UNIVERSIDAD AUTÓNOMA METROPOLITANA

Casa abierta al tiempo

Unidad Iztapalapa

Propiedades y Aplicaciones de los Cuadrados Latinos

T E S I S

QUE, PARA OBTENER EL GRADO ACADÉMICO DE:

Maestro en Ciencias

Matemáticas Aplicadas e Industriales

P R E S E N T A:

Mat. Celia Ivonne Cortés Pérez

Director de Tesis: Dr. Joaquín Tey Carrera

Iztapalapa, D.F., a 26 de Octubre de 2011

1960 ROMA OLİMPİYATLARI

IMPRESSION COURVOISIER S.A., LA CHAUX-DE-FONDS (SUISSE)

Índice general

Introducción

Los cuadrados latinos han sido estudiados durante siglos. Sin embargo, fue en 1779 cuando Leonhard Euler los definió formalmente en su manuscrito *Recherches sur une nouvelle espece de quarre magique* (Investigaciones de una Nueva Especie de Cuadrados Mágicos) (ver [16]). Euler utilizó letras del latín como elementos de tales cuadrados, llamándolos cuadrados latinos. Él estaba interesado en la solución del Problema de los 36 oficiales que será examinado con detalle en la sección 1.6.1.

Este trabajo se divide en dos capítulos. En el capítulo 1 presentamos conceptos y propiedades básicas de los cuadrados latinos, destacando el concepto de ortogonalidad y el capítulo 2 está dedicado especialmente a la aplicación de los cuadrados latinos en diversas áreas de las matemáticas.

Hasta el momento no se conoce el número exacto de cuadrados latinos de orden $n > 10$. Sin embargo, se han dado distintas cotas a este número. En la sección 1.1 desarrollamos a detalle algunas de estas cotas, por mencionar alguna, la cota superior dada por Ronald Alter en 1975.

El problema de determinar el número máximo de cuadrados latinos de orden n mutuamente ortogonales ($MOLS$) es extraordinariamente difícil de resolver. Para ver esto, en la sección 1.3 se muestra la equivalencia que existe entre la existencia de $n-1$ $MOLS$ de orden n y un plano proyectivo de orden n. Solo se conocen planos proyectivos de orden la potencia de un primo, a pesar de los grandes esfuerzos realizados durante muchos años por una larga lista de matemáticos. No es difícil aceptar que este problema fuera denominado por Mullen en 1995 el "Nuevo problema de Fermat".

En las secciones 1.4, 1.5 y 1.6 se desarrollan las herramientas que utilizaron Bose, Parker y Shrikhande en 1960 para contradecir la conjetura hecha por Euler en 1782 que afirmaba que no existen dos $MOLS$ de orden n para $n \equiv 2 \pmod 4$. Estas herramientas son: los cuadrados latinos auto-ortogonales ($SOLS$) donde además, mostramos su uso en la construcción de los Torneos Dobles Mixtos; los arreglos ortogonales, que son una alternativa de representar a un conjunto de $MOLS$ y los diseños balanceados. Por último, en la sección 1.6.1 se muestra la prueba dada por Stinson en 1984 que nos muestra de manera particular la no existencia de dos $MOLS$ de orden 6.

Los juegos matemáticos en años recientes han ganado gran popularidad como pasatiempo, entre ellos tenemos a los cuadrados mágicos que durante la Edad Media se grababan en láminas de plata como amuletos contra la peste negra. Los astrólogos los aconsejaban como amuletos protectores,

precisamente, contra la melancolía. En la sección 2.1 desarrollamos el método para construir estos cuadrados mediante el uso de los cuadrados latinos dado por Euler. Un juego de gran popularidad en el siglo XX es el Sudoku, la relación que existe entre este juego y los cuadrados latinos es que la solución de un Sudoku es, precisamente, un cuadrado latino que llamaremos cuadrado latino Sudoku, la sección 2.2 esta dedicada al estudio de la propiedad de ortogonalidad y construcción de conjuntos ortogonales de dichos cuadrados. Además, en la sección 2.3.3 desarrollamos las cotas superior e inferior para el número de cuadrados latinos Sudoku dadas por Agnes M. Herzberg y M. Ram Murty en el 2007.

En la sección 2.3 presentamos la equivalencia de los cuadrados latinos de orden n con 1-factorizaciones de familias especiales de gráficas, como son: la gráfica bipartita completa ($\mathbb{K}_{n,n}$), la gráfica completa dirigida sin lazos ($\overrightarrow{\mathbb{K}_n}$) y la gráfica completa ($\mathbb{K}_n$). En el caso de $\overrightarrow{\mathbb{K}_n}$, el número de 1-factorizaciones de este tipo de gráficas esta muy relacionado con el número de cuadrados latinos de orden n. En 1847, Kirkman establece la existencia de un Sistema de Ternas de Steiner de orden $n \equiv 1, 3 \bmod 6$, $n \geq 3$, en la sección 2.4 presentamos los métodos de Bose y Skolem que hacen uso de los cuadrados latinos simétricos e idempotentes y los simétricos y semi-idempontes en la construcción de tales sistemas.

En Matemáticas, Computación y Teoría de la Información, la detección y corrección de errores es una importante práctica para el mantenimiento e integridad de los datos a través de canales ruidosos y medios de almacenamiento poco confiables. Uno de los principales problemas dentro de la Teoría de códigos es encontrar códigos de gran tamaño, donde la longitud de las palabras esta dada al igual que la distancia mínima entre ellas, en la sección 2.5 haremos uso de los cuadrados latinos ortogonales para la construcción de algunos de estos códigos.

La criptografía (escritura oculta) como concepto, son las técnicas utilizadas para cifrar y descifrar información utilizando técnicas matemáticas que hagan posible el intercambio de mensajes de manera que sólo puedan ser leídos por las personas a quienes van dirigidos, en la sección 2.6.2 presentamos el uso de los cuasigrupos en la codificación de datos. La relación que existe entre los cuasigrupos y los cuadrados latinos es que la tabla de Cayley asociada a un cuasigrupo es un cuadrado latino.

La integridad de un sistema de información consiste en exigir que determinadas operaciones sólo puedan ser llevadas acabo por una o mas personas que tienen derechos de acceso. El acceso a este sistema es a menudo adquirida a través de una clave, cuyo uso se rige por un sistema de generación de claves. En la sección 2.7 describimos un esquema de secreto compartido construido mediante el uso de los cuadrados latinos parciales que es precisamente un generador de claves.

Dentro de un conjunto de cuadrados latinos de orden n, el Isotopismo es una relación de equivalencia cuyas clases laterales son llamadas clases Isotópicas, los cuadrados latinos pertenecientes a la misma clase son llamados isotópicos. En la sección 2.6.3 describimos de forma breve esta relación.

Finalmente, en la sección 2.7 damos una breve introducción del uso de los cuadrados latinos en el diseño de experimentos, los cuales tienen sus orígenes en experimentos agrícolas y otras áreas como la biología, el estudio de mercados y procesos industriales, entre otros.

CAPÍTULO 1

Cuadrados Latinos

En este capítulo abordaremos los aspectos teóricos de los cuadrados latinos, describiremos propiedades básicas de los mismos, entre las que se encuentran la ortogonalidad entre ellos y algunos métodos para construirlos. Se desarrollarán algunas de las cotas inferiores y superiores para el número de cuadrados latinos distintos de orden n. Así como la prueba que contradice la conjetura de Euler y la demostración de la no existencia de dos $MOLS$ de orden 6. Las ideas desarrolladas en este capítulo están basadas en el libro Combinatorial Designs (ver [2]).

Un **cuadrado latino** es una matriz de tamaño $n \times n$ cuyos elementos pertenecen a un conjunto finito A de cardinalidad n y cada uno de ellos aparece exactamente una vez en cada renglón y en cada columna de L. A es llamado el **conjunto base** del cuadrado y n su **orden**.

Ejemplo 1.0.1. *Sea $A = \{A, B, C, D\}$. La siguiente matriz es un cuadrado latino de orden 4.*

$$\begin{pmatrix} A & B & C & D \\ D & A & B & C \\ C & D & A & B \\ B & C & D & A \end{pmatrix}$$

Teorema 1.0.1. *Existe un cuadrado latino de orden n para cualquier entero positivo n.*

Demostración. Sea $A = \{1, 2, \ldots, n\}$. Tomemos como primer renglón del cuadrado a $123 \cdots n$. Ahora a partir del segundo renglón se desplazan los elementos de la fila anterior una posición a la izquierda y el primer elemento del renglón anterior se coloca al final de la fila que se esta construyendo, es decir, el i-ésimo renglón es un desplazamiento cíclico de una posición a la izquierda del renglón $i - 1$. El cuadrado latino que construimos de esta manera es

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & & & n \\ 2 & 3 & 4 & \cdots & & n & 1 \\ 3 & 4 & 5 & \cdots & n & 1 & 2 \\ \vdots & \vdots & \vdots & & & & \vdots \\ n & 1 & 2 & \cdots & & & n-1 \end{pmatrix}.$$

□

La tabla del grupo aditivo $\mathbb{Z}/n\mathbb{Z}$ de enteros módulo n es un ejemplo del teorema.

1.1. Número de Cuadrados Latinos

El número de cuadrados latinos de orden n se ha estudiado durante mucho tiempo. En esta sección daremos algunos de los resultados obtenidos hasta el momento para este número, basándonos en [1, 7, 11, 12].

Se sabe que para $n = 2$, el número de cuadrados latinos distintos es 2, los cuales son

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

Un cuadrado latinos de orden n con conjunto base $\{0, 1, \ldots, n-1\}$ es **reducido** si los elementos de su primer renglón y su primera columna están en orden natural, es decir, $012 \ldots n-1$.

Denotaremos al número de cuadrados latinos de orden n como $L(n)$ y $l(n)$ denota el número de cuadrados latinos reducidos de orden n. Entonces, el siguiente teorema nos dice que para $n > 2$ el número de cuadrados latinos de orden n depende del número de cuadrados latinos reducidos de orden n.

Teorema 1.1.1. *Para $n \geq 2$*

$$L(n) = n!(n-1)!l(n).$$

Demostración. Dado un cuadrado latino de orden n podemos permutar las columnas del cuadrado de $n!$ formas posibles. Al permutar las columnas, el arreglo resultante sigue siendo un cuadrado latino además de ser distinto al cuadrado dado inicialmente.

Ahora los últimos $n-1$ renglones del cuadrado latino pueden permutarse de $(n-1)!$ formas posibles, de igual manera cualquier permutación de renglones nos da un cuadrado latino distinto. Lo mas importante es que estos también son distintos a los cuadrados latinos obtenidos de permutar las columnas, ya que la primer fila se mantuvo fija. Por lo tanto, a partir de un cuadrado latino reducido, las $n!$ y $(n-1)!$ permutaciones de columnas y renglones respectivamente dan como

resultado $n!(n-1)!$ cuadrados latinos distintos de orden n y exactamente uno de estos cuadrados será reducido y dado que se tienen $l(n)$ cuadrados reducidos , entonces

$$L(n) = n!(n-1)!l(n).$$

□

Hasta el momento se conoce el número exacto de cuadrados reducidos para n pequeño, así que se han dado distintas cotas para el cálculo de este número. A continuación presentamos algunas de ellas.

1.1.1. Cotas Inferiores para $L(n)$

Una primera cota inferior para el número de cuadrados latinos se construye de la siguiente forma

Dado un arreglo vacío de tamaño $n \times n$. Tenemos $n!$ maneras de llenar el primer renglón del arreglo. Ahora consideremos el segundo renglón, tenemos $n-1$ posiciones donde podemos colocar al 0. Hay $n-1$ o $n-2$ lugares donde podemos colocar al 1 dependiendo en donde se haya colocado el 0, si se colocó bajo el 1 del primer renglón o no, por lo que tenemos al menos $n-2$ lugares donde colocar el 1. De manera similar tenemos al menos $n-3$ lugares donde colocar el 2. Por lo que tenemos al menos $(n-1)!$ formas de llenar el segundo renglón. Siguiendo con un argumento similar para los renglones restantes llegamos a que

$$L(n) \geq n!(n-1)!(n-2)!\ldots 2!1!.$$

Una segunda cota inferior para el número de cuadrados latinos se construye mediante la permanente de una matriz.

Sea $A = (a_{ij})$ una matriz de tamaño $n \times n$, la **permanente** de A es

$$perA = \sum_{\sigma \in S_n} a_{1\sigma(1)} a_{2\sigma(2)} \ldots a_{n\sigma(n)}$$

donde S_n denota al grupo simétrico sobre el conjunto $\{1, 2, \ldots, n\}$. La matriz A es llamada **doblemente estocástica** si la suma de los elementos en cada renglón y cada columna es igual a 1.

En 1926 B. L. van der Waerden propuso el problema de determinar la permanente mínima entre todas la matrices doblemente estocásticas. Él conjeturó que este mínimo es alcanzado por la matriz constante en donde todas sus entradas son iguales a $\frac{1}{n}$, es decir,

$$perA \geq \frac{n!}{n^n}$$

para cualquier matriz A doblemente estocástica.

Esta conjetura fue probada en 1981 independientemente por G. P. Egorychev y D. I. Falikman (ver [13]). Este resultado se utiliza para dar una cota inferior del número de cuadrados latinos de orden n.

Un *SRD* (Sistema de Representantes Distintos) para los conjuntos $A_1, A_2, \ldots, A_n$ es una n-upla $(a_1, a_2, \ldots, a_n)$ donde $a_i \neq a_j$ para $i \neq j$ y $a_i \in A_i$ para todo $i = 1, 2, \ldots, n$.

Teorema 1.1.2. *Los conjuntos $A_1, A_2, \ldots, A_n$ tienen un SRD si y sólo si para todo $k = 1, 2, \ldots, n$ la unión de cualesquiera k conjuntos tiene al menos k elementos.*

Sean $A_1, A_2, \ldots, A_n$ subconjuntos del conjunto $\{1, 2, \ldots, n\}$. Observe que el número de maneras en que podemos elegir a un *SRD* coincide con la *permanente* de la $(0,1)$-matriz H de tamaño $n \times n$ donde la entrada (i, j) es igual a 1 si y sólo si $i \in A_j$. H es llamada **matriz de Hall** asociada a los conjuntos $A_1, A_2, \ldots, A_n$.

Dado un cuadrado latino de orden n, el número de formas distintas en que podemos llenar el primer renglón es $n!$. Supongamos que se tienen k renglones llenos del cuadrado latino. Para cada posición i del renglón $k+1$ se define a A_i como el conjunto de números que aún no se han usado en la i-ésima columna del cuadrado, de tal manera que $|A_i| = n - k$. El problema de llenar el renglón $k+1$ del cuadrado latino es equivalente a encontrar un *SRD* de los conjuntos $A_1, A_2, \ldots, A_n$. De tal manera que el número de formas distintas en que se puede llenar el renglón $k+1$ del cuadrado latino es la *permanente* de la matriz de Hall asociada a los conjuntos $A_1, A_2, \ldots, A_n$.

Sea H la matriz de Hall asociada a los conjuntos $A_1, A_2, \ldots, A_n$. Como se mencionó la entrada (i, j) de H es igual a 1 si y sólo si $i \in A_j$, sabemos que $|A_i| = n - k$ para $i = 1, 2, \ldots, n$ por lo que la matriz H tiene $n - k$ 1's en cada columna y $n - k$ 1's en cada renglón ya que a cada elemento del conjunto $\{1, 2, \ldots, n\}$ esta en $n - k$ conjuntos A_i. Entonces la matriz $\overline{H} = (n-k)^{-1}H$ es una matriz doblemente estocástica. De tal manera que

$$\begin{aligned} per\overline{H} &\geq \frac{n|!}{n^n} \\ \frac{1}{(n-k)^n} perH &\geq \frac{n!}{n^n} \\ perH &\geq \frac{(n-k)^n n!}{n^n}. \end{aligned}$$

Esto sólo es el número de formas distintas en que se puede llenar el renglón $k+1$ del cuadrado latino, entonces el número de formas distintas en que se pueden llenar los n renglones de un cuadrado

latino es

$$\begin{aligned}\prod_{k=0}^{n-1}\frac{(n-k)^n n!}{n^n} &= \frac{n^n n!}{n^n}\frac{(n-1)^n n!}{n^n}\frac{(n-2)^n n!}{n^n}\cdots\frac{1^n n!}{n^n}\\ &= \frac{n!^n n^n (n-1)^n (n-2)^n \ldots 1^n}{n^{n^2}}\\ &= \frac{n!^n (n(n-2)(n-2)\cdots 1)^n}{n^{n^2}}\\ &= \frac{n!^{2n}}{n^{n^2}}.\end{aligned}$$

Por lo tanto

$$L(n) \geq \frac{n!^{2n}}{n^{n^2}}$$

es una mejor cota inferior para el número de cuadrados latinos distintos de orden n.

Por otra parte

$$e^n = 1 + \frac{n}{1!} + \frac{n^2}{2!} + \cdots \frac{n^r}{r!} + \cdots > \frac{n^r}{r!}$$

por lo que $r! > e^{-n}n^r$, usando esta desigualdad en la primer cota inferior dada para $L(n)$ obtenemos $L(n) > \prod_{r=1}^{n} e^{-n}n^r = e^{-n^2}n^{1+2+\cdots n}$, entonces se tiene lo siguiente

$$L(n) > (e^{-2}n)^{n^2/2}$$

Ahora usando la desigualdad $n! > e^{-n}n^n$ en la segunda cota inferior dada para $L(n)$ se obtiene

$$L(n) > (e^{-2}n)^{n^2}$$

1.1.2. Cotas Superiores para $L(n)$

A continuación daremos la cota superior para el número de cuadrados latinos reducidos de orden n propuesta por Ronald Alter en 1975 (ver [14]).

Sea l la siguiente matriz con el primer renglón y primera columna llenas

$$\begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 2 & * & * & * & & * \\ 3 & * & * & * & & * \\ 4 & * & * & * & & * \\ \vdots & & & & & \vdots \\ n & * & * & * & & * \end{pmatrix}$$

Para $l(2,2)$ se tienen $n-1$ posibles valores a elegir, $l(2,3)$ tiene $n-2$ o $n-3$ posibles valores a elegir dependiendo del valor que se haya elegido para $l(2,2)$, de tal manera que $l(2,3)$ tiene a lo más

$n-2$ posibles valores a elegir. Ahora $l(2,3)$ tiene $n-3$ o $n-4$ posibles valores a elegir, entonces a lo más tiene $n-3$ posibles valores a elegir, siguiendo de forma similar podemos decir que el número de formas distintas en que se puede llenar el segundo renglón es de a lo más $(n-1)!$. $l(3,2)$ puede tomar $n-2$ o $n-3$ posibles valores dependiendo del valor que tenga $l(2,2)$, si $l(2,2)=2$ tiene $n-2$ valores a elegir y $n-3$ si no tiene, por lo que $l(3,2)$ tiene a lo más $n-2$ posibles valores a elegir. $l(3,3)$ tiene a lo más $n-2$ posibles valores. $l(3,4)$ tiene a lo más $n-3$ posibles valores a elegir y siguiendo este proceso se tiene que el número de formas distintas en que se puede llenar el tercer renglón es a lo más $(n-2)(n-2)!$. Siguiendo con un argumento similar para los demás renglones se puede concluir que

$$l(n) \leq n-1!((n-2)(n-2)!)(n-3)^2(n-3)!\cdots((n-i+1)^{i-2}(n-i+1)!)\cdots 2^{n-3}2!1^{n-2}1!$$

$$l(n) \leq \prod_{i=2}^{n}(n-i+1)^{i-2}(n-1)!(n-2)!\cdots 2!1!.$$

Por lo tanto una cota superior para el número de cuadrados latinos $LS(n)$ es

$$L(n) \leq n!(n-1)!\prod_{i=2}^{n}(n-i+1)^{i-2}(n-1)!(n-2)!\cdots 2!1!.$$

En 1967 H. Minc conjeturó que si A es una $(0,1)$-matriz, entonces

$$perA \leq \prod_{i=1}^{n} r_i!^{\frac{1}{r_i}}$$

donde r_i es la suma de los elementos del i-ésimo renglón de A.

Esta conjetura fue probada en 1973 por L. M. Brégman (ver [15]).

Ahora, tal como se hizo con la cota inferior, utilizaremos (*) para dar una cota superior para el número de cuadrados latinos.

De manera similar como se construyó la cota inferior para el número de cuadrados latinos usando la cota inferior del permanente de una matriz utilizaremos ahora la cota superior del permanente de una matriz para dar una cota superior al número de cuadrados latinos.

Sea H la $(0,1)$-matriz asociada a los conjuntos $A_1, A_2, \ldots, A_n$.

Sabemos que H tiene $n-k$ 1's en cada renglón, de tal manera que $r_i = n-k$ para todo $i = 1, 2, \ldots, n$. Por lo tanto

$$perH \leq \prod r_i!^{\frac{1}{r_i}} = \prod_{i=1}^{n}(n-k)!^{\frac{1}{n-k}}$$

entonces

$$perH \leq (n-k)!^{\frac{n}{n-k}}.$$

De tal manera que el número de formas distintas en que podemos llenar el renglón $k+1$ de un cuadrado latino es a lo más $(n-k)!^{\frac{n}{n-k}}$. Entonces

$$L(n) \leq \prod_{k=0}^{n-1} (n-k)!^{\frac{n}{n-k}}$$

es una mejor superior para el número de cuadrados latinos de orden n. $L(n)$ aumenta muy rápidamente y es realmente grande, incluso para n bastante pequeño, cabe señalar que el número de cuadrados latinos reducidos es conocido para $n \leq 10$ (McKay and Rogoyski, 1995).

n	$l(n)$
2	1
3	1
4	4
5	56
6	9048
7	16942080
8	535281401585
9	377597570964258816
10	7580721483160132811489280

las estimaciones de los cuadrados latinos reducidos de orden $n = 11, 12, 13, 14, 15$ son

n	$l(n)$
11	5.36×10^{33}
12	1.62×10^{44}
13	2.51×10^{56}
14	2.33×10^{70}
15	1.50×10^{86}

Para $n > 15$ las cotas de $L(n)$ se pueden calcular usando las mejores cotas dadas

$$\prod_{k=0}^{n-1} (n-k)!^{\frac{n}{n-k}} \geq L(n) \geq \frac{(n!)^{2n}}{n^{n^2}}.$$

Las estimaciones para el número de cuadrados latinos de orden n, para $n = 2^k$ con $k = 4, 5, 6, 7, 8$ son

$$0.689 \times 10^{138} \geq L(16) \geq 0.101 \times 10^{119}$$
$$0.985 \times 10^{784} \geq L(32) \geq 0.414 \times 10^{726}$$
$$0.176 \times 10^{4169} \geq L(64) \geq 0.133 \times 10^{4008}$$
$$0.164 \times 10^{21091} \geq L(128) \geq 0.337 \times 10^{20666}$$
$$0.753 \times 10^{102805} \geq L(256) \geq 0.304 \times 10^{101724}$$

1.2. Cuadrados Latinos Mutuamente Ortogonales ($MOLS$)

Una propiedad importante de los cuadrados latinos es la ortogonalidad, que surge cuando Euler en 1779 publica el problema que consiste en asignar a 36 oficiales de 6 diferentes rangos y 6 regimientos diferentes en un arreglo de tamaño 6×6 de manera que cada renglón y cada columna contenga a un oficial de cada regimen y uno de cada rango. Él conjeturó que tal arreglo era imposible.

Definamos de forma más precisa, lo que Euler buscaba basándonos en [2].

Sean $A = (a_{ij})$ y $B = (b_{ij})$ dos matrices de tamaño $n \times n$. La **unión** (A, B) es una matriz de tamaño $n \times n$ donde la entrada (i, j) es el par (a_{ij}, b_{ij}).

