$\lfloor (\varphi - 1) \lfloor \varphi^2 k \rfloor \rfloor - \lfloor \varphi^2 k \rfloor = -k \ \forall k \in \mathbb{N} \tag{7.3}$$

Así, el resultado se cumple de (7.2) y (7.3). ■

Conjeturamos que las filas de la matriz Q descrita en el Corolario 7.6 se distribuyen asintóticamente cerca de un conjunto finito de filas. Consideraremos también las filas 0-ésimas con todas sus entradas 0 que se omitieron en la salida del algoritmo 1.

Mostraremos los gráficos de las primeras cinco sucesiones, lo que da soporte numérico a la conjetura, en la que el número de líneas es 1, 1, 2, 3, 5, 8:

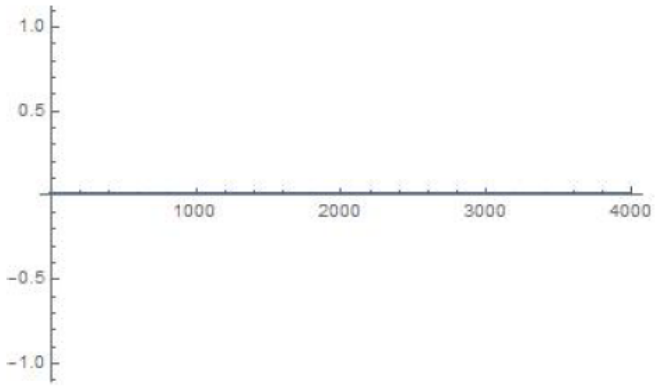

FIGURA 7.1. Fila 0

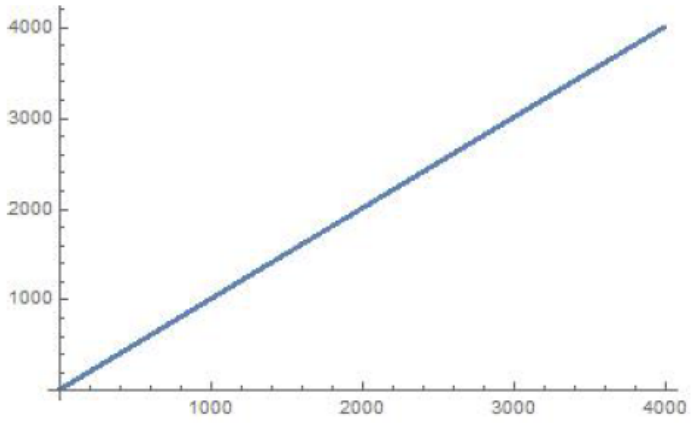

FIGURA 7.2. Fila 1

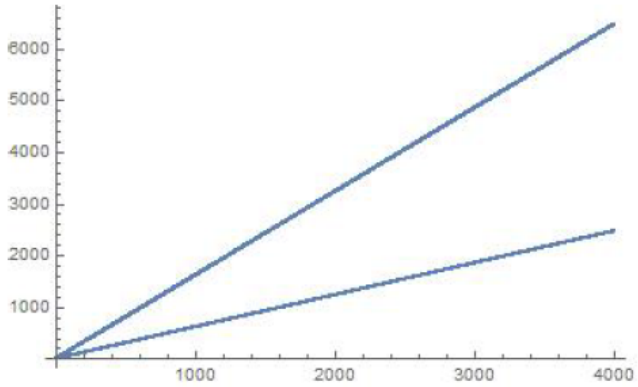

FIGURA 7.3. Fila 2

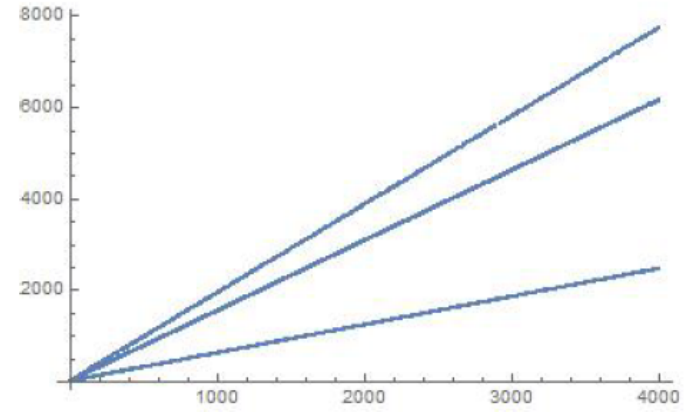

FIGURA 7.4. Fila 3

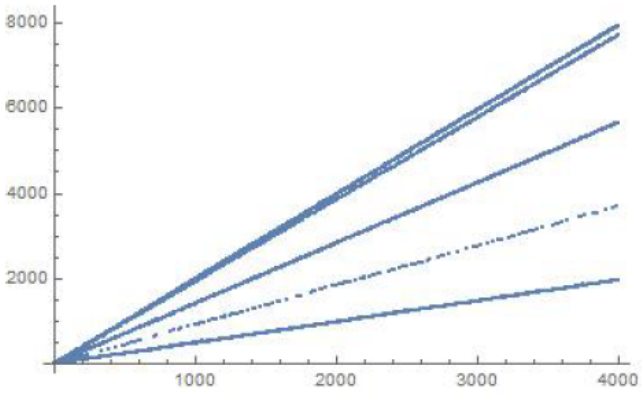

FIGURA 7.5. Fila 4

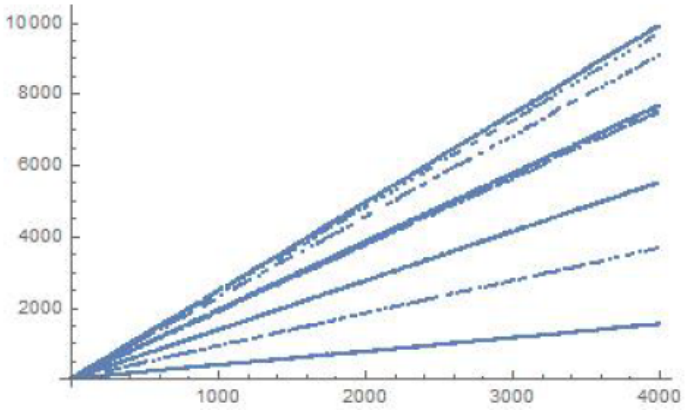

FIGURA 7.6. Fila 5

LISTA DE FIGURAS

LISTA DE TABLAS

BIBLIOGRAFÍA

[1] Abel, R. J. R. (2008). Some V (12, t) vectors and designs from difference and quasi-difference matrices. AUSTRALASIAN JOURNAL OF COMBINATORICS, 40, 69.

[2] Araluze, A., Kovács, I., Kutnar, K., Martínez, L., & Marušič, D. (2012). Partial sum quadruples and bi-Abelian digraphs. Journal of Combinatorial Theory, Series A, 119(8), 1811-1831.