Ejemplo 1.2.1. *Sean*

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix}, B = \begin{pmatrix} 1 & 3 & 2 \\ 3 & 2 & 1 \\ 2 & 1 & 3 \end{pmatrix}$$

entonces

$$(A, B) = \begin{pmatrix} (1,1) & (2,3) & (3,2) \\ (2,3) & (3,2) & (1,1) \\ (3,2) & (1,1) & (2,3) \end{pmatrix}$$

o de manera equivalente

$$(A, B) = \begin{pmatrix} 11 & 23 & 32 \\ 23 & 32 & 11 \\ 32 & 11 & 23 \end{pmatrix}$$

.

Cabe mencionar, que a la matriz (A, B) Euler la llamó cuadrado **Greco-latino**, ya que usó letras latinas y griegas para definirla.

Decimos que dos cuadrados latinos A y B de orden n son **ortogonales** si todas las entradas en la unión (A, B) son distintas. Si A y B son ortogonales B es llamado el **compañero ortogonal** de A.

Los cuadrados latinos de orden 3 del ejemplo anterior no son ortogonales.

Notemos que el decir que todas las entradas de (A, B) sean diferentes es equivalente a que todos los posibles pares ocurran exactamente una vez. Tenemos solo n^2 posibles pares. De tal manera que la condición de ortogonalidad puede ser expresada de la siguiente manera

$$a_{ij} = a_{IJ} \quad \text{y} \quad b_{ij} = b_{IJ} \Longrightarrow i = I \quad \text{y} \quad j = J$$

De tal manera que el problema de Euler consistía en dar dos cuadrados latinos ortogonales de orden 6. Pero, él no sólo conjeturó que no existían tales cuadrados, sino que para además lo generalizó para cuadrados latinos de orden $n \equiv 2 \bmod 4$. En 1901, Gaston Tarry probó que no existían cuadrados latinos ortogonales de orden 6 construyéndolos exhaustivamente (9,408, considerando solo cuadrados latinos reducidos) agregando evidencia a la conjetura de Euler. Sin embargo, en 1959, Parker,

Bose y Shrikhande fueron capaces de construir un par de cuadrados latinos ortogonales de orden 10 y proporcionar una construcción para el resto de los valores, por supuesto a excepción de $n = 2$ y $n = 6$. La construcción de estos cuadrados la mostraremos más adelante.

Cuando $A_1, .., A_r$ sea un conjunto de cuadrados latinos de orden n ortogonales dos a dos, diremos que son **mutuamente ortogonales**. En adelante usaremos la abreviación $MOLS$ para referirnos a Cuadrados Latinos Mutuamente Ortogonales.

Denotaremos a $N(n)$ como el valor mas grande r para el cual existen r $MOLS$ de orden n, es decir, es el número máximo de $MOLS$ de orden n.

El siguiente teorema nos dice que para n siempre existe un par de cuadrados latinos ortogonales de orden n y su demostración nos da el método para construirlos.

Teorema 1.2.1. *$N(n) \geq 2$ para todo n impar.*

Demostración. Sean A y B dos matrices de tamaño $n \times n$ cuyas entradas pertenecen al conjunto $\{1, .., n\}$ definidas como

$$a_{ij} \equiv (j - i + 1) \bmod n \quad \text{y} \quad b_{ij} \equiv (j + i - 1) \bmod n.$$

Verifiquemos que A y B son cuadrados latinos.

$$a_{ij} = a_{ik} \Longrightarrow j - i + 1 \equiv (k - i + 1) \bmod n \Longrightarrow j \equiv k \bmod n \Longrightarrow j = k$$

de manera que las entradas en el i-ésimo renglón de A son todas distintas.

Análogamente $a_{ij} = a_{kj} \Longrightarrow j - i + 1 \equiv (j - k + 1) \bmod n \Longrightarrow i \equiv k \bmod n \Longrightarrow i = k$, por lo que las entradas en la j-ésima columna de A son todas distintas. Entonces A es un cuadrado latino de orden n. De forma similar se verifica que B es un cuadrado latino de orden n. Falta mostrar que A y B son ortogonales.

Supongamos que $(a_{ij}, b_{ij}) = (a_{IJ}, b_{IJ})$
$\Rightarrow a_{ij} = a_{IJ}$ y $b_{ij} = b_{IJ}$
$\Longrightarrow j - i + 1 \equiv (J - I + 1) \bmod n$ y $j + i - 1 \equiv (J + I - 1) \bmod n$
$\Longrightarrow j - i \equiv (J - I) \bmod n$ y $j + i \equiv (J + I) \bmod n$

sumando las dos últimas congruencias obtenemos $2j \equiv 2J \bmod n$ y si las restamos obtenemos $2i \equiv 2I \bmod n$ como n es impar se tiene que $j \equiv J \bmod n$ y $i \equiv I \bmod n$ de tal manera que $i = I$ y $j = J$. □

Ejemplo 1.2.2. *Los siguientes cuadrados latinos de orden 5 son ortogonales, dado que se construyeron mediante el método dado en la demostración del teorema anterior.*

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 3 & 4 \\ 4 & 5 & 1 & 2 & 3 \\ 3 & 4 & 5 & 1 & 2 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} \; y \; \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \\ 3 & 4 & 5 & 1 & 2 \\ 4 & 5 & 1 & 2 & 3 \\ 5 & 1 & 2 & 3 & 4 \end{pmatrix}$$

Una **transversal** de un cuadrado latino de orden n es un conjunto de n posiciones donde cualquiera dos de ellas no están en el mismo renglón ni en la misma columna, conteniendo a los n símbolos del conjunto base exactamente una vez.

El siguiente teorema nos da otra forma de saber cuando un cuadrado latino de orden n tiene un compañero ortogonal.

Teorema 1.2.2. *Un cuadrado latino de orden n tiene un compañero ortogonal si y sólo si tiene n transversales disjuntas.*

Ejemplo 1.2.3. *Sea C un cuadrado latino de orden 3*

$$C = \begin{pmatrix} 2 & 1 & 3 \\ 3 & 2 & 1 \\ 1 & 3 & 2 \end{pmatrix}$$

Tiene 3 transversales disjuntas

1. $(1,3),(2,2),(3,1)$
2. $(1,2),(2,1),(3,3)$
3. $(1,1),(2,3),(3,2)$

De tal manera que C tiene un compañero ortogonal C', el cual construimos de la siguiente forma

Sea (i,j) un elemento de la k-ésima transversal, entonces $C'(k,i) = j$. De tal manera que

$$C' = \begin{pmatrix} 3 & 2 & 1 \\ 2 & 1 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

.

El siguiente lema nos da una cota superior para $N(n)$.

Lema 1.2.1. *Para $n \geq 2$ se tiene que $N(n) \leq n-1$.*

Demostración. Supongamos que tenemos k $MOLS$ de orden n con conjunto base $\{1, 2, \ldots, n\}$. Podemos renombrar las entradas de cada uno de los cuadrados latinos de modo que el primer renglón de cada uno de ellos sea $12 \ldots n$.

Consideremos las k entradas en la posición $(2, 1)$, ninguna de ellas es 1, ya que 1 aparece en la posición $(1, 1)$ y como sabemos, cada elemento del conjunto base aparece exactamente una vez en cada columna. Sea s el valor de la entrada $(2, 1)$ en un cuadrado latino, la entrada $(2, 1)$ de cualquier otro cuadrado latino no puede tener el valor s, ya que si lo tuviera el par (s, s) aparecería dos veces al superponer los cuadrados latinos, ya que en la posición $(1, s)$ de ambos cuadrados se tiene el valor s, contradiciendo el hecho de ser ortogonales. Por lo que la entrada $(2, 1)$ tiene a lo mas $n - 1$ valores posibles. Por lo tanto $k \leq n - 1$. □

Llamaremos **cuadrado latino estándar** de orden n al cuadrado latino de orden n con conjunto base $A = \{a_1, a_2, \ldots, a_n\}$ cuyo primer renglón es $a_1 a_2 a_3 \cdots a_n$ y al conjunto de $n - 1$ $MOLS$ de orden n **Conjunto Completo**.

La cota superior para $N(n)$ se alcanza cuando n es potencia de un primo, la demostración del siguiente teorema nos proporciona un método para construir Conjuntos Completos de $MOLS$ de orden primo.

Teorema 1.2.3. *Sea q potencia de un primo, entonces existen q-1 MOLS de orden q.*

Demostración. Dado que q es potencia de un primo, entonces existe $GF(q) = \{\lambda_1, \lambda_2, ..., \lambda_{q-1}, \lambda_q = 0\}$. Sean $A_1, A_2, ..., A_{q-1}$ matrices de tamaño $q \times q$ donde la entrada (i, j) de A_k tendrá el valor

$$\lambda_i \lambda_k + \lambda_j \ \ , \ \ 1 \leq k \leq q - 1$$

Primero verificamos que cada A_k es un cuadrado latino.

Si dos entradas en el i-ésimo renglón de A_k son iguales

$\lambda_i \lambda_k + \lambda_j = \lambda_i \lambda_k + \lambda_J \Rightarrow \lambda_j = \lambda_J \Rightarrow j = J$.

Si dos entradas en la j-ésima columna de A_k son iguales tenemos que

$\lambda_i \lambda_k + \lambda_j = \lambda_I \lambda_k + \lambda_j \Rightarrow \lambda_i \lambda_k = \lambda_I \lambda_k \Rightarrow \lambda_i = \lambda_I$.

Dado que $\lambda_k \neq 0$ entonces existe λ_k^{-1} su inverso multiplicativo, de tal manera que $\lambda_i = \lambda_I \Rightarrow i = I$.

Falta probar que los cuadrados son mutuamente ortogonales.

Sea $k \neq K$, supongamos que

$\lambda_i \lambda_k + \lambda_j = \lambda_I \lambda_k + \lambda_J$ y $\lambda_i \lambda_K + \lambda_j = \lambda_I \lambda_K + \lambda_J$

sumandolas obtenemos $\lambda_i(\lambda_k - \lambda_K) = \lambda_I(\lambda_k - \lambda_K)$ dado que $\lambda_k \neq \lambda_K \Rightarrow (\lambda_k - \lambda_K) \neq 0$ por lo cual $\lambda_i = \lambda_I \Rightarrow i = I$. Sustituyendo $\lambda_i = \lambda_I$ en la primera igualdad se tiene que $\lambda_j = \lambda_J \Rightarrow j = J$. □

Ejemplo 1.2.4. *usando* $GF(4) = \{0, 1, x, x^2\}$ *donde* $x^2 = x + 1$ *y mediante el método dado en la demostración anterior se construye el siguiente conjunto completo de cuadrados latinos de orden 4.*

Con $\lambda_1 = 1, \lambda_2 = x, \lambda_3 = x^2, \lambda_4 = 0$ *obtenemos*

$$\begin{pmatrix} 0 & x^2 & x & 1 \\ x^2 & 0 & 1 & x \\ x & 1 & 0 & x^2 \\ 1 & x & x^2 & 0 \end{pmatrix}, \begin{pmatrix} x^2 & 0 & 1 & x \\ x & 1 & 0 & x^2 \\ 0 & x^2 & x & 1 \\ 1 & x & x^2 & 0 \end{pmatrix}, \begin{pmatrix} x & 1 & 0 & x^2 \\ 0 & x^2 & x & 1 \\ x^2 & 0 & 1 & x \\ 1 & x & x^2 & 0 \end{pmatrix}.$$

Si se invierte el orden de las filas y reemplazando a $1, x, x^2, 0$ *por* $1, 2, 3, 4$ *tenemos a los siguientes 3 MOLS de orden 4*

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

El siguiente teorema tiene un papel muy importante en el estudio de los $MOLS$.

Teorema 1.2.4 (**Moore-MacNeish**). $N(mn) \geq \min(N(m), N(n))$.

Demostración. Sean $A^{(1)}$,...,$A^{(s)}$ $MOLS$ de orden m con conjunto base $\{0, 1, ..., m-1\}$ y sean $B^{(1)}$,...,$B^{(s)}$ s $MOLS$ de orden n con conjunto base $\{0, 1, ..., n-1\}$.

Debemos construir s $MOLS$ $C^{(1)}, ..., C^{(s)}$ de orden mn con conjunto base $\{0, 1, ..., mn-1\}$.

Sea A es un cuadrado latino de orden m y B uno de orden n, se define el producto de A y B como

$$C = A \times B = \begin{pmatrix} B + a_{11}nJ & B + a_{12}nJ & \cdots & B + a_{1m}nJ \\ \vdots & & & \\ B + a_{m1}nJ & B + a_{m2}nJ & \cdots & B + a_{mm}nJ \end{pmatrix}$$

.

Entonces C es una matriz de tamaño $mn \times mn$ y como a_{ij} toma valores de $1, ..., m-1$ y las entradas de B toman valores de $0, ..., n-1$ entonces las entradas de C toman valores de 0 hasta $n - 1 + n(m-1) = mn - 1$, mas aún C es un cuadrado latino.

Consideremos cualquier renglón de C, los a_{ij} toman valores de $0, ..., m-1$ exactamente una vez de igual manera para las entradas de B encontramos cada valor de $0, ..., n-1$ exactamente una vez, por lo que las entradas en los renglones de C son precisamente los posibles números de la forma $an + b$ con $0 \leq a \leq m-1$ y $0 \leq b \leq n-1$, es decir, los números pueden tomar valores de 0 a $mn - 1$. Un argumento similar se cumple para las columnas.

Sea $C^{(t)}$ el producto de $A^{(t)}$ y $B^{(t)}$, $1 \leq t \leq s$. Debemos mostrar que $C^{(1)}, ..., C^{(s)}$ son $MOLS$ de orden mn.

Supongamos que $(C_{ij}^{(r)}, C_{ij}^{(t)}) = (C_{IJ}^{(r)}, C_{IJ}^{(t)})$
$\Rightarrow C_{ij}^{(r)} = C_{IJ}^{(r)}$ y $C_{ij}^{(t)} = C_{IJ}^{(t)}$ (1).

Para encontrar C_{ij} definimos a i y a j de la siguiente manera

$$i = (k-1)n + l \quad , \ 1 \leq l \leq n \ \text{ y}$$
$$j = (g-1)n + h \quad , \quad 1 \leq h \leq n$$

entonces $C_{ij}^{(r)} = b_{lh}^{(r)} + na_{kg}^{(r)}$.

De manera similar escribimos $I = (K-1)n + L$, $J = (G-1)n + H$ entonces (1) se convierte en

$$b_{lh}^{(r)} + na_{kg}^{(r)} = b_{LH}^{(r)} + na_{KG}^{(r)}$$
$$b_{lh}^{(t)} + na_{kg}^{(t)} = b_{LH}^{(t)} + na_{KG}^{(t)}$$

entonces cada entero tiene una representación única de la forma $an + b$, por lo que se sigue

$$b_{lh}^{(r)} = b_{LH}^{(r)}$$
$$b_{lh}^{(t)} = b_{LH}^{(t)}$$
$$a_{kg}^{(r)} = a_{KG}^{(r)}$$
$$a_{kg}^{(t)} = a_{KG}^{(t)}$$

entonces $B^{(r)}$ y $B^{(t)}$ son ortogonales ya que $l = L$ y $h = H$. De igual manera $A^{(r)}$ y $A^{(t)}$ son ortogonales ya que $k = K$ y $g = G$ finalmente $i = I$ y $j = J$. □

Puesto que $N(p^\alpha) = p^\alpha - 1$ cuando p es primo obtenemos el siguiente resultado.

Corolario 1.2.1. *Si $n = p_1^{\alpha_1} ... p_r^{\alpha_r}$, entonces $N(n) \geq (\min p_i^{\alpha_i}) - 1$.*

Ejemplo 1.2.5. *Sea $n = 12m + 7$ entonces la potencia del primo más pequeño que posiblemente divide a n es 5, entonces $N(n) \geq 5 - 1 = 4$.*

Notemos que si n es impar tenemos que para cada $p_i^{\alpha_i}$ es por lo menos 3, entonces $N(n) \geq 2$ y si n es múltiplo de 4 entonces cada $P_i^{\alpha_i}$ es nuevamente por lo menos 3, por lo que $N(n) \geq 2$.

1.3. $MOLS$ y Planos Proyectivos de orden n

En ésta sección mostraremos como un conjunto completo de $MOLS$ es equivalente a un plano proyectivo. Con esta relación nos podemos dar cuenta que el determinar un conjunto completo de $MOLS$ puede ser extremadamente difícil, ya que el mostrar la inexistencia de un plano proyectivo de orden 10 es un problema que hasta el momento no se a podido demostrar.

Sea $S = \{1, \ldots, v\}$. Decimos que una colección D de subconjuntos distintos de S es llamada un (v, k, λ) **diseño** si $2 \leq k < v, \lambda > 0$ y

- Cada conjunto en D contiene exactamente k elementos.
- Cada subconjunto de 2 elementos de S esta contenido en exactamente λ de los subconjuntos de D.

Los conjuntos de D son llamados **bloques** y el número de bloques de D es denotado por b. Decimos que un diseño es **simétrico** cuando $b = v$.

Un **Plano Proyectivos** de orden n es un $(n^2 + n + 1, n + 1, 1)$ diseño simétrico. Se sabe que para toda potencia de un número primo q, existe un plano proyectivo de orden q.

El siguiente teorema relaciona al conjunto completo de $MOLS$ con los planos proyectivos.

Teorema 1.3.1. *Un conjunto completo de n-1 $MOLS$ de orden n existe si y sólo si existe un plano proyectivo finito de orden n.*

Demostración. Sea $\{L_1, L_2, \ldots, L_{n-1}\}$ el conjunto de $n - 1$ $MOLS$ de orden n. Definimos el siguiente arreglo de tamaño $(n + 1) \times n^2$

$$\left(\begin{array}{cccccccccccccccc}
1 & 1 & 1 & \cdots & 1 & 2 & 2 & 2 & \cdots & 2 & \cdots & n & n & n & \cdots & n \\
1 & 2 & 3 & \cdots & n & 1 & 2 & 3 & \cdots & n & \cdots & 1 & 2 & 3 & \cdots & n \\
 & \text{renglón} & 1 & \text{en} & L_1 & & \text{renglón} & 2 & \text{en} & L_1 & \cdots & & \text{renglón} & n & \text{en} & L_1 \\
 & \text{renglón} & 1 & \text{en} & L_2 & & \text{renglón} & 2 & \text{en} & L_2 & \cdots & & \text{renglón} & n & \text{en} & L_2 \\
 & & & \vdots & & & & & & & & & & & & \\
 & \text{renglón} & 1 & \text{en} & L_{n-1} & & \text{renglón} & 2 & \text{en} & L_{n-1} & \cdots & & \text{renglón} & n & \text{en} & L_{n-1}
\end{array}\right)$$

. Este arreglo tiene las siguientes propiedades de ortogonalidad

Tomando cualesquiera dos renglones, los n^2 pares verticales posibles $\binom{1}{1}, \binom{1}{2}, \ldots, \binom{1}{n}$ aparecen exactamente una vez.

El primer y segundo renglón por definición satisfacen la propiedad. Si $i \leq 2 < j$ comparando el i-ésimo y el j-ésimo renglón tenemos los n^2 pares verticales posibles, ya que si $i = 1$ implicaría que el j-ésimo cuadrado latino tiene a un elemento del conjunto base mas de una vez en un renglón y si $i = 2$ implicaría que el j-ésimo cuadrado latino tiene más de una vez aun elemento del conjunto base en una de sus columnas, pero esto no es posible por definición de cuadrado latino.

Si $i, j \geq 3$ ambos renglones provienen de un cuadrado latino, por lo que satisfacen la propiedad por la ortogonalidad de los cuadrados.

Etiquetamos las columna del arreglo por $1, 2, \ldots, n^2$. Cada uno de los $n + 1$ renglones nos da n bloques que definimos de la siguiente manera: para $i = 1, \ldots, n$ tomo como bloque al conjunto de etiquetas de las columnas donde el renglón toma el valor i. Estos $n(n+1) = n^2 + n$ bloques forman un $(n^2, n, 1)$ diseño.

Falta demostrar que $\lambda = 1$, es decir que cualesquiera par de elementos del conjunto $\{1, 2, \ldots, n^2\}$ no puede estar en más de 1 bloque. Esto es equivalente a probar que toda pareja posible esta en

el arreglo, en total el arreglo debe tener $\binom{n^2}{2} = \frac{n^2(n^2-1)}{2}$. Los bloques juntos forman $n(n+1)\binom{n}{2} = \frac{n(n+1)n(n-1)}{2} = \frac{n^2(n^2-1)}{2}$. Por lo tanto toda pareja esta.

Sea D un $(n^2, n, 1)$ diseño con clases paralelas $D_1, D_2, \ldots, D_{n+1}$. Podemos (por renombramiento del conjunto base) suponer que las primeras dos clases paralelas son representadas por los dos primeros renglones del arreglo anterior y escribiendo las otras $n-1$ clases paralelas como los últimos $n-1$ renglones. Dado que los renglones se originan de un diseño con $\lambda = 1$, el arreglo tiene la propiedad de ortogonalidad. Entonces interpretando los últimos $n-1$ renglones como matrices de tamaño $n \times n$ nos dan $n-1$ cuadrados latinos mutuamente ortogonales. □

1.4. Cuadrados Latinos Auto-Ortogonales ($SOLS$)

La importancia de esta sección y las siguientes es que son parte importante del trabajo desarrollado por Bose, Shrikhande y Parker que prueba la existencia de dos $MOLS$ de orden n para $n \neq 2, 6$, hasta el momento sabemos que $N(n) \geq 2$ para n impar, para $n \geq 2$ se tiene que $N(n) \leq n-1$ y que para n potencia de un primo $N(n) = n-1$.

Ahora, presentamos un nuevo tipo de cuadrados latinos, los cuadrados latinos auto-ortogonales.

Un cuadrado latino de orden n es **auto-ortogonal** si es ortogonal a su transpuesto y lo denotaremos como $SOLS(n)$.

Ejemplo 1.4.1. *El siguiente cuadrado latinos de orden 4 es auto-ortogonal*

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

entonces (A, A^t) *es*

$$\begin{pmatrix} 11 & 24 & 32 & 43 \\ 42 & 33 & 21 & 14 \\ 23 & 12 & 44 & 31 \\ 34 & 41 & 13 & 22 \end{pmatrix}$$

como podemos observar, en la unión se encuentran todas las parejas posibles.

Los siguientes resultados nos dicen para que orden n un $SOLS(n)$ existe.

Teorema 1.4.1 (**Mendelshn, 1971**). *Un SOLS existe cuando* $(n, 6) = 1$.

Demostración. Definimos una matriz A cuadrada de tamaño $n \times n$, $A = (a_{ij})$ donde

$$a_{ij} = 2i - j(\mathrm{mod}\, n),\ 1 \leq a_{ij} \leq n$$

Primero verifiquemos que A es un cuadrado latino.
Sea

$$\begin{aligned} a_{ij} &= a_{ik} \\ \Rightarrow 2i - j &\equiv 2i - k(\mathrm{mod}\, n) \\ \Rightarrow j &\equiv k(\mathrm{mod}\, n) \\ \Rightarrow j &= k. \end{aligned}$$

Ahora sea

$$\begin{aligned} a_{ij} &= a_{kj} \\ \Rightarrow 2i - j &\equiv (2k - j)\,\mathrm{mod}\, n \\ \Rightarrow 2i &\equiv 2k\,\mathrm{mod}\, n \\ \Rightarrow i &= k. \end{aligned}$$

Por lo tanto A es un cuadrado latino.
Ahora verifiquemos que A y A^t son ortogonales.

Sea

$$A^t = (a_{ij}^t) = (a_{ji}).$$

Supongamos que

$$a_{ij} = a_{kl} \text{ y } a_{ij}^t = a_{kl}^t,$$

es decir

$$a_{ij} = a_{kl} \text{ y } a_{ji} = a_{lk}$$

entonces

$$\begin{aligned} 2i - j &\equiv (2k - l)\,\mathrm{mod}\, n \quad (1) \\ 2j - i &\equiv (2l - k)\,\mathrm{mod}\, n. \end{aligned}$$

Sumandolas obtenemos

$$i + j \equiv (k + l)\,\mathrm{mod}\, n$$

de la congruencia anterior tenemos

$$i \equiv (k + l - j) \bmod n.$$

Sustituyendo i en (1)

$$\begin{aligned} 2(k + l - j) &\equiv (2k - l) \bmod n \\ 2k + 2l - 2j - j &\equiv (2k - l) \bmod n \\ 3j &\equiv 3l \bmod n \end{aligned}$$

entonces $(n, 3) = 1$,
además

$$\begin{aligned} j &\equiv l \bmod n \\ \Rightarrow j &= l \ \text{ y } k = i \end{aligned}$$

Por lo tanto A y A^t son ortogonales. □

Ejemplo 1.4.2. *Los siguientes SOLS de orden* 5 *y* 7 *son obtenidos de la construcción dada en la demostración del teorema anterior.*

$$\begin{pmatrix} 1 & 5 & 4 & 3 & 2 \\ 3 & 2 & 1 & 5 & 4 \\ 5 & 4 & 3 & 2 & 1 \\ 2 & 1 & 5 & 4 & 3 \\ 4 & 3 & 2 & 1 & 5 \end{pmatrix} \begin{pmatrix} 1 & 7 & 6 & 5 & 4 & 3 & 2 \\ 3 & 2 & 1 & 7 & 6 & 5 & 4 \\ 5 & 4 & 3 & 2 & 1 & 7 & 6 \\ 7 & 6 & 5 & 4 & 3 & 2 & 1 \\ 2 & 1 & 7 & 6 & 5 & 4 & 3 \\ 4 & 3 & 2 & 1 & 7 & 6 & 5 \\ 6 & 5 & 4 & 3 & 2 & 1 & 7 \end{pmatrix}.$$

Teorema 1.4.2 (**Mendelsohn, 1971**). *Si n es potencia de primos, $n \neq 2, 3$ entonces un $SOLS(n)$ existe.*

Demostración. Se construirá un $SOLS(n)$ con los elementos de $GF(n) = \{c_1 = 0, c_2, ..., c_n\}$) como entradas. Eligiendo $\lambda \in GF(n)$ tal que $\lambda \neq 0$, $\lambda \neq 1$, $2\lambda \neq 1$ definimos una matriz $A = (a_{ij})$ de tamaño $n \times n$ donde

$$a_{ij} = \lambda c_i + (1 - \lambda) c_j.$$

Es fácil verificar que A es un cuadrado latino de orden n. Entonces mostremos que A es auto-ortogonal.

Sea

$$a_{ij} = a_{kl} \quad \text{y} \quad a^t_{ij} = a^t_{kl}$$

$$\Rightarrow \lambda c_i + (1-\lambda)c_j = \lambda c_k + (1-\lambda)c_l \text{ y}$$
$$\lambda c_j + (1-\lambda)c_i = \lambda c_l + (1-\lambda)c_k.$$

Sumando las dos ecuaciones anteriores obtenemos

$$c_i + c_j = c_k + c_l$$

despejando a c_i y sustituyéndola en la primera ecuación nos queda

$$\lambda(c_k + c_l - c_j) + (1-\lambda)c_j = \lambda c_k + (1-\lambda)c_l,$$

es decir,

$$(1-2\lambda)c_j = (1-2\lambda)c_l$$

$$\Rightarrow c_j = c_l$$
$$\Rightarrow 2\lambda \neq 1.$$

Además

$$j = l \quad \text{y} \quad i = k.$$

□

Estos resultados garantizan la existencia de $SOLS$ de orden n=4,8,16,... y n=9,27,81,.... En 1973 Brayton, Coppersmith y Hoffman probaron el siguiente resultado.

Teorema 1.4.3. *Si $n \neq 2, 3, 6$, un $SOLS(n)$ existe.*

1.4.1. $SOLS$ y Torneo Doble Mixto

En esta subsección mostramos la relación que existe entre los $SOLS$ y cierto tipo de torneos.

Un **torneo** $SAMDRR(n)$ (spouse-avoiding mixed doubles round robin) es un torneo doble mixto donde participan n matrimonios, en cada juego participan dos equipos, donde cada equipo consta de dos jugadores de sexo opuesto. Los partidos son tales que cada dos jugadores del mismo sexo juegan entre sí exactamente una vez y cada jugador con cada miembro del sexo opuesto (que no sea su cónyuge) exactamente una vez como compañero y una vez como oponente.

En 1917 Dudeney dio el siguiente ejemplo resoluble para n=4, donde los matrimonios son (H_i, M_i) para $1 \leq i \leq 4$.

Ejemplo 1.4.3.

$$H_1M_3 \ vs \ H_2M_4 \quad H_3M_1 \ vs \ H_4M_2$$

$$H_1M_4 \ vs \ H_3M_2 \quad H_4M_1 \ vs \ H_2M_3$$

$$H_1M_2 \ vs \ H_4M_3 \quad H_2M_1 \ vs \ H_3M_4$$

es un $SAMDRR(4)$.

Como observamos el torneo puede jugarse en 3 rondas.

Antes de mostrar la relación entre los $SOLS$ y $SAMDRR$ necesitamos dar la siguiente propiedad de los $SOLS$.

Lema 1.4.1. *Sea A un $SOLS(n)$, entonces su diagonal principal es una transversal.*

Demostración. A^t tiene la misma diagonal que A. Si $a_{ii} = a_{jj} = k$ entonces el par (k, k) aparecería dos veces en la union de A con A^t, contradiciendo la propiedad de ortogonalidad. Por lo tanto la diagonal principal de A es una transversal. □

Ahora, el siguiente teorema nos da la relación que existe entre los $SOLS(n)$ con los $SAMDRR(n)$.

Teorema 1.4.4. *Un $SAMDRR(n)$ existe si y sólo si un $SOLS(n)$ existe.*

Demostración. Supongamos que un $SAMDRR(n)$ existe. Denotamos a los matrimonios como (H_i, M_i) para $1 \leq i \leq n$. Entonces definimos a A una matriz de tamaño $n \times n$ como sigue

$a_{ii} = i$ y
$a_{ij} = l$, donde M_l es el compañero de H_i cuando H_i y H_j juegan con $i \neq j$.

Dado que las asociaciones no se repiten, podemos concluir que A es un cuadrado latino.

Ahora verifiquemos que A y A^t son ortogonales. Supongamos que $a_{ij} = a_{IJ}$ y $a_{ji} = a_{JI}$.

Si $a_{ij} = l$ y $a_{ji} = m$ se tienen los siguientes juegos

$$H_iM_l \text{ vs } H_jM_m \ \text{ y } \ H_IM_l \text{ vs } H_JM_m$$

pero como sabemos, jugadores del mismo sexo juegan entre sí exactamente una vez, por lo que $i = I$ y $j = J$. De tal manera que A es un $SOLS(n)$.

Ahora, sea A un $SOLS(n)$ donde las entradas de A pueden ser renombradas de la siguiente forma

$a_{ii} = i$ para todo i y si $a_{ij} = l$ y $a_{ji} = m$, de tal manera que los juegos se definen como H_iM_l vs H_jM_m. □

Ejemplo 1.4.4. *Sea* $A = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \end{pmatrix}$ *un* $SOLS(4)$*, renombrando las entradas como nos dice la demostración del teorema anterior obtenemos* $A = \begin{pmatrix} 1 & 4 & 2 & 3 \\ 3 & 2 & 4 & 1 \\ 4 & 1 & 3 & 2 \\ 2 & 3 & 1 & 4 \end{pmatrix}$ *de tal manera que este* $SOLS(4)$ *nos da un* $SAMDRR(4)$ *con las siguientes rondas*

$$H_1M_4 \text{ vs } H_2M_3 \quad H_1M_2 \text{ vs } H_3M_4 \quad H_1M_3 \text{ vs } H_4M_2$$

$$H_2M_4 \text{ vs } H_3M_1 \quad H_2M_1 \text{ vs } H_4M_3 \quad H_3M_2 \text{ vs } H_4M_1$$

.

Ahora veremos como algunos teoremas que se estudiaron para los $MOLS$ se satisfacen también para los $SOLS$.

Teorema 1.4.5. *Si existe un* $SOLS(m)$ *y un* $SOLS(n)$*, entonces existe un* $SOLS(mn)$

Demostración. Sean A y B $SOLS$ de orden m y n con conjuntos base $\{0, 1, \ldots, m-1\}$ y $\{0, 1, \ldots, n-1\}$ respectivamente. Entonces los productos $A \times B$ y $A^t \times B^t$ como se definieron en la prueba del teorema de Moore-MacNeish son $MOLS$ de orden mn. Verificando que $(A \times B)^t = A^t \times B^t$ se tiene que $A \times B$ es auto-ortogonal. □

De los Teoremas 1.4.2 y 1.4.5 se sigue el siguiente resultado.

Corolario 1.4.1. *Si* $n = 2^\alpha 3^\beta 5^r \ldots$*, donde* $\alpha \neq 1$ *y* $\beta \neq 1$*, entonces existe un* $SOLS(n)$*.*

El siguiente resultado relaciona a los diseños balanceados con los $SOLS$.

Teorema 1.4.6. *Supongamos que un* $PBD(v, k, 1)$ *existe y que para cada* $k \in K$ *un* $SOLS(k)$ *existe. Entonces un* $SOLS(v)$ *existe.*

Demostración. Para cada k, reemplazamos cada bloque de tamaño k por un $SAMDRR(k)$ sobre sus elementos. La union de estos torneos es un $SAMDRR(v)$, entonces por el teorema 1.4.4 un $SOLS(v)$ existe. □

De los teoremas 1.4.2. y 1.4.5 se sigue el siguiente resultado.

Teorema 1.4.7. *Para cada* $k \geq 1$*, un* $SOLS(4k)$ *existe.*

Ejemplo 1.4.5. *El siguiente cuadrado es un $SOLS(12)$.*

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

El siguiente $SOLS$ de orden 14 nos permite afirmar que $N(14) \geq 2$.

Ejemplo 1.4.6.

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

1.5. Arreglos Ortogonales

En esta sección mostramos la relación que existe entre los $MOLS$ y los arreglos ortogonales que nos permitirá mostrar algunos resultados importantes para $N(n)$.

Los arreglos ortogonales son una forma alternativa de representar a un conjunto de $MOLS$.

Ejemplo 1.5.1. *Tenemos el siguiente arreglo ortogonal*

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

los primeros dos renglones determinan las posiciones de los elementos de los cuadrados, es decir, el primero nos indica el renglón y el segundo la columna. El tercero y cuarto renglón son los valores de los cuadrados latinos en la posición que nos indican los primeros dos renglones. De tal manera que el arreglo nos representa a un conjunto de 2 cuadrados latinos de orden 3.

Un **arreglo ortogonal** sobre un alfabeto de n símbolos es una matriz de tamaño $s \times n^2$ en donde al elegir cualesquiera dos renglones podemos encontrar a todos los pares verticales posibles exactamente una vez. A este tipo de arreglo lo denotaremos como $OA(s, n)$.

Con los arreglos ortogonales se pueden establecer algunas cotas para $N(n)$.

Teorema 1.5.1. *Un $OA(s, n)$ existe si y sólo si $N(n) \geq s - 2$.*

Demostración. Sean $M_1, M_2, \ldots, M_{s-2}$ $MOLS$ de orden n, construimos una matriz de tamaño $s \times n^2$ donde sus primeros dos renglones sean

$$\begin{pmatrix} 1 & 1 & \ldots & 1 & 2 & 2 & \ldots & 2 & \ldots & n & n & \ldots & n \\ 1 & 2 & \ldots & n & 1 & 2 & \ldots & n & \ldots & 1 & 2 & \ldots & n \end{pmatrix}$$

y el i-ésimo renglón del arreglo es

$$\begin{pmatrix} M_{i-2}(1,1) & M_{i-2}(1,2) & \ldots & M_{i-2}(1,n) & M_{i-2}(2,1) & \ldots & M_{i-2}(2,n) & \ldots & M_{i-2}(n,1) & \ldots & M_{i-2}(n,n) \end{pmatrix}$$

para $2 < i \leq s$. Falta verificar que este arreglo es ortogonal.

Si $i \geq 1$. El renglón 1 y el renglón $i+2$ tienen cada par ordenado exactamente una vez entonces cada renglón del i-ésimo cuadrado contiene a cada elemento exactamente una vez. De manera similar para los renglones 2 y el $i+2$.

Para los renglones $i+2$ y $j+2$ por la ortogonalidad de los cuadrados i y j encontramos a todos los pares verticales posibles exactamente una vez. De tal manera que el arreglo definido es ortogonal.

Inversamente, sea un $OA(s, n)$. Reordenando las columnas de tal manera que los primeros dos renglones queden de la siguiente manera

$$\begin{pmatrix} 1 & 1 & \ldots & 1 & 2 & 2 & \ldots & 2 & \ldots & n & n & \ldots & n \\ 1 & 2 & \ldots & n & 1 & 2 & \ldots & 1 & \ldots & 1 & 2 & \ldots & n \end{pmatrix}$$

Entonces los cuadrados M_k con $1 \leq k \leq s-2$ definidos por tomar como valor para $M_k(i,j)$ la entrada en el renglón $k+2$ sobre la columna que contiene en sus dos primeros renglones el par $\binom{i}{j}$ son ortogonales. □

Ejemplo 1.5.2. *El siguiente $OA(5,4)$ corresponde a 3 $MOLS$ de orden 4.*

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 & 3 & 3 & 3 & 3 & 4 & 4 & 4 & 4 \\ 1 & 2 & 3 & 4 & 1 & 2 & 3 & 4 & 1 & 2 & 3 & 4 & 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 & 2 & 1 & 4 & 3 & 3 & 4 & 1 & 2 & 4 & 3 & 2 & 1 \\ 1 & 2 & 3 & 4 & 4 & 3 & 2 & 1 & 2 & 1 & 4 & 3 & 3 & 4 & 1 & 2 \\ 1 & 2 & 3 & 4 & 3 & 4 & 1 & 2 & 4 & 3 & 2 & 1 & 2 & 1 & 4 & 3 \end{pmatrix}$$

Teorema 1.5.2. *Si $N(m) \geq 2$, entonces $N(3m+1) \geq 2$.*

Demostración. Consideremos el siguiente arreglo A_0 de tamaño $4 \times 4m$

$$\begin{pmatrix} 0 & 0 & \dots & 0 & 1 & \dots & m & 2m & \dots & m+1 & x_1 & \dots & x_m \\ 1 & 2 & \dots & m & 0 & \dots & 0 & x_1 & \dots & x_m & 2m & \dots & m+1 \\ 2m & 2m-1 & \dots & m+1 & x_1 & \dots & x_m & 0 & \dots & 0 & 1 & \dots & m \\ x_1 & x_2 & \dots & x_m & 2m & \dots & m+1 & 1 & \dots & m & 0 & \dots & 0 \end{pmatrix}.$$

En el arreglo los x_i son m símbolos distintos de $0, \dots, 2m$.

Sea A_i el arreglo obtenido de A_0 por sumar i a cada entrada numérica (mód $2m+1$) y dejando a cada x_i sin cambios. Dado que $N(m) \geq 2$, existe un $OA(4,m)$ sobre $x_1, \dots, x_m$ que denotaremos como A^* y si también

$$E = \begin{pmatrix} 0 & 1 & \dots & 2m \\ 0 & 1 & \dots & 2m \\ 0 & 1 & \dots & 2m \\ 0 & 1 & \dots & 2m \end{pmatrix}$$

podemos afirmar que el arreglo

$$D = [EA_0A_1 \dots A_{2m}A^*]$$

es un $AO(4, 3m+1)$. Ciertamente, el número de columnas es $2m+1+(2m+1)4m+m^2 = 9m^2+6m+1 = (3m+1)^2$. Para cualquier par de filas, el par ordenado (x_i, n) aparecerá exactamente una vez para cada i y cada n, al igual que el par (n, x_i) y los arreglos E y A^* tienen a cada par ordenado de la forma (n,n) o (x_i, x_i) exactamente una vez. Queda por demostrar que si $0 \leq u \leq 2m$ y $0 \leq v \leq 2m$, $u \neq v$ el par (u,v) aparece exactamente una vez. Sin perdida de generalidad consideremos el segundo y tercer renglón de A_0. La diferencia entre números correspondientes en esos dos renglones son $2m-1, 2m-3, \dots, 3, 1$ y sus negativos mód $(2m+1)$, es decir, también

están $0, 2, 4, \ldots, 2m$ exactamente una vez. Al tener todas las diferencias posibles podemos concluir que están todas las (u, v) exactamente una vez. Un argumento similar se satisface para cualquier par de renglones. □

Corolario 1.5.1. *$N(12t + 10) \geq 2$ para todo entero t*

Demostración. Sea $m = 4t + 3$, sustituyendo m en el teorema anterior tenemos que

$$N(3(4t + 3) + 1) \geq 2$$
$$N(12t + 10) \geq 2$$

□

Teorema 1.5.3. *Si existe un $OA(n_1, s)$ y un $OA(n_2, s)$ entonces existe un $OA(n_1 n_2, s)$*

Demostración. Sea un $OA(n_1, s)$ la matriz $A = (a_{ij})$ con $i = 1, \ldots, s$ y $j = 1, \ldots, n_1^2$ y un $OA(n_2, s)$ la matriz $B = (b_{ij})$ con $i = 1, \ldots, s$ y $j = 1, \ldots, n_2^2$.

Con A y B formemos la matriz $D = (d_{ij})$ con $i = 1, \ldots, s$ y $j = 1, \ldots, n_1^2 n_2^2$. Reemplazando a_{ij} de A por el vector renglón

$$(b_{i1} + m_{ij}, b_{i2} + m_{ij}, \ldots, b_{in_2^2} + m_{ij})$$

donde $m_{ij} = (a_{ij} - 1)n_2$ para todo i, j.

Sabemos que a_{ij} toma valores de 1 hasta n_1 y b_{ij} toma valores de 1 hasta n_2, entonces $b_{it} + m_{ij} = b_{it} + (a_{ij} - 1)n_2$ toma valores desde 1 hasta $n_1 n_2$.

Consideremos los renglones h e i de D y sean u, v cualesquiera dos números de $1, 2, \ldots, n_1 n_2$, de tal manera que podemos escribir a $u = u_1 + (u_2 - 1)n_2$ y a $v = v_1 + (v_2 - 1)n_2$ con $1 \leq u_1, v_1 \leq n_2$ y $1 \leq u_2, v_2 \leq n_1$.

En A vamos a determinar a j como una columna en donde

$$a_{ht} = u_2, a_{ij} = v_2$$

y en B vamos a determinar a t como una columna en donde

$$b_{ht} = u_1, b_{it} = v_1$$

. Entonces en D, en la columna $g = t + n_2^2(j - 1)$ tenemos

$$d_{hg} = b_{ht} + (a_{hj} - 1)n_2 = u_1 + (u_2 - 1)n_2 = u$$

y

$$d_{ig} = b_{it} + (a_{ij} - 1)n_2 = v_1 + (v_2 - 1)n_2 = v$$

. Por lo cual los renglones h e i de D son ortogonales y como fueron elegidos de manera arbitraria podemos concluir que D es un arreglo ortogonal. □

Corolario 1.5.2. *Si $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ es la factorización del entero n en potencias de los primos distintos $p_1, \ldots, p_r$, entonces existen al menos $N(n)$ $MOLS$ de orden n, donde $N(n) \geq \min(p_i^{e_i} - 1)$ con $i = 1, \ldots, r$.*

Demostración. Dado que para $n = p_i^{e_i}$, $i = 1, \ldots, r$ hay un $OA(n_i, n_i + 1)$ para $i = 1, \ldots, r$. Si tomamos a s como el mínimo de todos los $n_i + 1$, existe un $OA(n_i, s)$. Si aplicamos repetidas veces el teorema anterior, entonces existe un $OA(n, s)$ y así podemos decir que $s - 2 = min(n_i - 1)$ $MOLS$ de orden n □

El siguiente ejemplo es el cuadrado greco-latino dado por Parker(1959) que muestra que $N(10) \geq 2$.

Ejemplo 1.5.3.

$$\begin{pmatrix} 00 & 47 & 18 & 76 & 29 & 93 & 85 & 34 & 61 & 52 \\ 86 & 11 & 57 & 28 & 70 & 39 & 94 & 45 & 02 & 63 \\ 95 & 80 & 22 & 67 & 38 & 71 & 49 & 56 & 13 & 04 \\ 59 & 96 & 81 & 33 & 07 & 48 & 72 & 60 & 24 & 15 \\ 73 & 69 & 90 & 82 & 44 & 17 & 58 & 01 & 35 & 26 \\ 68 & 74 & 09 & 91 & 83 & 55 & 27 & 12 & 46 & 30 \\ 37 & 08 & 75 & 19 & 92 & 84 & 66 & 23 & 50 & 41 \\ 14 & 25 & 36 & 40 & 51 & 62 & 03 & 77 & 88 & 99 \\ 21 & 32 & 43 & 54 & 65 & 06 & 10 & 89 & 97 & 78 \\ 42 & 53 & 64 & 05 & 16 & 20 & 31 & 98 & 79 & 87 \end{pmatrix}$$

.

El siguiente cuadrado latinos de orden 10 fue dado por Hedayat (1973) que satisface la propiedad de ser auto-ortogonal, dando así una prueba independiente de que $N(10) \geq 2$.

Ejemplo 1.5.4.

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

.

1.6. Colapso de la conjetura de Euler

Usando los diseños balanceados Parker mostró que $N(21) \geq 4$.

Un **diseño balanceado** PBD (v, K, λ) es una colección de subconjuntos (bloques) de un conjunto S de cardinalidad v tal que

1. El tamaño de cada bloque esta en K y es menor que v.
2. Cada par de elementos de S aparecen juntos en exactamente λ de los bloques.

Lema 1.6.1. *Si existe un PBD (v, K, λ) con b_i bloques de tamaño k_i para cada $k_i \in K$, entonces*

$$\lambda v(v-1) = \sum b_i k_i (k_i - 1)$$

.

Demostración. Hay $\binom{v}{2} = \frac{1}{2}v(v-1)$ parejas de elementos, cada pareja aparece λ veces, dando $\frac{1}{2}\lambda v(v-1)$ parejas en el total de bloques. Por otra parte, cada bloque de tamaño k_i, contiene $\binom{k_i}{2} = \frac{1}{2}k_i(k_1 - 1)$ parejas, de tal manera que el número total de parejas en los bloques es por lo tanto $\sum_i \frac{1}{2}b_i k_i(k_i - 1)$. Por lo tanto

$$\lambda v(v-1) = \sum_i b_i k_i (k_i - 1)$$

□

El siguiente teorema relaciona a los diseños balanceados con los cuadrados latinos.

Teorema 1.6.1. *Si un PBD $(v, K, 1)$ existe, entonces*

$$N(v) \geq \min_{k \in K} N(k) - 1$$

Demostración. Sea $q = \min_{k \in K} N(k)$, entonces para cada $k \in K$ existen q $MOLS$ de orden k y por lo tanto un $OA(q+2, k)$ sobre $\{1, \ldots, k\}$. Sin perdida de generalidad supongamos que el primer renglón del $OA(q+2, k)$ es

$$11 \ldots 122 \ldots 2kk \ldots k$$

y que cualquier otro renglón comienza con $12 \ldots k$. Quitamos el primer renglón y las primeras k columnas de cada arreglo para obtener los arreglos D_k con $q+1$ renglones y $k(k-1)$ columnas en el que las parejas verticales en cualesquiera dos renglones son precisamente todos los pares ordenados de elementos distintos de $\{1, \ldots, k\}$. Sean los bloques del PBD $B_1, \ldots, B_b$. Para cada B, reemplazamos cada entrada i en $D_{|B|}$ por el i-ésimo elemento de B y denotamos al arreglo resultante por E_B. Ordenamos a todos los E_B's en un renglón y lo añadimos al arreglo

$$F = \begin{pmatrix} 1 & 2 & \dots & v \\ 1 & 2 & \dots & v \\ \vdots & & & \vdots \\ 1 & 2 & \dots & v \end{pmatrix}_{(q+1)\times v}$$

entonces $A = [E_{B_1} \dots E_{B_b} F]$ por el lema anterior tiene

$$v + \sum_{k_i \in K} b_i k_i (k_i - 1) = v + v(v-1) = v^2$$

columnas. Además es un $AO(q+1, v)$. Consideremos el i-ésimo y j-ésimo renglón. Para encontrar donde el par $(a, b)'$ aparece en estos renglones, hay que tener en cuenta que precisamente un bloque B contiene a a y b. En E_B, el par $(a, b)'$ aparecerá en el i-ésimo y j-ésimo renglón exactamente una vez y claramente no se encuentra fuera de E_B, Por lo tanto un $OA(q+1, v)$ existe y así $N(v) \geq q - 1$. □

Teorema 1.6.2. *Si un diseño $(k^2 - k + 1, k, 1)$ existe, entonces $N(k^2 - k + 1) \geq N(k)$.*

Usando un diseño $(21, 5, 1)$ por el teorema 1.6.2 se tiene que $N(21) \geq 4$ y usando un diseño (57,8,1) tenemos que $N(57) \geq 7$.