[3] Araluze, A., Kutnar, K., Martínez, L., & Marušič, D. (2011). Edge connectivity in difference graphs and some new constructions of partial sum families. European Journal of Combinatorics, 32(3), 352-360.

[4] ARINA. Computational cluster from IZO-SGI, SGIker, UPV/EHU. 2021, http://www.ehu.eus/sgi/recursos/cluster-arina.

[5] Bernasconi, A., Codenottl, B., & Vanderkam, J. M. (2001). A characterization of bent functions in terms of strongly regular graphs. IEEE Transactions on Computers, 50(9), 984-985.

[6] Bernoulli, J. (1713). Ars conjectandi, opus posthumum: accedit tractatus de seriebus infinitis, et epistola Gallice scripta de ludo pilæ reticularis. Impensis Thurnisiorum Fratrum.

[7] Bose, R. C. (1963). Strongly regular graphs, partial geometries and partially balanced designs.

[8] Bose, R. C., & Bush, K. A. (1952). Orthogonal arrays of strength two and three. The Annals of Mathematical Statistics, 508-524.

[9] Bose, R. C., & Shrikhande, S. S. (1959). On the falsity of Euler's conjecture about the non-existence of two orthogonal Latin squares of order 4t+ 2. Proceedings of the National Academy of Sciences, 45(5), 734-737.

[10] Bose, R. C., Shrikhande, S. S., & Parker, E. T. (1960). Further results on the construction of mutually orthogonal Latin squares and the falsity of Euler's conjecture. Canadian Journal of Mathematics, 12, 189-203.

[11] Brouwer, A. E., & Haemers, W. H. (2011). Spectra of graphs. Springer Science & Business Media.