Si los bloques de tamaños en $\{k_1, \dots, k_r\}$ en un $PBD(v, k, 1)$ son todos disjuntos, entonces se dice que forman un **Conjunto Claro de Bloques**. El siguiente teorema dado por Bose en 1960 fortalece el teorema 1.6.1 dado por Parker.

Teorema 1.6.3. *Si existe un $PBD(v, k, 1)$ con $k = \{k_1, \dots, k_r, k_{r+1}, \dots, k_m\}$ donde no hay dos bloques de tamaños en $\{k_1, \dots, k_r\}$ que se intersecten, entonces*
$N(v) \geq min\{N(k_1), \dots, N(k_r), N(k_{r+1}) - 1, \dots, N(k_m) - 1)\}$.

Demostración. Sea $q = 1 + min\{N(k_1), \dots, N(k_r), N(k_{r+1}) - 1, \dots, N(k_m) - 1\}$, entonces para cada $i > r$ hay q $MOLS$ de orden k_i. Si todos tienen como primera fila a $12 \dots k$, podemos construir un $OA(q+2, k_i)$, a continuación eliminamos el primer renglón y las primeras k_i columnas, para obtener un arreglo P_i con $q+1$ renglones y $k_i(k_i - 1)$ columnas, en el que los pares verticales obtenidos por tomar cualesquiera dos renglones son precisamente todos los pares ordenados de elementos distintos de $\{1, \dots, k_i\}$. Ahora para cada $i \leq r$, definimos P_i como un $OA(q+1, k_i)$ correspondiente a $q-1$ $MOLS$ de orden k_i, cada uno tiene como primer renglón a $1, \dots, k_i$. Entonces cada P_i tiene $q+1$ renglones y P_i tiene k_i^2 columnas si $i \leq r$, pero $k_i^2 - k_i$ columnas si $i > r$.

Ahora tomemos cualquier bloque B_j del PBD, si éste es de tamaño k_i, reemplazamos cada h de P_i por el elemento h de B_j, a fin de obtener un arreglo C_j. Hacemos esto para cada $j = 1, \dots, b$. Finalmente queda

$$C = [C_1 C_2 \dots C_b F]$$

donde F tiene una columna constante para cada elemento del PBD, no en cualquier bloque del Conjunto Claro. El número de columnas es

$$\sum_{i\leq r} b_i k_i^2 + \sum_{i>r} b_i k_i(k_i-1) + v - \sum_{i\leq r} k_i b_i$$

donde b_i es el número de bloques de tamaño k, por el lema 1.4.2 éste es

$$\sum_{i=1}^{m} b_i k_i^2 - \sum_{i=1}^{m} b_i k_i + v = v + v^2 - v = v^2$$

Por lo que el número de columnas en C es v^2 y C es un arreglo de tamaño $(q+1)\times v^2$. Podemos afirmar que C es un $OA(q+1,v)$, de modo que $N(v)\geq q-1$ según sea necesario.

Consideremos cualesquiera dos renglones y cualesquiera dos elementos x, y de el PBD

Si $x=y$ el par $(x,y)'$ se presenta en F o en un C_j correspondiente a un bloque del Conjunto Claro que contiene a x. Si $x\neq y$, x y y se presentan en un único bloque B_j y el par $(x,y)'$ se presenta en C_j. □

Teorema 1.6.4. *Si $N(m)\geq k-1$ entonces existe un $PBD(km,\{k,m\},1)$ resoluble con $m+1$ clases de resolución, en el que el bloque de tamaño m, es una forma de las clases de resolución.*

Demostración. Como $N(m)\geq k-1$, entonces existe un $OA(k+1,m)$ cuyo primer renglón es

$$11\ldots122\ldots2\ldots mm\ldots m$$

Consideremos las m^2 columnas que se le asignó de m grupos, aquellos en el grupo i están los que tienen i, en la posición de la primera fila. Elimina el primer renglón del OA y sustituye cada i en la j-ésima fila que resulta por $i+(j-1)m$, esto da una matriz de km elementos $1,\ldots,km$.

Consideremos las columnas de éste arreglo como el bloque de un diseño, entonces tenemos un diseño de $v=km$ elementos con m^2 bloques, cada uno de tamaño k. Además por la propiedad de un OA los bloques en cada grupo contienen en su unión a cada elemento de $1,\ldots,km$ exactamente una vez, por lo que el diseño es resoluble con m clases de resolución, no es sin embargo balanceado, dado que no hay dos elementos de la forma $i+(j-1)m, i'+(j-1)m$ que puedan estar en el mismo bloque. Para obtener un diseño balanceado, añadimos k bloques $B_1,\ldots,B_k$. Definimos a $B_j=\{i+(j-1)m | 1\leq i\leq m\}$. Éstos bloques de tamaño m claramente forman una clase de resolución mas y junto con los bloques de tamaño k forman un $PBD(km,\{k,m\},1)$ con las propiedades requeridas. □

Ejemplo 1.6.1. *Sea $m=4$ y $k=3$. Los primeros dos cuadrados latinos del ejemplo 1.2.4 nos dan*

el siguiente $OA(4,4)$

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 & 3 & 3 & 3 & 3 & 4 & 4 & 4 & 4 \\ 1 & 2 & 3 & 4 & 1 & 2 & 3 & 4 & 1 & 2 & 3 & 4 & 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 & 2 & 1 & 4 & 3 & 3 & 4 & 1 & 2 & 4 & 3 & 2 & 1 \\ 1 & 2 & 3 & 4 & 4 & 3 & 2 & 1 & 2 & 1 & 4 & 3 & 3 & 4 & 1 & 2 \end{pmatrix}$$

Borramos el primer renglón, sumamos 4 a cada elemento del tercer renglón y 8 a cada entrada del cuarto renglón obteniendo

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

Tomamos a las columnas como bloques y también a los siguientes bloques $\{1,2,3,4\},\{5,6,7,8\}y\{9,10,11,12\}$ *, así obtenemos un* $PBD(12,\{3,4\},1)$ *resoluble.*

Corolario 1.6.1. *Si* $N(m) \geq k-1$ *y* $x < m$*, entonces*

a) Existe un $PBD(km+x,\{x,m,k,k+1\},1)$ *y*

b) $N(km+x) \geq \text{mín}\{N(m),N(x),N(k)-1,N(k+1)-1\}$

Demostración. Por el teorema anterior, existe un $PBD(km,\{k,m\},1)$ resoluble con $m+1$ clases de resolución. Sean $B_1,\ldots,B_k$ bloques de tamaño k que forman la clase $(m+1)$. Para cada $i \leq x$, añadimos a un nuevo elemento que es ∞, a cada bloque de la i-ésima clase de bloques de tamaño e introducimos un nuevo bloque $B_\infty = (\infty_1,\ldots,\infty_k)$. B_∞ es la partición del conjunto de elementos.

Si ni m, ni x son iguales a k o $k+1$, éstos $k+1$ bloques forman un Conjunto Claro y se sigue (b). En otros casos (b) se sigue manteniendo, ya que la función mínima rechaza a $N(m)$ y/o $N(x)$ de todas maneras. Note que si $x=1$ el resultado todavía se mantiene bajo la convención de que $N(1)=\infty$. □

Ejemplo 1.6.2.

- $N(62) = N(4\cdot 13+10)$ *de modo que* $k=4, m=13yx=10$*. Entonces* $N(13)=12 \geq k-1$ *de esto se sigue* $N(62) \geq \text{mín}\{N(13),N(10),N(4)-1,N(5)-1\} = 2$.
- $N(74) = N(4\cdot 16+10) \geq \text{mín}\{N(16),N(10),N(4)-1,N(5)-1\} = 2$.
- $N(86) = N(4\cdot 19+10) \geq \text{mín}\{N(19),N(10),N(4)-1,N(5)-1\} = 2$.
- $N(100) = N(7\cdot 13+9) \geq \text{mín}\{N(13),N(9),N(7)-1,N(8)-1\} = 5$.

Como observamos, varios de los ejemplos usan el inciso (b) del corolario anterior con $k=4$. De este valor de k obtenemos el siguiente teorema.

Teorema 1.6.5. *Si $N(m) \geq 3$, $N(x) \geq 2$ y $1 \leq x < m$, entonces $N(4m + x) \geq 2$.*

Lema 1.6.2. $N(4t) \geq 3$ *para todo* $t \geq 1$.

Demostración. Por el teorema Moore-MacNeish $N(4t) \geq 3$, excepto posiblemente cuando t es divisible por 3, pero no por 9. Para hacer frente a éstos casos, escribimos $4t = 2^{2a+b}3u$ donde $(u, 6) = 1$ y $b = 2$ ó 3.

Si $u2^{2a} \neq 1$, entonces $N(u2^{2a}) \geq 3$, de modo que $N(4t) \geq min\{N(3 \cdot 2^b), 3\}$, en cualquier caso necesitamos solamente probar que $N(12) \geq 3$ y $N(24) \geq 3$. □

Ahora podemos probar el teorema principal.

Teorema 1.6.6. $N(n) \geq 2$ *para todo entero positivo* $n \neq 2$ *ó 6.*

Demostración. En vista del teorema 2.3 sólo es necesario considerar $n \equiv 2($ mód 4). Cualquier n puede escribirse como $n = 16k+y = 16(k-1)+(16+y)$ donde $y = 2$,6,10 ó 14, pero $N(16+y) \geq 2$ para cada y
$N(18) \geq 2$, $N(22) \geq 2$, $N(26) \geq 2$, $N(30) \geq$ mín$\{N(3), N(10)\} = 2$. Así por el teorema 2.11 y el lema 2.1
$N(16k+y) = N(4, 4(k-1)+(16+y)) \geq 2$, siempre que $k-1 \geq 1$ y $16+y < 4(k-1)$, es decir, siempre que $k \geq 2$ y $4k - 3 > 30$, es decir, siempre que $k \geq 9$. Todo lo que queda por hacer es verificar que $N(n) \geq 2$ para todo $n \equiv 2($ mód 4), $6 < n < 144$. Todos los $n \leq 30$ ya se han discutido. Del resto se ocupa el corolario 2.2 con 34,46,58,70,82,94,106,118,130,142.Finalmente $42 = 3 \times 14$, $50 = 5 \times 10$, $54 = 3 \times 18$, $66 = 3 \times 22$, $78 = 3 \times 26$, $90 = 3 \times 30$, $98 = 7 \times 14$, $102 = 3 \times 34$, $110 = 10 \times 11$, $114 = 4 \times 38$, $122 = 4 \times 27 + 14$, $126 = 3 \times 42$, $134 = 4 \times 27 + 26$, $138 = 4 \times 46$ son tratados como el resto. □

Ahora se ha establecido que $N(n) \geq 2$ para todo $n \neq 2$ ó 6. Claramente $N(2) = 1$. El hecho que $N(6) = 1$ se demostrara en la siguiente sección.

1.6.1. No existen dos $MOLS$ de orden 6

El número 6 es la única excepción del resultado general $N(n) \geq 2$ para todo $n > 2$. Recordemos que el problema de los oficiales de Euler es equivalente al problema de la existencia de dos $MOLS$ de orden 6 y que la conjetura de Euler nos dice que tales $MOLS$ no existen. En esta sección presentamos la prueba dada por Stinson (1984) de que efectivamente no existen dos $MOLS$ de orden 6.

Supongamos que existen dos $MOLS$ de orden 6, entonces existe un $OA(4, 6)$. Tomemos un OA sobre $\{1, \ldots, 6\}$ y siguiendo el proceso de la demostración del Teorema 1.6.4 añadimos 6 a cada entrada del segundo renglón, 12 a cada entrada del tercer renglón y 18 a cada entrada del cuarto

renglón. Entonces las 36 columnas podemos verlas como 36 bloques $B_1, \ldots, B_{36}$ cada uno de tamaño 4 y cada uno contiene precisamente un elemento de cada uno de los siguientes conjuntos

$$G_1 = \{1, \ldots, 6\}, G_2 = \{7, \ldots, 12\}, G_3 = \{13, \ldots, 18\}, G_4 = \{19, \ldots, 24\}.$$

Estos conjuntos G_i y B_i son los grupos y los bloques de un diseño de grupos divisible, si tomamos a los grupos como 4 bloques más. $G_1 = B_{37}, \ldots, G_4 = B_{40}$, entonces los conjuntos $B_1, \ldots, B_{40}$ son los bloques de un $PBD(24, \{4, 6\}, 1)$ sobre $X = \{1, \ldots, 24\}$ que denotaremos como P. Entonces cada elemento sobre X esta en exactamente un G_i y en otros $\frac{1}{3}(18) = 6$ bloques más, es decir, en siete bloques en total.

Sea $M = (m_{ij})$ es la matriz de incidencia de P, entonces M tiene 40 renglones y 24 columnas. Denotamos a las columnas de M como $c_1, \ldots, c_{24}$ donde $c_i^{'} = (m_{1i}, \ldots, m_{40i})$ y definimos a C como el espacio vectorial sobre $GF(2)$ generado por $c_1, \ldots, c_{24}$ (C consiste en todas las combinaciones lineales sobre $GF(2)$ de $c_1, \ldots, c_{24}$).

Lema 1.6.3. *La dimensión de C es a lo más 20.*

Demostración. Dado que P es balanceado con $\lambda = 1$, tenemos $c_i \cdot c_j = 1$ siempre que $i \neq j$, pero $c_i \cdot c_i = 7 \equiv 1 (\bmod 2)$ para todo i, por lo que $c_i \cdot (c_j + c_k) = 0$ en $GF(2)$ para cualquier elección de i, j, k.

Supongamos que C tiene dimensión d, de tal manera $c_1, \ldots, c_d$ forman una base para C. Entonces $c_1 + c_2, c_1 + c_3, \ldots, c_1 + c_d$ son ortogonales para cada c_i . Por lo tanto están en el espacio dual de $C^{\perp}$ y además son linealmente independientes por lo cual se sigue que $dim(C^{\perp}) \geq d - 1$, es decir, $dim(C^{\perp}) \geq dim(C) - 1$. Además, por otra parte

$$dim(C) + dim(C^{\perp}) = 40 \text{ entonces } dim(C) \leq 20.$$

Y como M tiene 24 columnas, hay al menos cuatro relaciones de dependencia entre ellas. Una dependencia entre las columnas corresponden a un conjunto Y de elementos que cumplen $|B_j \bigcap Y| = 0 (\bmod 2)$ para todo $j \leq 40$. Llamaremos a tal Y un **subconjunto par** de $x = 1, \ldots, 24$. Por ejemplo, un subconjunto par Y es $B_{37} \bigcup B_{38}$, ya que

$$|B_i \bigcap (B_{37} \bigcup B_{38})| = \begin{cases} 6 & \text{si } i = 37 \quad \text{o } 38 \\ 0 & \text{si } i = 39 \quad \text{o } 40 \\ 2 & \text{si } i \leq 36 \end{cases}$$

Similarmente $B_{37} \bigcup B_{39}$ y $B_{37} \bigcup B_{40}$ son también subconjuntos pares. Al igual que $B_{39} \bigcup B_{40}$, pero esté ya esta implícito en los anteriores. Así que tres relaciones de dependencia independientes entre las columnas ya han sido expuestos y el lema dice que debe haber otra. La prueba para $N(6) = 1$ se realiza ahora demostrando que no puede existir otra relación de dependencia.

Supongamos que existe otro subconjunto par Y independiente a los ya dados. Sea $|Y| = m$, como el complemento de un subconjunto par es también par podemos asumir que $m \leq 12$. Supongamos que hay b_0 valores de i para $|B_i \bigcap Y| = 0$, b_2 para $|B_i \bigcap Y| = 2$, b_4 para $|B_i \bigcap Y| = 4$ y b_6 para $|B_i \bigcap Y| = 6$, entonces

$$b_0 + b_2 + b_4 + b_6 = 40 \ldots (1)$$

y dado que cada elemento esta en exactamente siete bloques

$$2b_2 + 4b_4 + 6b_6 = 7m \ldots (2)$$

y además, puesto que $\lambda = 1$

$$b_2 + 6b_4 + 15b_6 = \frac{1}{2}m(m-1) \ldots (3).$$

Por (2) y (3)

$$\frac{7}{2}m - 2b_4 - 3b_6 = \frac{1}{2}m(m-1) - 6b_4 - 15b_6$$

, es decir,

$$b_4 + 3b_6 = \frac{m(m-8)}{8} \ldots (4).$$

Dado que $m \leq 12$ y $\frac{1}{8}m(m-8)$ son enteros, solo existen dos posibles valores para m, que son 8 y 12. Estas dos posibilidades las consideraremos de manera separada y se mostrara que ambas son imposibles.

CASO I. $m = 8$.

Si $m = 8$ las relaciones (1) y (4) nos dan $b_4 = 0, b_6 = 0, b_2 = 28, b_0 = 12$. Tenemos que 12 bloques son disjuntos de Y y 28 bloques intersectan a Y en 2 elementos. Y no pude tener mas de dos elementos de cualquiera de los cuatro grupos $B_{37}, \ldots, B_{40}$. Por lo que debe tener precisamente 2 elementos de cada uno de los 4 grupos.

Si ahora eliminamos los elementos de Y de los bloques B_i obtenemos un nuevo diseño Q sobre 16 elementos que tiene a los 12 bloques de P disjuntos a Y que no se alteran, los bloques $B_{37}, \ldots, B_{40}$ dan 4 bloques de tamaño 4 a Q y los restantes 24 bloques de P dan 24 bloques de tamaño 2 a Q, así se establece el siguiente lema.

Lema 1.6.4. *Q es un $PBD(16, \{4, 2\}, 1)$ con 16 bloques de tamaño 4 y 24 bloques de tamaño 2.*

Por conveniencia, renombramos a los elementos de P de tal manera que $Y = \{a, b, \ldots, h\}$, los elementos de Q son $1, \ldots, 16$ y los grupos de P son $B_{37} = \{1, \ldots, 4, a, b\}, B_{38} = \{5, \ldots, 8, c, d\}, B_{39} = \{9, \ldots, 12, e, f\}, B_{40} = \{13, \ldots, 16, g, h\}$.

Lema 1.6.5. *Cada $i \leq 16$ pertenece a tres bloques de Q de tamaño 2, es decir, $\{i, j\}, \{i, k\}, \{i, l\}$ donde i, j, k, l pertenecen a diferentes grupos.*

Demostración. Supongamos que i se encuentra en u bloques de tamaño 2 y v bloques de tamaño 4, entonces $u + v = 7$ y dado que $\lambda = 1$, $u + 3v = 15$, por lo tanto $u = 3$. Así cada elemento $i \geq 16$ pertenece a tres bloques de tamaño 2 , ahora estos tres bloques surgen de tres bloques de P,cada uno de los cuales contiene a i , dos elementos de Y y otro elemento. Ya que estos bloques de P no tienen mas de un elemento de cualquier grupo . Podemos suponer que $i \in B_{37}$ y que los tres bloques de P son $\{i, c, e, j\}, \{i, d, g, k\}, \{i, f, h, l\}$. Así j, k, l deben pertenecer a B_{40}, B_{39}, B_{38} respectivamente.

Estudiaremos a Q mediante la construcción de una gráfica G con 16 vértices etiquetados como $1, \ldots, 16$ (los elementos de Q) y con dos vértices unidos por una arista si y sólo si sus etiquetas forman un bloque de Q de 2-elementos. Vamos a identificar a los vértices con sus etiquetas. Entonces por el lema 2.4 G es regular de grado 3, es decir, en cada vértice de G se intersectan 3 aristas de G. □

Lema 1.6.6. *G no tiene triángulos*

Demostración. Si G tiene un triángulo ,por el lema 2.4 sus vértices deben de pertenecer a diferentes grupos, entonces decimos que G tiene a los siguientes bloques $\{1, 5, e, g\}$ y $\{1, 9, c, h\}$, pero esto no es posible, ya que ambos no satisfacen la condición de $\lambda = 1$. □

Lema 1.6.7. *Para cada $i \leq 16$, no hay un bloque de P que contenga a los tres vértices de G adyacentes a i.*

Demostración. Supongamos que 1 es adyacente a 5,9, 13 en G y que $\{2, 5, 9, 13\}$ es un bloque de P. Los bloques que contienen a 1 pueden tomarse como
$\{1, 5, e, g\}, \{1, 9, c, h\}, \{1, 13, d, f\}, B_{37}, \{1, 6, 10, 14\}, \{1, 7, 11, 15\}$ y $\{1, 8, 12, 16\}$, por lo tanto podemos suponer que $\{2, 6, 11, 16\}$ y $\{2, 7, 12, 14\}$ son bloques. Por lo que 2 debe de estar con 8,10 y 15 en otros bloques , de modo que 2 es adyacente a 8,10 y 15 en G. Recordemos que 12 bloques de P son disjuntos con Y, de estos 6 ya han sido mencionados y los otros seis contienen a 3 o 4 y a uno de 5,9 y 13, es decir,

$$\{3, 5, \_, \_\}, \{4, 5, \_, \_\}, \{3, \_, 9, \_\}, \{4, \_, 9, \_\}, \{3, \_, \_, 13\}, \{4, \_, \_, 13\}.$$

Observemos ahora que 2 aun no se ha presentado en un bloque con 8, 10 o 15, de modo que 2 debe de ser adyacente con 8, 10 y 15 en G, de esta manera {8,10},{8,15},{10,15} no son pares de vértices unidos por una arista en G(de otro modo formarían un triángulo) ,por lo que estos tres pares deben de pertenecer a bloques de tamaño 4, por lo que deben de llenar los vacíos en tres de los seis bloques incompletos descritos anteriormente, pero no hay manera de que encajen sin romper la condición $\lambda = 1$. □

Lema 1.6.8. *Para cada $i \leq 16$, los tres pares formados por los tres vértices adyacentes a i en G pertenecen a diferentes bloques de P.*

Demostración. Si i es adyacente a j, k, l en G y $\{j, k\}$ y $\{j, l\}$ pertenecen al mismo bloque de P, entonces j, k, l se encuentran todos en el bloque, contradiciendo el lema anterior. □

Ahora es posible tratar con el caso $m = 8$, reetiquetando de nuevo, pero manteniendo los grupos como $B_{37} = \{1, \ldots, 4, a, b\}, B_{38} = \{5, \ldots, 8, c, d\}, B_{39} = \{9, \ldots, 12, e, f\}, B_{40} = \{13, \ldots, 16, g, h\}$. Supongamos que en G , 1 es adyacente a 5,9,13; 2 es adyacente a 6,10, 4; 3 es adyacente a 7,11,15 y 4 es adyacente a 8,12,16. Sin pérdida de generalidad supongamos que el bloque que contiene a 6 y 10 es $\{1, 6, 10, 15\}$. Ahora debe de haber dos bloques de la forma $\{1, 7, \_, \_\}$ y $\{1, 8, \_, \_\}$ y como 1 apareció con 9, 10 y 8, éste ya no puede presentarse con 12, entonces se deduce del lema anterior que estos bloques deben ser $\{1, 7, 12, 14\}$ y $\{1, 8, 11, 16\}$. Ahora los elementos 5 y 9 deben de pertenecer juntos en algunos bloques de 4-elementos.