[12] Bruck, R. H., & Ryser, H. J. (1949). The nonexistence of certain finite projective planes. Canadian Journal of Mathematics, 1(1), 88-93.

[13] Bulutoglu, D. A., & Margot, F. (2008). Classification of orthogonal arrays by integer programming. Journal of Statistical Planning and Inference, 138(3), 654-666.

[14] Buratti, M. (1999). Old and new designs via difference multisets and strong difference families. Journal of Combinatorial Designs, 7(6), 406-425.

[15] Cammann, S. (1960). The evolution of magic squares in China. Journal of the American Oriental Society, 80(2), 116-124.

[16] Carlini, E., & Pistone, G. (2007). Hilbert bases for orthogonal arrays. Journal of Statistical Theory and practice, 1, 299-309.

[17] Cayley, P. (1879, April). On the colouring of maps. In Proceedings of the Royal Geographical Society and monthly record of geography (Vol. 1, No. 4, pp. 259-261). Blackwell Publishing; The Royal Geographical Society (with the Institute of British Geographers).

[18] Chowla, S., & Ryser, H. J. (1950). Combinatorial problems. Canadian Journal of Mathematics, 2, 93-99.

[19] Colbourn, C. J. (2010). CRC handbook of combinatorial designs. CRC press.

[20] Davis, J. A., Martínez, L., & Sodupe, M. J. (2016). Bi-Cayley normal uniform multiplicative designs. Discrete Mathematics, 339(9), 2224-2230.

[21] De Morgan, A. (1860). Review of the philosophy of discovery. The Athenaeum, 1694, 501-503.

[22] De Resmini, M. J., & Jungnickel, D. (1992). Strongly regular semi-Cayley graphs. Journal of Algebraic Combinatorics, 1, 171-195.

[23] Dean, A., & Voss, D. (Eds.). (1999). Design and analysis of experiments. New York, NY: Springer New York..

[24] Dey, A., & Mukerjee, R. (2009). Fractional factorial plans (Vol. 496). John Wiley & Sons.

[25] Dukanovic, I., & Rendl, F. (2007). Semidefinite programming relaxations for graph coloring and maximal clique problems. Mathematical Programming, 109(2), 345-365.

[26] Duval, A. M. (1988). A directed graph version of strongly regular graphs. Journal of Combinatorial Theory, Series A, 47(1), 71-100.

[27] Duval, A. M., & Iourinski, D. (2003). Semidirect product constructions of directed strongly regular graphs. Journal of Combinatorial Theory, Series A, 104(1), 157-167.

[28] Dvivedi, S., Prakash, S., & Sharma, R. S. (1966). Brahmasphutasiddhantah. 1966.

[29] Euler, L. (1766). Solution d'une question curieuse que ne paroit soumise à aucune analyse. Mémoires de l'académie des sciences de Berlin, 310-337.

[30] Euler, L. (1741). Solutio problematis ad geometriam situs pertinentis. Commentarii academiae scientiarum Petropolitanae, 128-140.

[31] Euler, L. (1782). Recherches sur une nouvelles espèce de quarrés magiques. Verhandelingen uitgegeven door het zeeuwsch Genootschap der Wetenschappen te Vlissingen 9. 85–239 = Opera Omnia: Ser. 1, Vol. 7, pp. 291–392. Translation by Andie Ho and Dominic Klyve: http://eulerarchive.maa.org/docs/translations/E530.pdf

[32] Fernández-Alcober, G. A., Kwashira, R., & Martínez, L. (2010). Cyclotomy over products of finite fields and combinatorial applications. European Journal of Combinatorics, 31(6), 1520-1538.

[33] Fiedler, F., Klin, M., & Muzychuk, M. H. (2002). Small vertex-transitive directed strongly regular graphs. Discrete mathematics, 255(1-3), 87-115.

[34] Franco, J., Dupuy, D., Roustant, O., Kiener, P., Damblin, G., Iooss, B., & Helbert, M. C. (2015). Package 'DiceDesign'.

[35] Franklin, P. (1922). The four color problem. American Journal of Mathematics, 44(3), 225-236.

[36] Gadelha Filho, T., Silvia, C., Aleksandar, D., Massimo, B., & Marco, M. (2021). Rural electrification planning based on graph theory and geospatial data: A realistic topology oriented approach. Sustainable Energy, Grids and Networks, 28, 100525.

[37] Gallager, R. G. (1968). Information theory and reliable communication (Vol. 588). New York: Wiley.

[38] García, M. A., Kutnar, K., Malnič, A., Martínez, L., Marušič, D., & Montoya, J. M. (2019). Construction of infinite families of vertex-transitive directed strongly regular graphs. Acta Mathematica Universitatis Comenianae, 88(2), 319-327.

[39] Ge, G. (2005). On (g, 4; 1)-difference matrices. Discrete mathematics, 301(2-3), 164-174.

[40] Godsil, C., & Royle, G. (2001). Algebraic graph theory (Vol. 207). Springer.

[41] Graham, R.L., Grötschel, M., & Lovász, L. (1995). Handbook of Combinatorics (Vol. 1). Elsevier.

[42] Green, P. E., & Srinivasan, V. (1990). Conjoint analysis in marketing: New developments with implications for research and practice. Journal of Marketing, 54(4), 3-19.

[43] Greenaway, K. H., Wright, R. G., Willingham, J., Reynolds, K. J., & Haslam, S. A. (2015). Shared identity is key to effective communication. Personality and Social Psychology Bulletin, 41(2), 171-182.

[44] Griffiths, M. (2015). On a Matrix Arising from a Family of Iterated Self-Compositions. J. Integer Seq., 18(11), 15-11.

[45] Grömping, U. (2018). R package DoE. base for factorial experiments. Journal of Statistical Software, 85, 1-41.

[46] Gyürki, Š. (2016). Infinite families of directed strongly regular graphs using equitable partitions. Discrete Mathematics, 339(12), 2970-2986.

[47] Gyürki, Š., & Klin, M. (2014, September). Sporadic examples of directed strongly regular graphs obtained by computer algebra experimentation. In International Workshop on Computer Algebra in Scientific Computing (pp. 155-170). Cham: Springer International Publishing.

[48] Haemers, W. H., Peeters, R., & Van Rijckevorsel, J. M. (1999). Binary codes of strongly regular graphs. Designs, Codes and Cryptography, 17(1-3), 187-209.

[49] Hainmueller, J., Hopkins, D. J., & Yamamoto, T. (2014). Causal inference in conjoint analysis: Understanding multidimensional choices via stated preference experiments. Political Analysis, 22(1), 1-30.

[50] Hall, M. (1998). Combinatorial theory (Vol. 71). John Wiley & Sons.

[51] Hayashi, T. (2008). Combinatorics in Indian Mathematics. Encyclopaedia of the History of Science, Technology and Medecine in Non-Western Cultures.

[52] Heawood, P. J. (1890). Map colour theorem', Quart. d. J. Math.

[53] Hedayat, A. S., Sloane, N. J. A., & Stufken, J. (2012). Orthogonal arrays: theory and applications. Springer Science & Business Media.

[54] Heesch, H. (1969). Untersuchungen zum Vierfarbenproblem. B. I. Hochschulscripten, 810/810a/810b.

[55] Hickernell, F. (1998). A generalized discrepancy and quadrature error bound. Mathematics of computation, 67(221), 299-322.

[56] Higman, D. G., & Sims, C. C. (1968). A simple group of order 44,352,000.

[57] Hobart, S. A., & Justin Shaw, T. (1999). A note on a family of directed strongly regular graphs. European Journal of Combinatorics, 20(8), 819-820.

[58] Holton, D. A., & Sheehan, J. (1993). The petersen graph (Vol. 7). Cambridge University Press.

[59] https://commons.wikimedia.org/wiki/Main_Page

[60] https://oeis.org/

[61] https://www.gap-system.org/

[62] Hujdurović, A. (2013). Quasi m-Cayley circulants. Ars mathematica contemporanea, 6(1), 147-154.

[63] IBM ILOG Cplex. V12. 1: User's manual for CPLEX. Int Bus Mach Corp 2009;46(53):157.

[64] Jaenisch, C. F. (1862). Traité des applications de l'analyse mathématique au jeu des échecs: précédé d'une introduction à l'usage des lecteurs soit étrangers aux échecs, soit peu versés dans l'analyse (Vol. 1). Londres.

[65] Jørgensen, L. K. (2001). Directed strongly regular graphs with $\mu = \lambda$. Discrete Mathematics, 231(1-3), 289-293.

[66] Jørgensen, L. K. (2003). Non-existence of directed strongly regular graphs. Discrete Mathematics, 264(1-3), 111-126.