Si fuera $\{2, 5, 9, j\}$ entonces j no puede ser 13 (por el lema 2.6) o 14, de modo que j=15 o 16. Si $\{2, 5, 9, 15\}$ es un bloque ,entonces el resto de los bloques de tamaño 4 que contienen a 2 son $\{2, 7, 11, \_\}$ y $\{2, 8, 12, \_\}$ donde faltan los elementos 13 y 16, y como 11 ya apareció con 16, entonces los bloques deben ser $\{2, 7, 11, 13\}$ y $\{2, 8, 12, 16\}$,pero 8,12,16 no satisfacen el lema 2.6. De tal manera que m no puede ser igual a 8.

CASO II $m = 12$

Para este caso los 12 elementos de Y tienen que ser distribuidos entre los cuatro grupos $B_{37}, \ldots, B_{40}$ con un número par en cada uno. La siguiente tabla muestra las diferentes posibilidades.

	B_{37}	B_{38}	B_{39}	B_{40}
(a)	6	6	0	0
(b)	6	4	2	0
(c)	6	2	2	2
(d)	4	4	4	0
(e)	4	4	2	2

En el (a) Y es justamente $B_{37} \bigcup B_{38}$, una posibilidad que ya se considero. En (b) $Y + (B_{37} \bigcup B_{38})$ es entonces otro subconjunto par de tamaño 4, contradiciendo el hecho de que m debe de ser 8 o 12(o 16). De manera similar para los casos (c),(d) y (e) llevan a otros subconjuntos par de tamaño 8, pero esta posibilidad ya fue rechazada.

Por lo que se ha establecido el resultado de Tarry. □

Teorema 1.6.7. *No existen dos MOLS de orden 6.*

CAPÍTULO 2

Aplicaciones de los Cuadrados Latinos

En este capítulo mostraremos algunas de las aplicaciones de los cuadrados latinos, es sorprendente la gran variedad de áreas matemáticas en donde dichos cuadrados ofrecen resultados importantes, por ejemplo, en la estadística, la teoría de gráficas y la criptología.

2.1. Cuadrados Mágicos

En esta sección presentamos el uso de los cuadrados latinos diagonales en la construcción de cuadrados mágicos.

Un **Cuadrado Mágico** es una matriz de tamaño $n \times n$ de enteros con la propiedad de que la suma de los números en cada renglón, cada columna y en las diagonales principales es la misma. El cuadrado es de orden n si los enteros son enteros consecutivos de 1 a n^2. La suma es llamada **número mágico** y la denotaremos como S_n. Donde $S_n = \frac{1}{2}n(n^2+1)$.

Ejemplo 2.1.1. *Cuadrado Mágico de orden 4 y 6*

16	*3*	*2*	*13*
5	*10*	*11*	*8*
9	*6*	*7*	*12*
4	*15*	*14*	*1*

35	*1*	*6*	*26*	*19*	*24*
3	*32*	*7*	*21*	*23*	*25*
31	*9*	*2*	*22*	*27*	*20*
8	*28*	*33*	*17*	*10*	*15*
30	*5*	*34*	*12*	*14*	*16*
4	*36*	*29*	*13*	*18*	*11*

$$S_4 = \frac{1}{2}4(4^2+1) = 34 \qquad S_6 = \frac{1}{2}6(6^2+1) = 111$$

Veremos un poco de historia de algunas variaciones de estas estructuras, que también llamaremos cuadrados mágico. El diagrama Lo Shu es el más antiguo ejemplo conocido de un cuadrado mágico en el mundo. Según la leyenda, en los tiempos antiguos en China hubo un desbordamiento en el río Lo; la gente, temerosa, intentó hacer una ofrenda al dios del río para calmar su ira mediante sacrificios. Sin embargo, cada vez que lo hacían, aparecía una tortuga que rondaba la ofrenda sin aceptarla, hasta que un niño se dio cuenta de que las peculiares marcas del caparazón de la tortuga formaban un patrón. Después de estudiar éstas marcas, la gente se dio cuenta de la cantidad correcta de sacrificios era 15, quedando el dios satisfecho y volviendo las aguas a su cauce. Los números en

Figura 2.1: Lo-shu

cada fila, arriba y abajo, a través, o en diagonal, suman 15, que pasa a ser el número de días que tarda la luna nueva para convertirse en una luna llena. El diagrama Lo Shu se remonta hasta 5600 años, según algunas estimaciones.

También se pueden encontrar cuadrados mágicos en el arte. El más famoso está incluido en un grabado de Alberto Durero, llamado Melancolía. En este cuadrado mágico de orden cuatro se obtiene la constante mágica (34) en filas, columnas, diagonales principales, y en las cuatro submatrices de orden 2 en las que puede dividirse el cuadrado, sumando los números de las esquinas, los cuatro números centrales, los dos números centrales de las filas (o columnas) primera y última, etc. y siendo las dos cifras centrales de la última fila 1514 el año de ejecución de la obra.

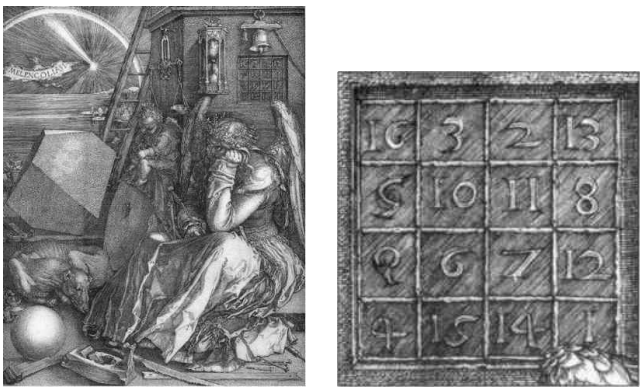


Figura 2.2: Alberto Durero. Melancolía

Otro cuadrado mágico es el que se encuentra en la fachada del templo de la Sagrada Familia, iniciado por el arquitecto Gaudí, en Barcelona. Cuyo número mágico es 33, edad en la que Jesucristo fue crucificado.

Figura 2.3: Sagrada Familia. Josep Maria Subirach.

Ahora les mostraremos el método desarrollado por Leonhard Euler en 1782 para construir cuadrados mágicos, utilizando cuadrados latinos (ver [16]).

Sean L_1 y L_2 dos cuadrados latinos ortogonales de orden n con conjunto base $S = \{0, 1, 2, \ldots, n-1\}$, definimos las entradas de la matriz M de la siguiente forma

$$M(i,j) = nL_1(i,j) + L_2(i,j)$$

como L_1 y L_2 son ortogonales, todas las posibles combinaciones de los elementos de S aparecen exactamente una vez en M. Ahora es suficiente sumar 1 a cada elemento de M para obtener una

nueva matriz CM que contiene a todos los números entre 1 y n^2. Verifiquemos que la suma de los elementos de cualquier fila o columna de CM es igual al número mágico.

Sumemos los elementos del i-ésimo renglón de CM

$$\begin{aligned}\sum_{j=1}^{n} CM(i,j) &= \sum_{j=1}^{n} M(i,j) + 1 \\ &= \sum_{j=1}^{n} nL_1(i,j) + L_2(i,j) + 1 \\ &= n\sum_{j=1}^{n} L_1(i,j) + \sum_{j=1}^{n} L_2(i,j) + \sum_{j=1}^{n} 1\end{aligned}$$

ahora

$$\sum_{j=1}^{n} L_1(i,j) = \sum_{j=1}^{n} L_2(i,j) = \frac{(n-1)((n-1)+1)}{2} = \frac{n(n-1)}{2}$$

ya que por ser L_1 y L_2 cuadrados latinos en cada renglón aparecen exactamente una vez cada uno de los elementos del conjunto $\{0, 1, 2, \ldots, n-1\}$, por lo que se están sumando los números del 1 hasta $n-1$. Entonces

$$\begin{aligned}\sum_{j=1}^{n} CM(i,j) &= n\left(\frac{n(n-1)}{2}\right) + \frac{n(n-1)}{2} + n \\ &= \frac{n(n-1)}{2}(n+1) + n \\ &= \frac{n(n^2-1)}{2} + n \\ &= n\left(\frac{(n^2-1)}{2} + 1\right) \\ &= n(\frac{n^2}{2} - \frac{1}{2} + 1) \\ &= \frac{1}{2}n(n^2+1)\end{aligned}$$

Como observamos la suma de los elementos del i-ésimo renglón es igual al número mágico y por ser i arbitrario se cumple para todos los renglones de CM. De manera análoga se muestra que la suma de los elementos de cualquier columna de CM es igual al número mágico.

Este método garantiza que la suma de los elementos de cualquier fila o columna de CM es igual al número mágico. Pero la suma de los elementos de las diagonales principales no siempre es igual al número mágico. De tal manera que para que esto último se cumpla se deben hacer las permutaciones necesarias de filas y columnas hasta que las diagonales principales satisfagan la propiedad.

Ejemplo 2.1.2. *Construyamos un cuadrado mágico de orden 3, que tendrá por elementos* $\{1, 2, \ldots, 9\}$.

Primero construyamos dos cuadrados latinos ortogonales. Mediante la demostración del Teorema 1.2.1 sabemos que

$$L_1(i,j) \equiv j - i + 1 \,(\mathrm{mod}\, 3) \quad y \quad L_2(i,j) \equiv j + i - 1 \,(\mathrm{mod}\, 3)$$

nos producen cuadrados latinos ortogonales.

$$L_1 = \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 2 \\ 2 & 0 & 1 \end{pmatrix} \; L_2 = \begin{pmatrix} 1 & 2 & 0 \\ 2 & 0 & 1 \\ 0 & 1 & 2 \end{pmatrix}$$

Ahora con L_1 *y* L_2 *construimos a la matriz* M *de la siguiente manera*

$$M(i,j) = 3L_1(i,j) + L_2(i,j)$$

quedando como sigue

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

Sumamos 1 *en cada entrada del cuadrado obtenido*

$$M' = \begin{pmatrix} 5 & 9 & 1 \\ 3 & 4 & 8 \\ 7 & 2 & 6 \end{pmatrix}$$

donde $S_3 = 15$. *Como observamos la diagonal inversa no suma el número mágico correspondiente, por lo que haremos las siguientes permutaciones*

1. *el primer renglón con el segundo.*
2. *la primera columna con la segunda columna.*

Por lo tanto el cuadrado mágico de orden 3 es

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

Ejemplo 2.1.3. *Ahora construyamos un cuadrado mágico de orden 4, que tendrá por elementos* $1, 2, \ldots, 16$. *Sean* L_1 *y* L_2 *dos cuadrados latinos ortogonales de orden 4*

$$L_1 = \begin{pmatrix} 1 & 2 & 3 & 0 \\ 2 & 1 & 0 & 3 \\ 3 & 0 & 1 & 2 \\ 0 & 3 & 2 & 1 \end{pmatrix} \; L_2 = \begin{pmatrix} 1 & 2 & 3 & 0 \\ 0 & 3 & 2 & 1 \\ 2 & 1 & 0 & 3 \\ 3 & 0 & 1 & 2 \end{pmatrix}$$

Ahora con L_1 y L_2 construyamos a la matriz M de la siguiente manera

$$M(i,j) = 4L_1(i,j) + L_2(i,j)$$

quedando como sigue

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

Sumemos 1 a cada entrada de M

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

Observemos que todos los renglones y columnas suman 34, excepto las diagonales principales, así que tendremos que hacer algunas permutaciones de filas y columnas para obtener al cuadrado mágico que satisfaga esta propiedad.
1.- Permutamos la columna 1 con columna 2.
2.- Permutamos la columna 2 con la columna 3.
3.- Permutamos la columna 3 con la columna 4.
4.- Permutamos el renglón 2 con el renglón 3.
Quedando de esta manera el cuadrado mágico que satisface que la suma de los elementos en cada columna, renglón y diagonales principales suman 34.

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

Como observamos el problema que se presenta en la construcción del cuadrado mágico anterior es que se tienen que hacer permutaciones de filas y renglones para que las diagonales del cuadrado mágico también sumen 34.

De tal manera que necesitamos que los cuadrados latinos ortogonales deben de tener elementos distintos en ambas diagonales, a este tipo de cuadrados latinos los llamaremos **Cuadrados Latinos Diagonales**.

Teorema 2.1.1. *Si n es impar y no es múltiplo de 3, entonces existe un cuadrado latino diagonal de orden n.*

Demostración. Primero mostremos que si $a > b$ son enteros positivos con la propiedad de que $a, b, a+b, a-b$ son todos primos relativos con n, entonces la siguiente matriz es un cuadrado latino

diagonal.

$$L = \begin{pmatrix} 0 & a & 2a & \cdots & (n-1)a \\ b & b+a & b+2a & \cdots & b+(n-1)a \\ 2b & 2b+a & 2b+2a & \cdots & 2b+(n-1)a \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ (n-1)b & (n-1)b+a & (n-1)b+2a & \cdots & (n-1)b+(n-1)a \end{pmatrix}$$

Como observamos los elementos de L en sus renglones $0 \leq i \leq n-1$ y columnas $0 \leq j \leq n-1$ están definidos de la siguiente manera

$$ib + ja$$

Los elementos en cada renglón son distintos. Supongamos que existen dos elementos del i-ésimo renglón que se repiten, entonces

$$\begin{aligned} ib + ja &\equiv ib + ka \,(\mathrm{mod}\, n) \;\text{ para }\; j \neq k \\ ja &\equiv ka \,(\mathrm{mod}\, n) \\ (j-k)a &\equiv 0 \,(\mathrm{mod}\, n). \end{aligned}$$

Sabemos que $(n, a) = 1$ y que $0 \leq j, k \leq n-1$, entonces $j = k$, lo cual es una contradicción.

De forma análoga se demuestra que los elementos en cada una de las columnas son distintos.

Ahora demostremos que los elementos en la diagonal principal son distintos, nuevamente supongamos que existen dos que son iguales, entonces tendríamos

$$\begin{aligned} ib + ia &\equiv jb + ja \,(\mathrm{mod}\, n) \\ i(b+a) &\equiv j(b+a) \,(\mathrm{mod}\, n) \\ (i-j)(b+a) &\equiv 0 \,(\mathrm{mod}\, n) \end{aligned}$$

por hipótesis tenemos que $(b+a, n) = 1$, entonces $(i-j) = 0$. Por lo tanto $i = j$. Sabemos que esta es una contradicción. Por lo tanto los elementos de la diagonal principal son distintos. De forma similar se muestra que los elementos de la diagonal inversa son distintos, utilizando la hipótesis $(a-b, 1) = 1$. □

Teorema 2.1.2. *Si n es impar y no es múltiplo de 3, entonces existe un par de cuadrados latinos diagonales mutuamente ortogonales.*

Demostración. Supongamos que $a > b$ son enteros positivos con la propiedad de que $a, b, a+b, a-b$ son todos primos relativos con n. En el teorema anterior se definió un cuadrado latino diagonal L. Sea L^T la matriz transpuesta de L. L^T es también un cuadrado latino. Demostremos que L y L^T son ortogonales.

Supongamos que no lo son, es decir, existe un par de coordenadas distintas (i_1, j_1) y (i_2, j_2) tales que

$$\begin{aligned}(i_1b + j_1a, i_1a + j_1b) &= (i_2b + j_2a, i_2a + j_2b)\\ i_1b + j_1a &= i_2b + j_2a\\ i_1a + j_1b &= i_2a + j_2b\end{aligned}$$

De tal manera que $i_1 = i_2$ y $j_1 = j_2$, lo cual es una contradicción. Por lo tanto L y L^T son ortogonales. □

Ejemplo 2.1.4. *Construyamos el cuadrado mágico de orden* 7*.*

Sean $n = 7, a = 3, b = 2, a - b = 1, a + b = 5$*. Entonces el cuadrado latino diagonal de orden 7 y su transpuesto obtenidos mediante la construcción de la demostración de los teoremas anteriores son*

$$L = \begin{pmatrix} 0 & 3 & 6 & 2 & 5 & 1 & 4\\ 2 & 5 & 1 & 4 & 0 & 3 & 6\\ 4 & 0 & 3 & 6 & 2 & 5 & 1\\ 6 & 2 & 5 & 1 & 4 & 0 & 3\\ 1 & 4 & 0 & 3 & 6 & 2 & 5\\ 3 & 6 & 2 & 5 & 1 & 4 & 0\\ 5 & 1 & 4 & 0 & 3 & 6 & 2 \end{pmatrix} \quad y \quad L^T = \begin{pmatrix} 0 & 2 & 4 & 6 & 1 & 3 & 5\\ 3 & 5 & 0 & 2 & 4 & 6 & 1\\ 6 & 1 & 3 & 5 & 0 & 2 & 4\\ 2 & 4 & 6 & 1 & 3 & 5 & 0\\ 5 & 0 & 2 & 4 & 6 & 1 & 3\\ 1 & 3 & 5 & 0 & 2 & 4 & 6\\ 4 & 6 & 1 & 3 & 5 & 0 & 2 \end{pmatrix}$$

Entonces el cuadrado mágico de orden 7 obtenido de L *y* $L^{\perp}$ *es*

$$\begin{pmatrix} 1 & 24 & 47 & 21 & 37 & 11 & 34\\ 18 & 41 & 8 & 31 & 5 & 28 & 44\\ 35 & 2 & 25 & 48 & 15 & 38 & 12\\ 45 & 19 & 42 & 9 & 32 & 6 & 22\\ 13 & 29 & 3 & 26 & 49 & 16 & 39\\ 23 & 46 & 20 & 36 & 10 & 33 & 7\\ 40 & 14 & 30 & 4 & 27 & 43 & 17 \end{pmatrix}$$

$$S_7 = 175$$

Sabemos que no existe un par de $MOLS$ de orden 6, pero a continuación mostramos un cuadrado mágico de orden 6, mismo que no puede ser construido mediante $MOLS$.

Ejemplo 2.1.5. *Cuadrado mágico de orden 6.*

34	*0*	*5*	*25*	*18*	*23*
2	*31*	*6*	*20*	*22*	*24*
30	*8*	*1*	*21*	*26*	*19*
7	*27*	*32*	*16*	*9*	*14*
29	*4*	*23*	*11*	*13*	*15*
3	*35*	*28*	*12*	*17*	*10*

2.2. Sudoku

El juego del **Sudoku** consiste en llenar una cuadrícula de 9×9 celdas (81 casillas) dividida en subcuadrículas de 3×3 con números del 1 al 9 partiendo de algunos números ya dispuestos en algunas de las celdas de tal manera que cada renglón, columna y subcuadrícula contenga a los números del 1 al 9 exactamente una vez.

Ejemplo 2.2.1. *Sudoku con 17 entradas dadas.*

							1	
4								
	2							
				5		4		7
		8				3		
		1		9				
3			4			2		
	5		1					
			8		6			

Algunas fuentes indican que el origen del juego puede situarse en Nueva York a finales de los años 1970. Entonces no se llamaba Sudoku sino simplemente Number Place (El lugar de los números). Posteriormente en los años 80 llega a Japón donde se publica en el periódico Monthly Nikolist en abril de 1984 bajo el título "Suji wa dokushin ni kagiru", que se puede traducir como "los números deben estar solos". Fue Kaji Maki, presidente de Nikoli, quien le puso el nombre. El nombre se abrevió a Sudoku (su = número, doku = solo).

Observemos que la solución de un Sudoku es un cuadrado latino de orden 9, pero no todo cuadrado latino de orden 9 es solución de un Sudoku dado que no todos los cuadrados latinos cumplen la condición de que en cada subcuadrícula aparecen los número del 1 al 9 exactamente una vez.

Ejemplo 2.2.2. *Solución del Sudoku de orden 9 del ejemplo anterior.*

6	9	3	7	8	4	5	**1**	2
4	8	7	5	1	2	9	3	6
1	**2**	5	9	6	3	8	7	4
9	3	2	6	**5**	1	**4**	8	**7**
5	6	**8**	2	4	7	**3**	9	1
7	4	**1**	3	**9**	8	6	2	5
3	1	9	**4**	7	5	**2**	6	8
8	**5**	6	**1**	2	9	7	4	3
2	7	4	**8**	3	**6**	1	5	9

Generalizando, tenemos que un Sudoku de orden n^2 consiste en llenar una cuadrícula de $n^2 \times n^2$ celdas dividida en subcuadrículas de $n \times n$ con números del 1 al n^2 partiendo de algunos números ya dispuestos en algunas de las celdas de tal manera que cada renglón, columna y subcuadrícula contenga a los números del 1 al n^2 exactamente una vez. De tal manera que a la solución de un Sudoku la llamaremos **cuadrado latino Sudoku** de orden n^2 o simplemente SLS de orden n^2.

Diremos que un cuadrado latino de orden n^2 tiene la **propiedad S** si y sólo si es un SLS.

Una cota superior para la cardinalidad del conjunto de cuadrados latinos Sudoku mutuamente ortogonales ($MOSLS$) de orden n^2 es $n^2 - n$, ya que si suponemos que los cuadrados latinos en el conjunto de $MOSLS$ están en forma estándar entonces la entrada $(2, 1)$ está en la primera subcuadrícula de cada cuadrado, los elementos del 1 al n ya aparecen en el primer renglón y dado que los cuadrados tienen que ser ortogonales no pueden tener el mismo valor en esa posición. Por lo que el número de los posibles valores para el elemento $(2, 1)$ es a lo más $n^2 - n$.

Ejemplo 2.2.3. *Para cuadrados latinos Sudoku de orden 4 podemos tener como máximo* $2^2 - 2 = 2$ *$MOSLS$.*

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

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

2.2.1. Construcción de un conjunto máximo de $MOSLS$ de orden k para k potencia de un primo

Las ideas desarrolladas en esta subsección se basan en el artículo realizado por Ryan M. Pedersen y Timothy L. Vis. [10].

Sea k una potencia de un primo, K el campo finito de orden k^2 y F el subcampo de K de orden k. Dado que el grupo aditivo de F es un subgrupo del grupo aditivo de K las clases laterales de F determinan una partición de K. Etiquetemos estas clases como P_i y c_i denotara un representante de la clase P_i para $0 \leq i \leq k-1$. Ahora para cada par ordenado (i, j) el cuadrado latino $B_{i,j}$ es la tabla de adición de F sobre los símbolos de P_m donde $c_m + F = (c_i + c_j) + F$. Entonces podemos escribir la tabla de adición para K de la siguiente manera

$+$	P_0	P_1	P_2	$\cdots$	P_{k-1}
P_0	$B_{0,0}$	$B_{0,1}$	$B_{0,2}$	$\cdots$	$B_{0,k-1}$
P_1	$B_{1,0}$	$B_{1,1}$	$B_{1,2}$	$\cdots$	$B_{1,k-1}$
P_2	$B_{2,0}$	$B_{2,1}$	$B_{2,2}$	$\cdots$	$B_{2,k-1}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
P_{k-1}	$B_{k-1,0}$	$B_{k-1,1}$	$B_{k-1,2}$	$\cdots$	$B_{k-1,k-1}$

Quitando las etiquetas de la tabla aditiva de K, lo que se obtiene es un cuadrado latino de orden k^2 que denotaremos como A. Este cuadrado esta dividido por bloques de tamaño $k \times k$ cada uno de los cuales contiene a los elementos de una única clase. De tal manera que cualquier renglón de A intersectado con cualquier bloque de tamaño $k \times k$ es precisamente una de las clases P_i. Esto se sigue cumpliendo si permutamos los renglones de A, para obtener otro cuadrado latino L con bloques $E_{i,j}$. De hecho, si dos renglones del bloque $E_{i,j}$ contienen los elementos de la misma clase P_n, entonces estos dos mismos renglones tienen que intersectar $E_{i,l}$ en los elementos de la misma clase P_m. Esto prueba la siguiente proposición

Proposición 2.2.1. *Sea L un cuadrado latino de orden k^2 obtenido de permutar los renglones de A definido arriba. Si dos bloques $E_{i,j}$ y $E_{i,k}$ están en el mismo renglón de bloques de L, entonces $E_{i,j}$ tiene la propiedad S si y sólo si $E_{i,k}$ también la tiene.*

Dado que cada renglón de un bloque contiene precisamente los elementos de una clase P_i requerimos simplemente que los renglones del bloque contenga a las diferentes clases para que se cumpla la propiedad S. Esto lo podemos verificar considerando los elementos en la primera columna de bloques de A y de aquí la siguiente proposición.