[67] Jørgensen, L. K. (2005). Rank of adjacency matrices of directed (strongly) regular graphs. Linear algebra and its applications, 407, 233-241.

[68] Jungnickel, D. (1979). On difference matrices, resolvable transversal designs and generalized Hadamard matrices. Mathematische Zeitschrift, 167(1), 49-60.

[69] Kan, X., Thayer, T. C., Carpin, S., & Karydis, K. (2021). Task planning on stochastic aisle graphs for precision agriculture. IEEE Robotics and Automation Letters, 6(2), 3287-3294.

[70] Ke, X., Zhang, R., & Ye, H. J. (2015). Two-and three-level lower bounds for mixture L2-discrepancy and construction of uniform designs by threshold accepting. Journal of Complexity, 31(5), 741-753.

[71] Kempe, A. B. (1879). On the geographical problem of the four colours. American journal of mathematics, 2(3), 193-200.

[72] Kenny, Y. The Uniform Design. 2004-10-14 [2019-12-10]. http://www. math. hkbu. edu. hk/UniformDesign.

[73] Klin, M., Munemasa, A., Muzychuk, M., & Zieschang, P. H. (2004). Directed strongly regular graphs obtained from coherent algebras. Linear algebra and its applications, 377, 83-109.

[74] Knuth, D. E. (1978). The art of computer programming. Vol. 1: Fundamental algorithms. Reading.

[75] Kovács, I., Kuzman, B., Malnič, A., & Wilson, S. (2012). Characterization of edge-transitive 4-valent bicirculants. Journal of Graph Theory, 69(4), 441-463.

[76] Kutnar, K., Malnic, A., Martinez, L., & Marusic, D. (2013). Quasi m-Cayley strongly regular graphs. Journal of the Korean Mathematical Society, 50(6), 1199-1211.

[77] Kutnar, K., Marušič, D., Miklavič, Š., & Šparl, P. (2009). Strongly regular tri-Cayley graphs. European Journal of Combinatorics, 30(4), 822-832.

[78] Lam, C. W., Thiel, L., & Swiercz, S. (1989). The non-existence of finite projective planes of order 10. Canadian journal of mathematics, 41(6), 1117-1123.

[79] Leung, K. H., & Ma, S. L. (1993). Partial difference triples. Journal of Algebraic Combinatorics, 2, 397-409.

[80] Lin, Y. L., Phoa, F. K. H., & Kao, M. H. (2017). Optimal design of fMRI experiments using circulant (almost-) orthogonal arrays.

[81] Ma, C. X., Fang, K. T., & Liski, E. (2000). A new approach in constructing orthogonal and nearly orthogonal arrays. Metrika, 50, 255-268.

[82] Ma, S. L. (1984). Partial difference sets. Discrete Mathematics, 52(1), 75-89.

[83] Macdonald, D. B. (1912). Description of a silver amulet. Zeitschrift für Assyriologie und Vorderasiatische Archäologie, 26(1-3), 267-269.

[84] Margot, F. (2002). Pruning by isomorphism in branch-and-cut. Mathematical Programming, 94, 71-90.

[85] Margot, F. (2003). Exploiting orbits in symmetric ILP. Mathematical Programming, 98, 3-21.

[86] Margot, F. (2003). Small covering designs by branch-and-cut. Mathematical Programming, 94, 207-220.

[87] Margot, F. (2007). Symmetric ILP: Coloring and small integers. Discrete Optimization, 4(1), 40-62.

[88] Martínez, L. (2014). Strongly regular m-Cayley circulant graphs and digraphs. ARS MATHEMATICA CONTEMPORANEA, 8(1).

[89] Martínez, L., & Araluze, A. (2010). New tools for the construction of directed strongly regular graphs: Difference digraphs and partial sum families. Journal of Combinatorial Theory, Series B, 100(6), 720-728.

[90] Martínez, L., Merino, M., & Montoya, J. M. (2023). An integer programming model for obtaining cyclic quasi-difference matrices. Operations Research Perspectives, 10, 100260.

[91] Marušič, D. (1987). Strongly regular bicirculants and tricirculants.

[92] McKay, B. D. (2013). A Note on the History of the Four-Colour Conjecture. Journal of Graph Theory, 72(3), 361-363.

[93] Michel, J. (2017). A note on directed strongly regular graphs. Graphs and Combinatorics, 33, 171-179.