Proposición 2.2.2. *Un bloque del cuadrado latino L que se definió anteriormente tiene la propiedad S si y sólo si la primera columna contiene exactamente un elemento de cada una de las clases P_i.*

Por la proposición tenemos una manera fácil de comprobar si un bloque de L tiene la propiedad S, sólo tenemos que determinar las permutaciones apropiadas de los renglones de A para tener SLS ortogonales. Para lograr esto, utilizamos la siguiente notación. r_g denota el renglón de A cuya entrada en la primera columna es g y (g, h) denota la celda en A cuyo renglón comienza con g y cuya columna comienza con h. Esto nos lleva al siguiente teorema.

Teorema 2.2.1. *Para cada $x \in K \backslash F$, el cuadrado latino L_x formado por aplicar la permutación $r_g \to r_{g \cdot x}$ a los renglones de A tienen la propiedad S. Mas aún, para $x_1, x_2 \in K \backslash F$ con $x_1 \neq x_2$, L_{x_1} y L_{x_2} son ortogonales.*

Demostración. Primero verifiquemos que L_x es un SLS.Sea B cualquier bloque de L_x. Por la proposición anterior tenemos que si la primera columna de B tiene exactamente un elemento de cada clase, entonces L_x es un SLS. Sea $g = a \cdot x$ y $h = b \cdot x$ elementos distintos en la primera columna de B. De la construcción de L_x se tiene que $g \cdot x^{-1}$ y $h \cdot x^{-1}$ se encuentran en la misma clase aditiva. Esto implica que la diferencia $g \cdot x^{-1} - h \cdot x^{-1}$ se encuentra en F. Pero, $g - h \in F$ si y sólo si $x^{-1} \in F$. Sin embargo $x^{-1} \notin F$, por lo cual g y h están en diferentes clases. Por lo tanto la primera columna de B contiene exactamente a un elemento de cada clase.

Ahora supongamos que $x_1 \neq x_2$ y que el valor de las celdas (g_1, h_1) y (g_2, h_2) en L_{x_1} es el mismo . De forma similar en L_{x_2}. Dado que la entrada en la celda (g_i, h_j) en el cuadrado L_{x_l} esta dada por $g_i \cdot x_l + h_j$, entonces se tienen las siguientes ecuaciones $g_1 \cdot x_1 + h_1 = g_2 \cdot x_1 + h_2$ y $g_1 \cdot x_2 + h_1 = g_2 \cdot x_2 + h_2$ que restandolas nos da $g_1 \cdot (x_1 - x_2) = g_2 \cdot (x_1 - x_2)$ y como $x_1 \neq x_2$ esto implica que $g_1 = g_2$ y por tanto $h_1 = h_2$. De tal manera que L_{x_1} y L_{x_2} son ortogonales. □

Dado que $K\backslash F$ tiene orden $k^2 - k$, esta construcción produce un conjunto de $MOSLS$ de cardinalidad máxima. Esto prueba el siguiente corolario.

Corolario 2.2.1. *Si k es potencia de un primo, entonces existe un conjunto de $k^2 - k$ MOSLS de orden k.*

2.2.2. Construcción de un conjunto de $MOSLS$ de orden k

Ahora para cuando k no es potencia de un primo utilizaremos el método de MacNeish que utiliza la técnica del producto directo para construir conjuntos de $MOLS$. En este caso se modificará esta método y haremos uso de los cuasigrupos.

Un sistema binario es un par $(Q, *)$ donde Q es un conjunto y $*$ una operación binaria sobre Q (una función que va de $Q \times Q$ a Q). Usualmente se escribe a la imagen de la operación sobre el par (a, b) como $a * b$.

Un **cuasigrupo** es un sistema binario $(Q, *)$ que satisface las condiciones

- Para cualquier $a, b \in Q$ existe un único $x \in Q$ tal que $a * x = b$.
- Para cualquier $a, b \in Q$ existe un único $y \in Q$ tal que $y * a = b$.

Una **tabla de Cayley** de un conjunto con una operación binaria es un arreglo cuadrado con filas y columnas indexadas por Q en algún orden (el mismo orden para filas y columnas). El valor de la entrada en la fila a y columna b será $a * b$.

Teorema 2.2.2. *Un sistema binario $(Q, *)$ es un cuasigrupo si y sólo su tabla de Cayley es un cuadrado latino.*

Demostración. Sea $A = (a_{ij})$ un cuadrado latino de orden n, etiquetamos a las columnas del 1 al n de igual forma etiquetamos a los renglones. Definimos $ij = a_{ij}$. Dado que A es un cuadrado latino al elegir cualquier renglón $\alpha \in \{1, 2, \ldots, n\}$ y cualquier entrada $\beta \in \{1, 2, \ldots, n\}$ en ese renglón, entonces existe una única columna $i \in \{1, 2, \ldots, n\}$ tal que $\alpha i = \beta$. De forma similar considerando α como cualquier columna, existe un único renglón j tal que $j\alpha = \beta$.

Sea $(Q, *)$ un cuasigrupo con n elementos, para cada par de elementos $q_i, q_j \in Q$ se tienen dos únicos elementos $q_k, q_l \in Q$ tal que $q_i q_k = q_j$ y $q_l q_i = q_j$. Notemos que $i, j, k, l \in \{1, 2, \ldots, n\}$. Tenemos que para cada i y j existe un único k tal que $ik = j$ y un único l tal que $li = j$. Esto es equivalente a decir que para cada renglón y columna existe una única entrada en la cual ellos se cruzan. Así podemos construir un cuadrado latino para G por tener $q_i q_k = q_j$ si y sólo si $a_{ij} = k$. □

Diremos que dos cuasigrupos son ortogonales siempre que sus cuadrados latinos asociados sean ortogonales.

Primero tenemos el siguiente resultado acerca de los productos directos en cuasigrupos.

Lema 2.2.1. *Sea* $(G, \cdot_1)$ *y* $(G, \cdot_2)$, $(H, \cdot_3)$ *y* $(H, \cdot_4)$ *pares de cuasigrupos ortogonales y las operaciones* $\cdot_{1,3}$ *y* $\cdot_{2,4}$ *sobre el conjunto* $G \times H$ *que se definen como* $(a, b) \cdot_{1,3} (c, d) = (a \cdot_1 c, b \cdot_3 d)$ *y* $(a, b) \cdot_{2,4} (c, d) = (a \cdot_2 c, b \cdot_4 d)$. *Entonces* $(G \times H, \cdot_{1,3})$ *y* $(G \times H, \cdot_{2,4})$ *son cuasigrupos ortogonales.*

Sea A y A' $MOSLS$ sobre el conjunto $G = \{1, 2, \ldots, m^2\}$ y B y B' $MOSLS$ sobre el conjunto $H = \{1, 2, \ldots, n^2\}$. Definimos a los cuasigrupos $(G, \cdot_A)$,$(G, \cdot_{A'})$,$(H \cdot_B)$ y $(H, \cdot_{B'})$ con $a \cdot_X b = X_{a,b}$ donde $X = A, A', B$ o B'.

Si definimos a los cuasigrupos $(G \times H, \cdot_{A,B})$ y $(G \times H, \cdot_{A',B'})$ con $(a, b) \cdot_{X,Y} (c, d) = (a \cdot_X, b \cdot_Y d)$, entonces el lema nos dice que para obtener un par de SLS ortogonales sólo tenemos que encontrar un ordenamiento de los elementos de $G \times H$, para que los cuadrados latinos resultantes cumplan la propiedad S.

Sea C el cuadrado latino asociado a el cuasigrupo $(G \times H, \cdot_{A,B})$, los bloques de C se obtienen como pares ordenados de un bloque de A y un bloque de B. De forma mas precisa, el arreglo de los bloques en A crea una partición $\{P_i\}$ de G de m conjuntos de cardinalidad m cada uno, donde cada conjunto P_i se compone de los números del $(i-1)m+1$ al im. De tal manera que dos elementos de G están en el mismo conjunto P_i si y sólo si los renglones (o columnas) correspondientes a x y y intersectan a los mismos bloques de tamaño $m \times m$ de A. En particular, cualquier bloque del SLS se determina de forma única por un par de elementos de la partición y viceversa. De forma similar, el arreglo de los bloques en B crea una partición $\{Q_i\}$ de H de n conjuntos de cardinalidad n cada uno, donde cada conjunto Q_i consta de los números del $(i-1)n+1$ al in. Estas particiones de G y H generan una partición $\{P_i\} \times \{Q_i\}$ en los elementos de $G \times H$ de mn conjuntos de cardinalidad mn cada uno.

Para obtener un SLS de orden $(mn)^2$, ordenamos a los elementos de $G \times H$ de tal manera que los elementos de cada elemento de la partición $P_i \times Q_i$ sean consecutivos. Utilizamos este orden en la construcción de la tabla de Cayley para el cuasigrupo $(G \times H, \cdot_{A,B})$. Quitamos las etiquetas a esta tabla, entonces los bloques de tamaño $mn \times mn$ del cuadrado latino C resultante se determinan nuevamente de forma única por un par de elementos de la partición y viceversa. Dado que este orden es independiente de A y B, lo que queda es demostrar que C es un SLS.

Para verificar que C es un SLS tenemos que demostrar que todo bloque de C cumple la propiedad S. Sea R un bloque arbitrario de C determinado por un par arbitrario de elementos de la partición ($P_i \times Q_j$ determina los renglones de R y $P_k \times Q_l$ las columnas). Entonces cualquier entrada de R tiene la forma $(a, b) \cdot_{A,B} (c, d)$, con $a \in P_i$, $b \in Q_j$,$c \in P_k$ y $d \in Q_l$. De este modo, sea $a_1, a_2 \in P_i$, $b_1, b_2 \in Q_j$,$c_1, c_2 \in P_k$ y $d_1, d_2 \in Q_l$ y supongamos que $(a_1, b_1) \cdot_{A,B} (c_1, d_1) = (a_2, b_2) \cdot_{A,B} (c_2, d_2)$. Entonces $a_1 \cdot_A c_1 = a_2 \cdot_A c_2$ y como A es un SLS se tiene que $a_1 = a_2$ y $c_1 = c_2$. De forma similar se tiene $b_1 \cdot_B d_1 = b_2 \cdot_B d_2$ y por ser B un SLS tenemos que $b_1 = b_2$ y $d_1 = d_2$. Por lo que todos los elementos de R son distintos y por lo tanto cumple la propiedad S. De tal manera que se acaba de demostrar la siguiente proposición.

Proposición 2.2.3. *Cualquier cuadrado latino construido por esta modificación del método de MacNeish es un SLS.*

Sea C_1 y C_2 los SLS asociados a los cuasigrupos $(G \times H, \cdot_{A,B})$ y $(G \times H, \cdot_{A',B'})$ respectivamente. Verifiquemos que son ortogonales. Supongamos que dos elementos en C_1 y C_2 son iguales, es decir, $(a_1, b_1) \cdot_{A,B} (c_1, d_1) = (a_2, b_2) \cdot_{A,B} (c_2, d_2)$ y $(a_1, b_1) \cdot_{A',B'} (c_1, d_1) = (a_2, b_2) \cdot_{A',B'} (c_2, d_2)$, entonces $(a_1 \cdot_A c_1, b_1 \cdot_B d_1) = (a_2 \cdot_A c_2, b_2 \cdot_B d_2)$ y $(a_1 \cdot_{A'} c_1, b_1 \cdot_{B'} d_1) = (a_2 \cdot_{A'} c_2, b_2 \cdot_{B'} d_2)$ de tal manera que tenemos $a_1 \cdot_A c_1 = a_2 \cdot_A c_2$, $a_1 \cdot_{A'} c_1 = a_2 \cdot_{A'} c_2$ y $b_1 \cdot_{B'} d_1 = b_2 \cdot_B d_2$, $b_1 \cdot_{B'} d_1 = b_2 \cdot_B d_2$. Entonces $a_1 = a_2$, $c_1 = c_2$, $b_1 = b_2$ y $d_1 = d_2$ por ser A, A' y B, B' pares de $MOSLS$. Por lo tanto C_1 y C_2 son ortogonales.

Corolario 2.2.2. *Si existen r MOSLS de orden m^2 y s MOSLS de orden n^2, entonces existen al menos* $\min\{r, s\}$ *MOSLS de orden $(mn)^2$.*

Demostración. Sea $t = \min\{r, s\}$. Tenemos t $MOSLS$ de orden m^2 y t de orden n^2, aplicando la construcción del producto directo se tienen un total de t SLS que son mutuamente ortogonales, es decir existe un conjunto de t MOSLS de orden $(mn)^2$. □

Teorema 2.2.3. *Sea $n = P_1^{a_1} P_2^{a_2} \cdots P_k^{a_k}$ la factorización en primos de n y sea $q = \min\{P_1^{a_1}, P_2^{a_2}, \cdots, P_k^{a_k}\}$. Entonces existen al menos $q^2 - q$ $MOSLS$ de orden n^2.*

Demostración. Se sigue de forma inductiva del corolario anterior y de la construcción para potencias de primos. □

Corolario 2.2.3. *Existen $MOSLS$ de orden n^2 para todo número natural $n > 1$.*

Demostración. Por el teorema anterior, el valor más pequeño que puede tener q es 2. Pero $2^2 - 2 = 2$ de tal manera que al menos existen dos $MOSLS$ para todo orden más grande que uno. Para $n = 1$ existe un cuadrado latino de orden 1, claramente es auto-ortogonal y cumple la propiedad S. □

2.2.3. Polinomio cromático

El desarrollo de este tema esta basado en el artículo de Agnes M. Herzberg y M. Ram Murty [11].

Una **λ-coloración** de una gráfica G es una función del conjunto de vértices a el conjunto $\{1, 2, \ldots, \lambda\}$. Esta función es llamada **coloración propia** si $f(x) \neq f(y)$ siempre que x y y sean adyacentes en G.

El mínimo número de colores requerido para colorear propiamente a los vértices de una gráfica G es llamado el **número cromático** de G y se denota como $\chi(G)$.

El juego del Sudoku lo podemos ver como un problema de coloración de una gráfica. Por ejemplo la gráfica asociada a un Sudoku de orden 9 tendrá 81 vértices donde cada uno de ellos corresponde a una celda del Sudoku. Dos vértices distintos serán adyacentes si y sólo si las celdas correspondientes

están en el mismo renglón o en la misma columna o en la misma subcuadrícula. Entonces la solución del Sudoku corresponde a una coloración propia de esta gráfica.

De forma más general, consideremos una cuadrícula de tamaño $n^2 \times n^2$. A cada celda de esta cuadrícula le asociaremos un vértice (i, j) con $1 \leq i, j \leq n^2$. Diremos que (i, j) y (i', j') son adyacentes si $i = i'$ o $j = j'$ o $\lceil \frac{i}{n} \rceil = \left\lceil \frac{i'}{n} \right\rceil$ y $\left\lceil \frac{j}{n} \right\rceil = \left\lceil \frac{j'}{n} \right\rceil$. A esta gráfica la llamaremos **gráfica Sudoku de orden** n^2 y la denotaremos como X_n.

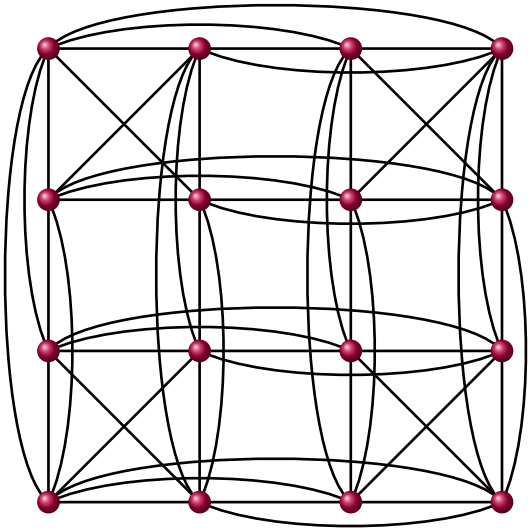


Figura 2.4: Gráfica Sudoku de orden 4

Un SLS de orden n^2 será una coloración propia de su gráfica usando n^2 colores. Un Sudoku corresponde a una coloración parcial de X_n.

Una gráfica es llamada **regular** si el grado de cada uno de los vértices de G es el mismo. X_n es una gráfica regular, ya que tomando al vértice (i, j) este es adyacente a $n^2 - 1$ vértices por renglón y a $n^2 - 1$ vértices por columna y a $n^2 - 1 - 2(n - 1)$ vértices por subcuadrícula. De tal manera que (i, j) tiene grado $n^2 - 1 + n^2 - 1 + n^2 - 1 - 2(n - 1) = 3n^2 - 2n - 1 = (3n + 1)(n - 1)$.

Es bien conocido que el número de formas de obtener una coloración propia de G con λ colores es un polinomio en λ de grado igual a el número de vértices de G.

El siguiente teorema dice que dada una coloración parcial propia C de G, el número de formas de completar la coloración para obtener una propia usando λ colores es también un polinomio en λ, siempre que λ sea mayor o igual al número de colores usados en C.

Teorema 2.2.4. *Sea G una gráfica finita con v vértices y C una coloración parcial propia de t vértices de G usando d_0 colores. Denotemos a $P_{G,C}(\lambda)$ el número de formas de completar esta*

coloración usando λ colores para obtener una coloración propia de G. Entonces $P_{G,C}(\lambda)$ es un polinomio mónico de grado $v-t$ en λ con coeficientes enteros para $\lambda \geq d_0$.

Demostración. Para la demostración consideraremos dos casos

Caso 1. Sea e una arista en G con a lo más un vértice en C. Aplicando inducción sobre el número de aristas tenemos

Sea G una gráfica con v vértice y cero aristas y C una coloración parcial propia de t vértices de G usando d_0 colores. Entonces $P_{G,C}(\lambda) = \lambda^{v-t}$ ya que a cada vértice fuera de C lo podemos colorear de λ formas distintas.

Ahora supongamos que el teorema es válido para cualquier gráfica con v vértices y n aristas, falta demostrar que también es válido para G una gráfica con v vértices y $n+1$ aristas.

Denotaremos a la gráfica obtenida de quitarle la arista e, pero no sus puntos finales como $G-e$ y G/e es la contracción de G que consiste en eliminar a la arista e tomar a sus puntos finale x y y y unirlos. Al vértice que resulta de unir a x y y conservará todas las aristas que eran incidentes a x y y.

Con las gráficas anteriores tenemos que

$$P_{G,C}(\lambda) = P_{G-e,C}(\lambda) - P_{G/e,C}(\lambda)$$

ya que cada coloración propia de G es también coloración propia de $G-e$ y una coloración propia de $G-e$ es coloración propia de G si y sólo si se le dan colores distintos a los puntos finales de e. De tal manera que $P_{G,C}(\lambda)$ es igual a $P_{G-e,C}(\lambda)$ menos aquellas coloraciones en las que x y y tienen el mismo color que están dadas por $P_{G/e,C}(\lambda)$. Tenemos que las gráficas $G-e$ y G/e tienen n aristas, por lo cual $P_{G-e,C}(\lambda)$ y $P_{G/e,C}(\lambda)$ son polinomios mónicos de grado $v-t$ en λ con coeficientes enteros y por ser $P_{G,C}(\lambda)$ resta de estos es por lo tanto un polinomio mónicos de grado $v-t$ en λ con coeficientes enteros.

Caso 2. Supongamos que G tiene un vértice v_0 que no esta contenido en C y no es adyacente a ningún vértice de C, entonces $G = C \bigcup v_0$, que es la unión disjunta de C y el vértice v_0. De tal manera que v_0 puede colorearse de λ. Por lo cual $P_{G,C}(\lambda) = \lambda$. □

Por lo anterior, se tiene que el número de formas de completar un Sudoku de orden 9 esta dado por $p_{X_3,C}(9)$. Un Sudoku (X_3, C) tiene solución única si y sólo si $p_{X_3,C}(9) = 1$. El siguiente teorema nos indica bajo qué condiciones una coloración parcial puede extenderse de forma única a una coloración propia.

Teorema 2.2.5. *Sea G una gráfica con número cromático $\chi(G)$ y C una coloración parcial de G usando sólo $\chi(G)-2$ colores. Si la coloración parcial puede ser completada a una coloración propia de G, entonces existen al menos dos formas de extender la coloración.*

Demostración. Dado que dos colores no se utilizaron en la coloración parcial C, estos colores se utilizaran para obtener una coloración propia de G y después intercambiandolos obtendremos otra coloración propia de G distinta a la anterior. □

Del teorema anterior tenemos que si C es una coloración parcial de G que puede ser completada de forma única a una coloración propia de G, entonces C debe de usar al menor $\chi(G)-1$ colores. En particular, tenemos que en cualquier Sudoku de orden 9 al menos 8 colores deben de ser utilizados en las celdas dadas. En general, para un Sudoku de tamaño $n^2 \times n^2$ al menos $n^2 - 1$ colores deben de ser usados en la coloración parcial dada para que tenga solución única.

2.2.4. Coloración explícita para X_n

A continuación daremos una coloración propia de X_n. Claramente la gráfica completa K_n tiene número cromático n.

Teorema 2.2.6. *Para todo número natural n, existe una coloración propia de la gráfica Sudoku X_n usando n^2 colores. Mas aún, el número cromático de X_n es n^2.*

Demostración. Notemos que cada una de las celdas de la subcuadrícula superior izquierda es adyacente a las demás celdas que pertenecen al bloque. De tal manera que su gráfica asociada es isomorfa a una gráfica completa de orden n^2 (K_{n^2}). El número cromático de K_{n^2} es n^2, por lo cual X_n necesita al menos n^2 colores para dar una coloración propia.

Ahora mostraremos que X_n puede ser coloreada usando n^2 colores.

Etiquetemos a los vértices de X_n como (i, j) con $0 \leq i, j \leq n^2 - 1$. Consideremos las clases residuales módulo n^2. Para $0 \leq i \leq n^2 - 1$ escribimos $i = t_i n + d_i$ con $0 \leq d_i, t_i \leq n - 1$ y de forma similar para $0 \leq j \leq n^2 - 1$. Ahora, asignamos el color $c(i, j) = d_i n + t_i + nt_j + d_j$ módulo n^2 a la celda (i, j) de la cuadrícula de tamaño $n^2 \times n^2$. Esto es una coloración propia ya que cualesquiera dos vértices adyacentes (i, j) y (i', j') tienen colores distintos. En efecto, si $i = i'$ debemos verificar que $c(i, j) \neq c(i, j')$ a menos que $j = j'$. Supongamos que $c(i, j) = c(i, j')$ entonces $d_i n + t_i + nt_j + d_j = d_i n + t_i + nt_{j'} + d_{j'}$ módulo n^2, de tal manera que $nt_j + d_j = nt_{j'} + d_{j'}$ módulo n^2, lo que significa que $j = j'$. De forma similar si $j = j'$, entonces $c(i, j) \neq c(i', j)$ a menos que $i = i'$. Ahora para los vértices (i, j) y (i', j') se cumple que $\left\lfloor \frac{i}{n} \right\rfloor = \left\lfloor \frac{i'}{n} \right\rfloor$ y $\left\lfloor \frac{j}{n} \right\rfloor = \left\lfloor \frac{j'}{n} \right\rfloor$, entonces $d_i = d_{i'}$ y $d_j = d_{j'}$ y si $c(i, j) = c(i', j')$, entonces $t_i + nt_j = t_{i'} + nt_{j'}$ reduciendo esta ecuación módulo n tenemos $t_i = t_{i'}$. Entonces $t_j = t_{j'}$. Por lo tanto $(i, j) = (i', j')$. De tal manera que la coloración dada es propia. □

Ejemplo 2.2.4. *Siguiendo el procedimiento anterior, la coloración propia obtenida para X_2 es*

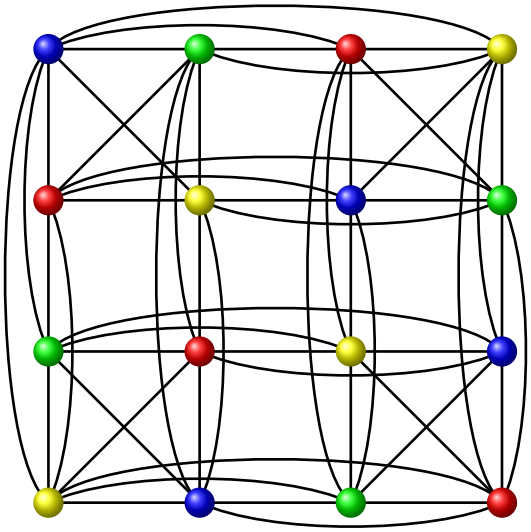


Figura 2.5: Coloración propia de X_2

Daremos algunas condiciones necesarias para que un Sudoku tenga solución única.