[94] Mohr, D. C., Cuijpers, P., & Lehman, K. (2011). Supportive accountability: A model for providing human support to enhance adherence to eHealth interventions. Journal of Medical Internet Research, 13(1), e30.

[95] Nie, C., & Leung, H. (2011). A survey of combinatorial testing. ACM Computing Surveys (CSUR), 43(2), 1-29.

[96] Parker, E. T. (1959). Construction of some sets of mutually orthogonal Latin squares. Proceedings of the American Mathematical Society, 10(6), 946-949.

[97] Parker, E. T. (1959). Orthogonal latin squares. Proceedings of the National Academy of Sciences, 45(6), 859-862.

[98] Péteri, R., & Ranchin, T. (2003, June). Multiresolution snakes for urban road extraction from ikonos and quickbird images. In 23nd EARSeL Annual Symposium" Remote Sensing in Transition (pp. 141-147). Ghent, Belgium.

[99] Plackett, R. L., & Burman, J. P. (1946). The design of optimum multifactorial experiments. Biometrika, 33(4), 305-325.

[100] Poinsot, L. (1809). Sur les polygones et les polyèdres, J. Ecole Polytech. 4 (Cah. 10) 16–48.

[101] R Core Team, R. (2013). R: A language and environment for statistical computing.

[102] Rao, C. R. (1947). Factorial experiments derivable from combinatorial arrangements of arrays. Supplement to the Journal of the Royal Statistical Society, 9(1), 128-139.

[103] Reiss, M. (1871). Evaluation du nombre de combinaisons desquelles les 28 dés d'un jeu du domino sont susceptibles d'après la règle de ce jeu. Annali di Matematica Pura ed Applicata (1867-1897), 5, 63-120.

[104] Robertson, N., Sanders, D., Seymour, P., Thomas, R. (1997). The four-colour theorem. journal of combinatorial theory, Series B, 70(1), 2-44.

[105] Seeger, A., & Torki, M. (2014). Centers of sets with symmetry or cyclicity properties. Top, 22(2), 716-738.

[106] Storer, T. (1967). Cyclotomy and difference sets. Lectures in Advanced Mathematics.

[107] Tarry, G. (1900). Le problème des 36 officiers. Secrétariat de l'Association française pour l'avancement des sciences.

[108] The Sage Developers, Stein William, Joyner David, Kohel David, Cremona John, Eröcal Burçin. SageMath, version 9.0. 2020, http://www.sagemath.org.

[109] Thomas, R. (1998). An update on the four-color theorem. Notices of the AMS, 45(7), 848-859.

[110] Vandermonde, A. T. (1771). Remarques sur les problèmes de situation. Mémoires de l'Académie Royale des Sciences (Paris), 2, 566-574.

[111] Veblen, O., & Bussey, W. H. (1906). Finite projective geometries. Transactions of the American mathematical society, 7(2), 241-259.

[112] Venkatachala, B. J. (2009). A Curious Bijection on Natural Numbers. Journal of Integer Sequences, 12(2), 3.

[113] Vieira Jr, H., Sanchez, S., Kienitz, K. H., & Belderrain, M. C. N. (2011). Generating and improving orthogonal designs by using mixed integer programming. European Journal of Operational Research, 215(3), 629-638.

[114] Wang, K., & Chen, K. (2018). A short disproof of Euler's conjecture based on quasi-difference matrices and difference matrices. Discrete Mathematics, 341(4), 1114-1119.

[115] Whitney, H. (1932). The coloring of graphs. Annals of Mathematics, 688-718.

[116] Wilson, R. M. (1972). Cyclotomy and difference families in elementary abelian groups. Journal of Number Theory, 4(1), 17-47.

[117] Wilson, R., & Nash, C. (2003). Four colours suffice: How the map problem was solved. The Mathematical Intelligencer, 25(4), 80-83.

[118] Wilson, R., & Watkins, J. J. (Eds.). (2013). Combinatorics: ancient & modern. OUP Oxford.

[119] Wu, C. F. J., & Hamada, M. (2011). Experiments: Planning, analysis, and parameter design optimization (2a ed.). Wiley.

[120] Zhou, Y. D., Fang, K. T., & Ning, J. H. (2013). Mixture discrepancy for quasi-random point sets. Journal of Complexity, 29(3-4), 283-301.