Como se mencionó anteriormente, si el número de colores usados en un Sudoku de orden 9 es a lo más 7 entonces existen al menos dos soluciones del juego. La multiplicidad de soluciones también se pueden ver en su polinomio cromático. Si d_0 es el número de colores distintos usados en la coloración parcial, hemos visto que $P_{X_3,C}(\lambda)$ es un polinomio en λ siempre que $\lambda \geq d_0$. Dado que $\chi(X_3) = 9$ se cumple que $P_{X_3,C}(\lambda) = 0$ para $\lambda = d_0, d_0+1, \ldots, 8$ y como $P_{X_3,C}(\lambda)$ es un polinomio mónico con coeficientes enteros lo podemos factorizar como

$$P_{X_3,C}(\lambda) = (\lambda - d_0)(\lambda - (d_0+1)) \cdots (\lambda - 8)q(\lambda)$$

para algún polinomio $q(\lambda)$ con coeficientes enteros. Sustituyendo $\lambda = 9$ obtenemos $P_{X_3,C}(9) = (9-d_0)!q(9)$ que será mayor o igual a 2 si $d_0 \leq 7$. Esto nos determina una condición necesaria para que exista solución única.

2.2.5. Cotas para el número de SLS

Sabemos que el número de cuadrados latinos de orden n es al menos

$$\frac{n!^{2n}}{n^{n^2}}. \tag{2.1}$$

Corolario 2.2.4. *El número de cuadrados latinos es al menos*

$$n^{2n^4}e^{-2n^4+O(n^2\log n)}.$$

Demostración. De (1) tenemos que el número de cuadrados latinos de orden n^2 es al menos

$$\frac{(n^2!)^{2n^2}}{((n^2)^{n^2})^2} = \frac{(n^2!)^{2n^2}}{n^{2n^4}}. \tag{2.2}$$

Usando la fórmula de Stirling

$$\log n! = n\log n - n + \frac{1}{2}\log n + O(1)$$

obtenemos que $\log n^2! = n^2\log n^2 - n^2 + \frac{1}{2}\log n^2 + O(1)$, aplicando la exponencial a ambos lados tenemos $n^2! = e^{2n^2\log n - n^2 + \log n + O(1)}$, sustituyendo $n^2!$ en (2) obtenemos

$$\begin{aligned}
\frac{(n^2!)^{2n^2}}{n^{2n^2}} &= \frac{(e^{2n^2\log n - n^2 + \log n + O(1)})^{2n^2}}{n^{2n^4}} \\
&= \frac{e^{2n^2(2n^2\log n - n^2 + \log n + O(1))}}{n^{2n^4}} \\
&= \frac{e^{(4n^4\log n - 2n^4 + n^2\log n + 2n^2O(1))}}{n^{2n^4}} \\
&= \frac{e^{4n^4\log n}}{n^{2n^4}} e^{-2n^4+2n^2\log n+2n^2O(1))} \\
&= n^{2n^4}e^{-2n^4+O(n^2\log n)}.
\end{aligned}$$

□

Ahora daremos una cota superior para el número de SLS.

Una cota superior cruda para este número es

$$(n^2!)^{n^2}$$

ya que un SLS es una cuadrícula de tamaño $n^2 \times n^2$ que esta compuesta por n^2 subcuadrículas de tamaño $n \times n$ y en cada subcuadrícula deben de aparecer los elementos del $\{1, 2, \ldots, n^2\}$, de tal manera que cada una de ellas puede ser llenada de $n^2!$ formas distintas, obteniendo la cota superior mencionada.

Ahora daremos una mejor cota superior para este número, en donde utilizaremos la cota superior dada para la permanente de una matriz de $(0, 1)$.

Teorema 2.2.7. *El número de SLS de orden n esta acotado superiormente por*

$$n^{2n^4}e^{-2.5}n^4 + O(n^3 \log n)$$

para n suficientemente grande.

Demostración. Llamaremos **banda** al grupo de n renglones sucesivos en una cuadrícula. De tal manera que un Sudoku de orden n^2 tiene n bandas. Primero estimaremos el número de formas distintas de completar la primera banda. Para el primer renglón hay $n^2!$ formas distintas de llenarlo. Para saber el número de formas de llenar el segundo renglón utilizaremos la permanente de la matriz A, donde A es de tamaño $n^2 \times n^2$ cuyos renglones representan las celdas del segundo renglón y las columnas a los números del 1 al n^2. Asignaremos 1 a la entrada (i, j) de la matriz A si j es un valor válido para la celda i y 0 si no. Observemos que cada celda del segundo renglón tiene $n^2 - n$ posibles valores a elegir, ya que en el primer renglón de su subcuadrícula ya se utilizaron n colores. Esto nos da una matriz $(0, 1)$ cuya permanente es a lo más

$$\prod_{i=1}^{n^2} r_i!^{\frac{1}{r_i}} = \prod_{i=1}^{n^2} (n^2 - n)!^{\frac{1}{n^2-n}} = (n^2 - n)!^{\frac{n}{n-1}}$$

que es el número de formas distintas de elegir un sistema de representantes distintos que es equivalente a el número de formas distintas de llenar el segundo renglón de la banda.

Procediendo de manera similar para el tercer renglón de la banda tenemos que el número de formas distintas de llenarlo es a lo más

$$\prod_{i=1}^{n^2} (n^2 - 2n)!^{\frac{1}{n^2-2n}} = (n^2 - 2n)!^{\frac{n}{n-2}}$$

ya que cada celda puede elegir su valor entre $n^2 - 2n$ posibles valores. De esta forma tenemos que el número de formas distintas de llenar la primera banda es a lo más

$$\prod_{k=0}^{n-1} (n^2 - kn)!^{\frac{n}{n-k}}$$

. Ahora supongamos $(i-1)$ de las n bandas están llenas. Calcularemos el número de formas distintas de llenar la i-ésima banda. El número de posibles valores que puede tomar la primera celda de la banda es $n^2 - (i-1)n$. De tal manera que el número de formas distintas de llenar el primer renglón esta acotada superiormente por

$$(n^2 - (i-1)n)!^{\frac{n^2}{n^2-(i-1)n}}$$

ya que cada celda no puede tomar los valores que fueron colocados en las primeras $i - 1$ posiciones de su columna. Similarmente para el segundo renglón de la i-ésima banda el número de formas de llenarlo esta acotado superiormente por

$$(n^2 - ((i-1)n + 1))!^{\frac{n^2}{n^2-((i-1)n+1)}}$$

. Siguiendo este procedimiento tenemos que para el i-ésimo renglón de la banda en número de formas de llenarlo esta acotado por

$$(n^2-((i-1)n+i))!^{\frac{n^2}{n^2-((i-1)n+i)}}$$

para llenar el renglón $i+1$ cambiamos la estrategia, ahora cada celda puede elegir su valor entre n^2-in posibilidades, ya que se excluyen los valores que ya fueron colocados en la subcuadrícula a la que pertenece. Por lo cual el número de formas de llenar el renglón esta acotado superiormente por

$$(n^2-in)!^{\frac{n^2}{n^2-in}}$$

por lo tanto tenemos que el número de SLS de orden n^2 esta acotado superiormente por

$$\begin{aligned}&\prod_{i=1}^{n}(n^2-(i-1)n)!^{\frac{n^2}{n^2-(i-1)n}}\\&(n^2-((i-1)n+1))!^{\frac{n^2}{n^2-((i-1)n+1)}}\\&\cdots(n^2-((i-1)n+i))!^{\frac{n^2}{n^2-((i-1)n+i)}}\\&(n^2-in)!^{\frac{n^2}{n^2-in}}\cdots(n^2-(n-1)n)!^{\frac{n^2}{n^2-(n-1)n}}.\end{aligned}$$

Así

$$\frac{\log S_n}{n^2}\leq\sum_{i=1}^{n}\left(\sum_{j=0}^{i}\frac{\log(n^2-((i-1)n+j))!}{n^2-(i-1)n+j}+\sum_{k=i}^{n-1}\frac{\log(n^2-kn)}{(n^2-kn)}\right).$$

Usando la fórmula de Stirling obtenemos

$$\frac{\log S_n}{n^2}\leq\sum_{i=1}^{n}\left(\sum_{j=0}^{i}\log(n^2-[(i-1)n+j])+\sum_{k=i}^{n-1}\log(n^2-kn)\right)-n^2+O(\log^2 n)$$

luego

$$\frac{\log S_n}{n^2}\leq\sum_{i=1}^{n}\left(i\log(n^2-(i-1)n)+\sum_{k=i}^{n-1}\log(n^2-kn)\right)-n^2+O(\log^2 n).$$

Así, $(\log S_n)/n^2+n^2+O(n\log n)$ es

$$\leq\frac{1}{2}n^2\log n+\sum_{i=1}^{n}\left(i\log(n-i+1)+(n-i)\log n+\sum_{k=i}^{n-1}\log(n-k)\right).$$

La sumatoria sobre k es

$$\log(n-i)!=(n-i)\log(n-i)-(n-i)+O(\log n)$$

por la fórmula de Stirling. Entonces

$$\begin{aligned}
\frac{\log S_n}{n^2} &\leq 2n^2 \log n - 2.5n^2 + O(n \log n) \\
\log S_n &\leq 2n^4 \log n - 2.5n^4 + n^2 O(n \log n) \\
S_n &\leq e^{2n^4 \log n - 2.5n^4 + n^2 O(n \log n)} \\
&\leq n^{2n^4} e^{-2.5n^4 + O(n^3 \log n)}.
\end{aligned}$$

□

2.3. Gráficas

En esta sección haremos uso de los cuadrados latinos y cuadrados latinos reducidos, simétricos y unipotentes de orden n para dar 1-factorizaciones de las gráficas $\mathbb{K}_{n,n}$, $\mathbb{K}_n$ y $\overrightarrow{\mathbb{K}_n}$. También mostraremos la presencia de estos cuadrados en la teoría de Ramsey, concretamente en la determinación de una cota inferior para el número de Ramsey de un árbol.

Una **gráfica** es una pareja ordenada de conjuntos $G = (V, E)$. A los elementos de V los llamaremos **vértices**. Los elementos de E son subconjuntos de vértices de cardinalidad 2 a los que denominaremos **aristas** de G. Llamaremos **orden** de G a $|V| = |G|$.

2.3.1. Factorización de $\mathbb{K}_{n,n}$

Diremos que una gráfica G es **bipartita** si el conjunto V de vértices puede dividirse en dos subconjuntos independientes $U = \{u_1, u_2, \ldots, u_m\}$ y $W = \{w_1, w_2, \ldots, w_n\}$ tales que no existe arista que una vértices que pertenecen a U ni vértices en W.

Suponiendo que $|U| = |W|$, podemos relacionar a las gráficas bipartitas con los cuadrados latinos, ya que U y W representan los renglones y columnas de un cuadrado latino L de orden n. Si $L(i, j) = k$, quiere decir que a los vértices i e j los une una arista de color k, donde k toma valores en $\{1, \ldots, n\}$. Denotaremos a la gráfica bipartita con $|U| = |W| = n$, donde todo vértice de U es adyacente a todo vértice de W como $\mathbb{K}_{n,n}$. Los vértices de la gráfica bipartita construida de esta forma tienen exactamente una arista de cada color incidente en él.

Un 1-**factor** de una gráfica $G = (V, E)$ es una subgráfica $F = (V', E')$ de G donde $V' = V$ y E' es tal que cada vértice tiene exactamente una arista incidente en él.

Ejemplo 2.3.1. *En la figura mostramos un* 1*-factor de* $\mathbb{K}_{5,5}$.

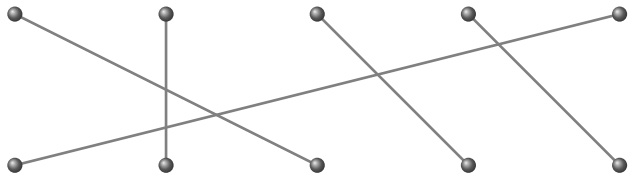


Figura 2.6: Un 1-factor de $\mathbb{K}_{5,5}$

Decimos que una gráfica es 1-**factorizable** si su conjunto de aristas admite una partición en 1-factores. Denotaremos a una 1-factorización de una gráfica G como $(F_1, F_2, \ldots, F_n)$ donde F_i es un 1-factor de G. El siguiente teorema nos determina la relación entre los cuadrados latinos de orden n y las gráficas bipartitas $\mathbb{K}_{n,n}$.

Teorema 2.3.1. *Un cuadrado latino de orden n es equivalente a una 1-factorización de $\mathbb{K}_{n,n}$.*

Demostración. Sea L un cuadrado latino de orden n, sabemos que cada elemento del conjunto base $B = \{1, \ldots, n\}$ aparece exactamente una vez en cada renglón y cada columna de L. Cada vértice de la gráfica bipartita que se obtiene a partir de L tiene exactamente una arista de cada color incidente en él, entonces cada elemento de B nos determina un 1-factor F_i monocromático de $\mathbb{K}_{n,n}$. Por lo tanto tenemos a $(F_1, F_2, \ldots, F_n)$ una 1-factorización de $\mathbb{K}_{n,n}$.

Recíprocamente, sea $(F_1, F_2, \ldots, F_n)$ una 1-factorización de $\mathbb{K}_{n,n}$, cuyas aristas de F_i son coloreadas con un único color tomado del conjunto $\{1, \ldots, n\}$. De modo que, se tiene una 1-factorización de $\mathbb{K}_{n,n}$ donde los 1-factores son monocromáticos. Al colocar el símbolo k en la posición (i, j) de la matriz L de tamaño $n \times n$ si existe una arista de color k del vértice i al vértice j, se tiene que cada columna de L tiene exactamente una vez cada color del conjunto $\{1, \ldots, n\}$. Por lo tanto, L es un cuadrado latino de orden n. □

Ejemplo 2.3.2. *Sea*

$L =$

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

un cuadrado latino de orden 3. Entonces la 1-factorización de $\mathbb{K}_{3,3}$ asociada a L es

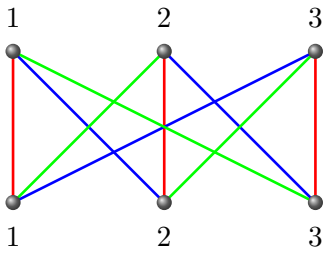


Figura 2.7: Una 1-factorización de $\mathbb{K}_{3,3}$.

Otra forma de saber cuando un cuadrado latino tiene compañero ortogonal es mediante la 1-factorización asociada a $\mathbb{K}_{n,n}$. Recordemos que una transversal de un cuadrado latino de orden n es un conjunto de n posiciones donde cualquiera dos de ellas no están en el mismo renglón ni en la misma columna, conteniendo a los n símbolos del conjunto base exactamente una vez.

Teorema 2.3.2. *Un cuadrado latino de orden n tiene un compañero ortogonal si y sólo si existe una 1-factorización asociada a $\mathbb{K}_{n,n}$ en donde cada 1-factor contiene una arista de cada color.*

Demostración. Sea L un cuadrado latino de orden n que tiene un compañero ortogonal. Por el teorema 1.2.2 L tiene n transversales disjuntas. Como cada transversal contiene una entrada de cada renglón y columna, las aristas asociadas a estas posiciones forman un 1-factor de la gráfica bipartita asociada a L. Dado que cada símbolo de $\{1,\dots,n\}$ aparece exactamente una vez en cada transversal, cada uno de los 1-factores tiene una arista de cada color.

Recíprocamente, dada una 1-factorización de $\mathbb{K}_{n,n}$ donde cada 1-factor tiene una arista de cada color, podemos construir una matriz L de tamaño $n\times n$ donde cada 1-factor determina una transversal. De aquí que los n 1-factores determinan n transversales disjuntas que en conjunto contiene las n^2 posiciones de L. Luego, por el teorema 1.2.2 L tiene un compañero ortogonal. □

2.3.2. Factorización de $\mathbb{K}_n$

Otras familias de gráficas son las gráficas completas dirigidas y las completas de orden n. Lo que veremos en esta sección es la relación que existe entre el número de cuadrados latinos y el número 1-factorizaciones de $\overrightarrow{\mathbb{K}_n}$ y $\mathbb{K}_n$.

A un cuadrado latino L de orden n con conjunto base $\{1,2,\dots,n\}$ lo podemos descomponer en n matrices $L_1, L_2, \dots, L_n$ de tamaño $n \times n$ tales que el conjunto base de L_i es $\{i\}$. Notese que

$$L = L_1 + L_2 + \cdots + L_n.$$

Ejemplo 2.3.3. *Al cuadrado latino*

$$L = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

lo descomponemos en la siguientes matrices

$$L_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \; L_2 = \begin{pmatrix} 0 & 2 & 0 & 0 \\ 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 \\ 0 & 0 & 2 & 0 \end{pmatrix} \; L_3 = \begin{pmatrix} 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 3 \\ 3 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \end{pmatrix} \; L_4 = \begin{pmatrix} 0 & 0 & 0 & 4 \\ 0 & 0 & 4 & 0 \\ 0 & 4 & 0 & 0 \\ 4 & 0 & 0 & 0 \end{pmatrix}$$

Como en la sección 2.3.1 diremos que la arista dirigida (i,j) tiene el color k si $L(i,j) = k$.

Cada una de las matrices $L_1, \dots, L_n$ es la matriz de incidencia de una gráfica dirigida. Al unirlas o superponerlas obtendremos una gráfica dirigida con las siguientes propiedades

1. Existe una arista dirigida del vértice i al vértice j para todo $i, j = 1, 2, \dots, n$.
2. Uno de los n colores esta asociado a cada arista dirigida.
3. Cada vértice tiene exactamente una arista dirigida de cada color que entra y que sale de él.

No es difícil comprobar que la gráfica que se obtiene es la completa dirigida con lazos de orden n y que la denotaremos por $\overrightarrow{\mathbb{K}_n}$. Recuerde que un **lazo** es una arista que sale de un vértice y llega al mismo vértice.

Para (i, j) cualquier par de vértices no necesariamente distintos, tal gráfica tiene una arista dirigida del vértice i al vértice j. En este caso un 1-factor de $\overrightarrow{\mathbb{K}_n}$ es una gráfica dirigida que contiene a todos los vértices de $\overrightarrow{\mathbb{K}_n}$ y sus aristas son un subconjunto de las aristas dirigidas de $\overrightarrow{\mathbb{K}_n}$, tales que cada vértice tiene una arista dirigida que entra y una que sale de él.

En el ejemplo 2.3.3 observamos que el cuadrado latino L se descompuso en cuatro matrices de incidencia, cada una de ellas representa a un 1-factor de la gráfica $\overrightarrow{\mathbb{K}_4}$ determinando así una 1-factorización de la misma. Ahora, podemos decir que cualquier cuadrado latino de orden n puede interpretarse como una 1-factorización de $\overrightarrow{\mathbb{K}_n}$. Recíprocamente, dada una 1-factorización de $\overrightarrow{\mathbb{K}_n}$ obtenemos un cuadrado latino de orden n asociado a ella.

Notemos que al renombrar a los vértices de $\overrightarrow{\mathbb{K}_n}$ obtendremos un cuadrado latino distinto, pero la 1-factorización sigue siendo la misma.

Teorema 2.3.3. *El número de* 1*-factorizaciones de* $\overrightarrow{\mathbb{K}_n}$ *esta dado por*

$$\overrightarrow{F_n} = \frac{L(n)}{n!} = (n-1)!l(n)$$

donde $L(n)$ *y* $l(n)$ *son respectivamente, el número de cuadrados latinos y cuadrados latinos reducidos de orden* n*.*

Demostración. Dada una 1-factorización de $\overrightarrow{\mathbb{K}_n}$, el número de formas distintas que se tienen para asignar colores a los 1-factores es $n!$ y como se hizo notar, al asignar de forma distinta los colores, los cuadrados latinos asociados a tal asignación serán distintos mientras que la 1-factorización sigue siendo la misma. De modo que, el número total de 1-factorizaciones de $\overrightarrow{\mathbb{K}_n}$ esta dado por $\overrightarrow{F_n} = \frac{L(n)}{n!}$ y del teorema 1.1.1 se tiene que $L(n) = n!(n-1)!l(n)$, por lo que $\overrightarrow{F_n} = (n-1)!l(n)$. □

Corolario 2.3.1. *El número de* 1*-factorizaciones de* $\overrightarrow{\mathbb{K}_n}$ *corresponde al número de cuadrados latinos de orden* n *con la primera fila fija.*

Demostración. Existen $n!$ formas distintas de llenar el primer renglón de un cuadrado latino de orden n, entonces el número de cuadrados latinos distintas cuya primera fila esta fija es $L_(n)/n!$ que corresponde al número de 1-factorizaciones de $\overrightarrow{\mathbb{K}_n}$. □

Ahora, denotaremos a la gráfica completa dirigida sin lazos como $\overrightarrow{\mathbb{K}'_n}$. Dada una 1-factorización de $\overrightarrow{\mathbb{K}'_n}$, asignaremos el color $i-1$ a la arista dirigida que sale del vértice i con $i = 1, \ldots, n$ de cada uno de los 1-factores, en este caso, el 0 indica la ausencia de lazos. La matriz obtenida de la 1-factorización de $\overrightarrow{\mathbb{K}'_n}$ que consiste en colocar k en la posición (i, j) cuando una arista dirigida

de color k va del vértice i al vértice j es un cuadrado latino de orden n, cuyo primer renglón se encuentra en orden natural y cuyos elementos de la diagonal principal son cero.

Al cuadrado latino cuyos elementos en la diagonal principal son iguales lo llamaremos **cuadrado latino unipotente**.

Sea L un cuadrado latino reducido, si aplicamos la debida permutación de renglones de L podemos obtener un cuadrado latino unipotente cuyos elementos de su primer renglón están en orden natural. Inversamente, si aplicamos la debida permutación de renglones a un cuadrado latino unipotente cuyos elementos de su primer renglón están en orden natural obtendremos un cuadrado latino reducido.

Ejemplo 2.3.4. *Sea*

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

un cuadrado latino reducido de orden 4, si aplicamos la permutación $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}$ *a sus renglones obtenemos*

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

que es un cuadrado latino unipotente cuyos elementos en su primer renglón están en orden natural.

El siguiente teorema es consecuencia de lo que se ha dicho antes.

Teorema 2.3.4. *La cardinalidad de cada uno de los siguientes conjuntos son iguales.*

1. *Las* 1*-factorizaciones de* $\overrightarrow{\mathbb{K}_n}$.
2. *Los cuadrados latinos unipotentes de orden n cuyos elementos en su primer renglón están en orden natural.*
3. *Los cuadrados latinos reducidos de orden n.*

A la gráfica completa sin dirección y sin lazos, con n vértices se denota como $\mathbb{K}_n$.

Teorema 2.3.5. *Una* 1*-factorización de* $\mathbb{K}_n$ *existe si y sólo si n es par.*

Demostración. Cada 1-factor consiste de una colección de aristas disjuntas, donde cada arista une 2 vértices, de tal manera que cada 1-factor tiene un número par de vértices y la unión de los 1-factores nos da la gráfica completa, por lo que n tiene que ser par.

Ahora, sea $n = 2m$ y los vértices de $\mathbb{K}_n$ están etiquetados como $\{\infty, 0, 1, \ldots, 2m-2\}$. Con la suma módulo $2m-1$ y definiendo a cada 1-factor como

$$F_i = \{(\infty, i), (i+1, 2m-2+i), (2+i, 2m-3+i), \ldots, (m-1+i, m+i)\}$$

obtenemos una 1-factorización de $\mathbb{K}_n$. □

Ejemplo 2.3.5. *De acuerdo a la demostración del teorema anterior, se construyen los 1-factores para* $\mathbb{K}_6$ $F_1 = \{(\infty, 1), (2, 0), (3, 4)\}$,$F_2 = \{(\infty, 2), (3, 1), (4, 0)\}$,$F_3 = \{(\infty, 3), (4, 2), (0, 1)\}$,$F_4 = \{(\infty, 4), (0, 3), (1, 2)\}$, $F_5 = \{(\infty, 0), (1, 4), (2, 3)\}$. *Esta 1-factorización la observamos en la siguiente gráfica*

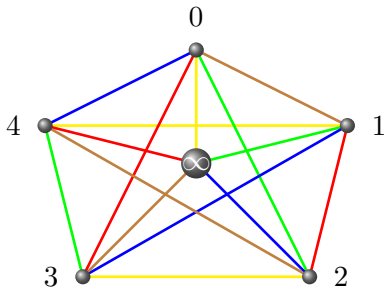


Figura 2.8: 1-factorización de $\mathbb{K}_6$

Usando las mismas etiquetas y orden de los vértices y la misma regla para la asignación de colores se tiene que cualquier 1-factorización de $\mathbb{K}_{2m}$ determina un cuadrado latino reducido, simétrico y unipotente.

Ejemplo 2.3.6. *El cuadrado latino que se obtiene de la 1-factorización de* $\mathbb{K}_6$ *que observamos en la Figura 2.8 es*

$$\begin{pmatrix} & \infty & 0 & 1 & 2 & 3 & 4 \\ \infty & 0 & 1 & 2 & 3 & 4 & 5 \\ 0 & 1 & 0 & 4 & 2 & 5 & 3 \\ 1 & 2 & 4 & 0 & 5 & 3 & 1 \\ 2 & 3 & 2 & 5 & 0 & 1 & 4 \\ 3 & 4 & 5 & 3 & 1 & 0 & 2 \\ 4 & 5 & 3 & 1 & 4 & 2 & 0 \end{pmatrix}.$$

De lo anterior se sigue el siguiente teorema.

Teorema 2.3.6. *El número de 1-factorizaciones de* $\mathbb{K}_{2m}$ *es igual al número de cuadrados latinos reducidos, simétricos y unipotentes.*

El siguiente teorema es de vital importancia, ya que será utilizado en la siguiente subsección.

Teorema 2.3.7. *Sea n par. Un cuadrado latino simétrico y unipotente de orden n es equivalente a una 1-factorización de $\mathbb{K}_n$.*

Demostración. Sea L un cuadrado latino simétrico y unipotente de orden n con conjunto base $B = \{0, 1, \dots\ n-1\}$ donde L tiene ceros en la diagonal principal. Definimos a F_i como

$$F_i = \{\{a, b\} | L(a, b) = i\} \text{ para } i = 1, 2, \dots, n-1.$$

Observe que por ser L simétrico cada arista en F_i aparece dos veces, luego $|F_i| = \frac{n}{2}$. Por ser L un cuadrado latino todas las aristas de F_i determina una partición del conjunto base, es decir, F_i es un 1-factor de $\mathbb{K}_n$. Por otra parte, $F_i \bigcap F_j = \emptyset\ \forall i \neq j$, luego $(F_1, F_2, \dots, F_{n-1})$ determinan una 1-factorización de $\mathbb{K}_n$ como se quería.

Sea $(F_1, F_2, \dots, F_{n-1})$ una 1-factorización de K_n con conjunto de vértices $V = \{1, 2, \dots, n\}$. Para construir nuestro cuadrado latino de orden n con conjunto base $B = \{0, 1, \dots, n-1\}$ asociaremos al 1-factor F_i el elemento $i \in B$ como sigue

$$\{a, b\} \in F_i \Rightarrow L(a, b) = L(b, a) = i,\ L(i, i) = 0, i \in V.$$

Claramente L es un cuadrado latino simétrico y unipotente. □

2.3.3. Número de Ramsey para árboles

Sea G una gráfica finita y k un número natural, una **k-coloración** de un conjunto S es una función $\Phi : S \to \{1, 2, ..., k\}$, aquí $\{1, 2, ..., k\}$ es el conjunto de colores. A una k-coloración de las aristas de una gráfica G la llamaremos simplemente k-coloración de G.

El **número de Ramsey** $r(G, k)$ de G se define como el mínimo número r tal que en toda k-coloración de la gráfica completa $\mathbb{K}_r$ aparece una copia monocromática de G. Sea $\mathcal{G}_n$ una familia de gráficas de tamaño n, de manera natural se define el número de Ramsey $r(\mathcal{G}_n, k)$ de $\mathcal{G}_n$ como

$$r(\mathcal{G}_n, k) = \text{mín}\left\{r| \begin{array}{c}\text{para toda } k\text{-coloración de las aristas de } \mathbb{K}_r, \text{ existe} \\ G \in \mathcal{G}_n \text{ tal que } G \text{ es una subgráfica monocromática de } \mathbb{K}_r\end{array}\right\}.$$

Denotaremos a la familia de árboles con n aristas o tamaño n ($n+1$ vértices) como $\mathcal{T}_n$.

A continuación mostraremos una cota inferior para $r(\mathcal{T}_n, k)$ mediante el uso conveniente de cuadrados latinos. Proponemos una prueba muy sencilla para la cota inferior de $r(\mathcal{T}_n, k)$, como alternativa a la demostración original de Bierbrauer y Brandis en [3].

Dadas las gráficas $G_1 = (V_1, E_1)$ y $G_1 = (V_2, E_2)$ con $V_1 \cap V_2 = \varnothing$, la **suma** de G_1 con G_2 es la gráfica definida como

$$G_1 + G_2 = (V_1 \cup V_2,\ E_1 \cup E_2 \cup \{\{x, y\} : x \in V_1,\ y \in V_2\}).$$

Teorema 2.3.8 (Bierbrauer y Brandis)**.** *Sean $n, k > 1$. Entonces*

$$r(\mathcal{T}_n, k) > 2\left\lfloor \frac{k+1}{2} \right\rfloor \left\lfloor \frac{n}{2} \right\rfloor.$$

Demostración. Sean $r = \left\lfloor \frac{k+1}{2} \right\rfloor, s = \left\lfloor \frac{n}{2} \right\rfloor$ y $t = 2rs$. Consideremos $\mathbb{K}_t$ como la suma de $2r$ copias de $\mathbb{K}_s$ etiquetadas como $\mathbb{K}_s^{(1)}, \mathbb{K}_s^{(2)}, ..., \mathbb{K}_s^{(2r)}$ respectivamente. Por el Teorema 2.3.5 sabemos que $\mathbb{K}_{2r}$ es 1-factorizable, denotemos por $F_1, F_2, ..., F_{2r-1}$ a los 1-factores de dicha 1-factorización. Una $(2r-1)$-coloración de $\mathbb{K}_{2r}$ resulta de asignar el color i a las aristas del 1-factor F_i, $i = 1, ..., 2r-1$. De manera natural, esta $(2r-1)$-coloración de $\mathbb{K}_{2r}$ determina una $(2r-1)$-coloración de $\mathbb{K}_t$ como sigue. Sea $V_{2r} = \{1, 2, ..., 2r\}$ el conjunto de vértices de $\mathbb{K}_{2r}$ entonces las aristas entre $\mathbb{K}_s^{(i)}$ y $\mathbb{K}_s^{(j)}$ en $\mathbb{K}_t$ tendrán el color de la arista $\{i, j\}$ en $\mathbb{K}_{2r}$; al resto de las aristas de $\mathbb{K}_t$ le asignamos cualquier color. Claramente, el número de vértices en una componente conexa monocromática no excede n, lo cual nos garantiza que dicha coloración de $\mathbb{K}_t$ es libre de copias monocromáticas de algún árbol de tamaño n, como se quería probar. □

Vale la pena aclarar que esta prueba es esencialmente la misma que la mostrada originalmente en [3]. La demostración que proponen Bierbrauer y Brandis depende de la complicada construcción de una familia de cuadrados latinos simétricos y unipotentes de orden par, pero como vimos en la subsección anterior, no es difícil comprobar que toda 1-factorización de $\mathbb{K}_{2r}$ se puede interpretar

como un cuadrado latino de este tipo (ver Teorema 2.3.7.). Es realmente curioso que este hecho fuera pasado por alto.

Ejemplo 2.3.7. *Sea* $n = 3$, $k = 6$. *Entonces por el teorema anterior tenemos que el número de Ramsey*

$$r(\mathcal{T}_3, 6) > 2\left\lfloor \frac{3}{2} \right\rfloor \left\lfloor \frac{6+1}{2} \right\rfloor = 6$$

Es decir, existe una 6*-coloración de la gráfica completa* $\mathbb{K}_6$ *libre de árboles de tamaño 3 monocromáticos. En este caso* $t = 2(3)\lfloor \frac{3}{2} \rfloor = 6$ *y* $s = 1$. *Entonces*

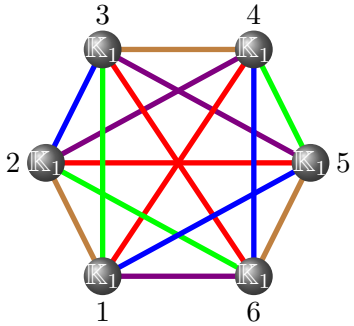
$$\mathbb{K}_6 = \sum_{i=1}^{6} \mathbb{K}_1^{(i)}.$$

Sea $B(6)$ *el cuadrado latino de orden 6 que utilizaremos para dar la* 6*-coloración de* $\mathbb{K}_6$.

	$\mathbb{K}_1^{(1)}$	$\mathbb{K}_1^{(2)}$	$\mathbb{K}_1^{(3)}$	$\mathbb{K}_1^{(4)}$	$\mathbb{K}_1^{(5)}$	$\mathbb{K}_1^{(6)}$
$\mathbb{K}_1^{(1)}$	*1*	*2*	*3*	*4*	*5*	*6*
$\mathbb{K}_1^{(2)}$	*2*	*1*	*5*	*6*	*4*	*3*
$\mathbb{K}_1^{(3)}$	*3*	*5*	*1*	*2*	*6*	*4*
$\mathbb{K}_1^{(4)}$	*4*	*6*	*2*	*1*	*3*	*5*
$\mathbb{K}_1^{(5)}$	*5*	*4*	*6*	*3*	*1*	*2*
$\mathbb{K}_1^{(6)}$	*6*	*3*	*4*	*5*	*2*	*1*

donde $b_{i,j} \in B(6)$ *nos indica el color de las aristas que van de* $\mathbb{K}_1^{(i)}$ *a* $\mathbb{K}_1^{(j)}$ *y cuya correspondencia de colores es*

$$2 \to cafe, 3 \to verde, 4 \to rojo, 5 \to azul, 6 \to morado.$$



2.4. Sistema de Ternas de Steiner

En esta sección presentamos el uso de los cuadrados latinos en la construcción de Sistemas de Ternas de Steiner mediante el Método de Bose y el Método de Skolem. Para ello, se usarán dos tipos de cuadrados latinos: los simétricos e idempotentes; y los simétricos y semi-idempotentes. El desarrollo de esta sección esta apoyado en [9, 8].

Un **Sistema de Ternas de Steiner** (STS) es un par ordenado (S, T) donde S es un conjunto finito de símbolos y T es un conjunto de subconjuntos de tres elementos de S llamados **ternas**, tal que cada par de elementos distintos de S aparecen exactamente en una terna de T. El orden de un STS es la cardinalidad del conjunto S.

Fue W. S. B. Woolhouse quien en 1844 se preguntó: "¿Para cuáles enteros positivos v existe un Sistema de Ternas de Steiner de orden v". Este problema fue resuelto en 1847 por Rev. T. P. Kirkman, quien probó el siguiente resultado.

Teorema 2.4.1. *Un STS de orden v existe si y sólo si $v \equiv 1, 3 \bmod 6$.*

Otro resultado importante es el siguiente

Teorema 2.4.2. *Sea S un conjunto de tamaño v y sea T un conjunto de subconjuntos de 3 elementos de S. Si se cumple que*

(a) cada par de elementos distintos de S pertenecen al menos a una terna de T y

(b) $|T| \leq \frac{v(v-1)}{6}$.

Entonces (S, T) es un STS de orden v.

Recordemos que un cuasigrupo de orden n es un par $(Q, \circ)$ donde Q es un conjunto de cardinalidad n y $\circ$ es una operación binaria sobre los elementos de Q, tal que para todo par de elementos $a, b \in Q$ las ecuaciones $a \circ x = b$ y $y \circ a = b$ tienen soluciones únicas y además su tabla de Cayley es un cuadrado latino.

Un cuadrado latino L (cuasigrupo) es llamado **idempotente** si la celda $L(i, i) = i$ para $1 \leq i \leq n$. Recordemos que un cuadrado latino es llamado **simétrico** si $L(i, j) = L(j, i)$ para $1 \leq i, j \leq n$.

Proposición 2.4.1. *Para todo $n \geq 1$, existe un cuadrado latino simétrico e idempotente de orden $2n + 1$.*

Demostración. Sea $n \geq 1$, consideremos al grupo cíclico $(\mathbb{Z}_{2n+1}, +)$, cuya tabla de Cayley es el cuadrado latino simétrico de orden $2n + 1$

$+$	0	1	2	$\cdots$	2n
0	0	1	2	$\cdots$	2n
1	1	2	3	$\cdots$	0
2	2	3	4	$\cdots$	1
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
2n	2n	0	1	$\cdots$	2n-1

Dado que los elementos pares se encuentran en la diagonal principal de la tabla, entonces a éstos les asignaremos los números del 1 al $n+1$ de modo que la entrada (i,i) de la tabla contenga el elemento i y los elementos que aún no se han renombrado se le asignaran los número del $n+2$ al $2n+1$. De esta forma el cuadrado latino resultante es simétrico e idempotente de orden $2n+1$. □

2.4.1. Método de Bose ($v \equiv 3 \bmod 6$)

Presentamos el método desarrollado por Bose para construir un STS de orden v, donde ($v \equiv 3 \bmod 6$) (Ver [17]).

Teorema 2.4.3. *Sea $v = 6n+3$ y $(Q, \circ)$ un cuasigrupo simétrico e idempotente de orden $2n+1$, donde $Q = \{1, 2, 3, \ldots, 2n+1\}$. Sea $S = Q \times \{1, 2, 3\}$ y definimos dos tipos de ternas*

Tipo 1 *Para $1 \leq i \leq 2n+1$, $\{(i,1),(i,2),(i,3)\} \in T$.*

Tipo 2 *Para $1 \leq i < j \leq 2n+1$, $\{(i,1),(j,1),(i \circ j, 2)\}$,$\{(i,2),(j,2),(i \circ j, 3)\}$, $\{(i,3),(j,3),(i \circ j, 1)\} \in T$.*

Entonces (S, T) es un STS de orden $6n+3$.

Demostración. Iniciamos contando el número de ternas de T. Las ternas de Tipo 1 son $2n+1$ y por definición de las ternas de Tipo 2 hay $\binom{2n+1}{2} = \frac{(2n+1)(2n)}{2}$ formas de elegir a i y j , cada una de las cuales nos determina tres ternas de Tipo 2. Por lo cual, el número total de ternas es

$$\begin{aligned} |T| &= (2n+1) + 3\left(\frac{(2n+1)(2n)}{2}\right) \\ &= (2n+1)(3n+1) \\ &= \frac{v(v-1)}{6} \end{aligned}$$

por lo tanto T contiene el número correcto de ternas. Ahora, falta verificar que cada par de elementos distintos de S aparecen juntos en al menos una terna de T.

Sea (a,b) y (c,d) un par de elementos distintos de S. Consideramos tres casos

(1) Si $a = c$, entonces la terna $\{(a,1),(a,2),(a,3)\} \in T$ de Tipo 1 contiene a (a,b) y (c,d).

(2) Si $b = d$, entonces $a \neq c$ y así la terna $\{(a, b), (c, b), (a \circ c, b + 1)\} \in T$ contiene a (a, b) y (c, d) (La adición en la segunda coordenada es módulo 3, donde $0 = 3$).

(3) Si $a \neq c$ y $b \neq d$. Supongamos que $b = 1$ y $d = 2$, para los otros casos es procedimiento es similar. Entonces, por ser $(Q, \circ)$ un cuasigrupo tenemos que existe $i \in Q$ tal que $a \circ i = c$ y por ser $(Q, \circ)$ idempotente y $a \neq c$ tenemos que $i \neq a$. Por lo tanto la terna $\{(a, 1), (i, 1), (a \circ i = c, 2)\} \in T$ de Tipo 2 contiene a (a, b) y (c, d).

Por lo tanto (S, T) es un STS de orden $6n + 3$. □

Ejemplo 2.4.1. *Construcción de un STS de orden 15.*

Tenemos que $15 = 6(2) + 3$*, entonces* $n = 2$*. Por lo cual necesitamos un cuasigrupo simétrico e idempotente de orden* $2(2) + 1 = 5$*.*
Sea

$\circ$	*1*	*2*	*3*	*4*	*5*
1	*1*	*5*	*2*	*3*	*4*
2	*5*	*2*	*4*	*1*	*3*
3	*2*	*4*	*3*	*5*	*1*
4	*3*	*1*	*5*	*4*	*2*
5	*4*	*3*	*1*	*2*	*5*

la tabla de Cayley asociada al cuasigrupo y $S = \{1, 2, 3, 4, 5\} \times \{1, 2, 3\}$*. Entonces las ternas de Tipo 1 son*

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

y las ternas de Tipo 2 son

Para $i = 1$ *y* $j = 2$	*Para* $i = 1$ *y* $j = 3$	*Para* $i = 1$ *y* $j = 4$
$\{(1,1),(2,1),(5,2)\}$	$\{(1,1),(3,1),(2,2)\}$	$\{(1,1),(4,1),(3,2)\}$
$\{(1,2),(2,2),(5,3)\}$	$\{(1,2),(3,2),(2,3)\}$	$\{(1,2),(4,2),(3,3)\}$
$\{(1,3),(2,3),(5,1)\}$	$\{(1,3),(3,3),(2,1)\}$	$\{(1,3),(4,3),(3,1)\}$
Para $i = 1$ *y* $j = 5$	*Para* $i = 2$ *y* $j = 3$	*Para* $i = 2$ *y* $j = 4$
$\{(1,1),(5,1),(4,2)\}$	$\{(2,1),(3,1),(4,2)\}$	$\{(2,1),(4,1),(1,2)\}$
$\{(1,2),(5,2),(4,3)\}$	$\{(2,2),(3,2),(4,3)\}$	$\{(2,2),(4,2),(1,3)\}$
$\{(1,3),(5,3),(4,1)\}$	$\{(2,3),(3,3),(4,1)\}$	$\{(2,3),(4,3),(1,1)\}$
Para $i = 2$ *y* $j = 5$	*Para* $i = 3$ *y* $j = 4$	*Para* $i = 3$ *y* $j = 5$
$\{(2,1),(5,1),(3,2)\}$	$\{(3,1),(4,1),(5,2)\}$	$\{(3,1),(5,1),(1,2)\}$
$\{(2,2),(5,2),(3,3)\}$	$\{(3,2),(4,2),(5,3)\}$	$\{(3,2),(5,2),(1,3)\}$
$\{(2,3),(5,3),(3,1)\}$	$\{(3,3),(4,3),(5,1)\}$	$\{(3,3),(5,3),(1,1)\}$
	Para $i = 4$ *y* $j = 5$	
	$\{(4,1),(5,1),(2,2)\}$	
	$\{(4,2),(5,2),(2,3)\}$	
	$\{(4,3),(5,3),(2,1)\}$	

Un cuadrado latino (cuasigrupo) L de orden $2n$ es llamado **semi-idempotente** si $L(i,i) = L(n+i, n+i) = i$ para $1 \leq i \leq n$.

Proposición 2.4.2. *Para todo $n \geq 1$, existe un cuadrado latino simétrico y semi-idempotente de orden $2n$.*

Demostración. Sea $n \geq 1$, consideremos al grupo $(\mathbb{Z}_{2n}, +)$ cuya tabla de Cayley es

+	0	1	2	$\cdots$	n	n+1	$\cdots$	2n-1
0	0	1	2	$\cdots$	n	n+1	$\cdots$	2n-1
1	1	2	3	$\cdots$	n+1	n+2	$\cdots$	0
2	2	3	4	$\cdots$	n+2	n+3	$\cdots$	1
$\vdots$	$\vdots$							$\vdots$
n	n	n+1	n+2	$\cdots$	0	1	$\cdots$	n-1
n+1	n+1	n+2	n+3	$\cdots$	1	2	$\cdots$	n
$\vdots$	$\vdots$						$\ddots$	$\vdots$
2n-1	2n-1	0	1	$\cdots$	n-1	n	$\cdots$	2n-2

Como observamos los primeros n elementos pares de $\mathbb{Z}_{2n}$ aparecen en la diagonal principal y después vuelven a repetirse, de modo que si renombramos a estos elementos con los números del 1 al n y asignamos los números del $n+1$ al $2n$ al resto de los elementos que faltan, el cuadrado latino resultante es simétrico y semi-idempotente de orden $2n$. □

2.4.2. Método de Skolem ($v \equiv 1 \bmod 6$)

Ahora, Presentamos el método desarrollado por Skolem para construir un STS de orden v, donde ($v \equiv 1 \bmod 6$) (Ver [18]).

Teorema 2.4.4. *Sea $v = 6n+1$ y $(Q, \circ)$ un cuasigrupo simétrico y semi-idempotente de orden $2n$ donde $Q = \{1, 2, \ldots, 2n\}$. Sea $S = \{\infty\} \bigcup (Q \times \{1, 2, 3\})$ y en T se definen tres tipos de ternas.*

Tipo 1 *Para $1 \leq i \leq n$, $\{(i,1),(i,2),(i,3)\} \in T$*

Tipo 2 *Para $1 \leq i \leq n$, $\{\infty,(n+i,1),(i,2)\}$,$\{\infty,(n+i,2),(i,3)\}$,$\{\infty,(n+i,3),(i,1)\} \in T$*

Tipo 3 *Para $1 \leq i < j \leq 2n$, $\{(i,1),(j,1),(i \circ j,2)\}$, $\{(i,2),(j,2),(i \circ j,3)\}$, $\{(i,3),(j,3),(i \circ j,1)\} \in T$.*

Entonces (S, T) es un STS de orden $6n+1$.

Demostración. Primero contemos las ternas de T. Ternas de Tipo 1 hay n, de Tipo 2 $3n$ y de Tipo 3 hay $3\binom{2n}{2} = 3n(2n-1)$. Por lo cual, el número total de ternas es

$$\begin{aligned} |T| &= n + 3n + 3n(2n-1) \\ &= n(6n+1) \\ &= \frac{v(v-1)}{6} \end{aligned}$$

Ahora, verifiquemos que cada par de elementos distintos de S aparecen juntos en al menos una terna de T.

Sean ∞ y $(a, b) \in S$

- si $1 \leq a \leq n$ entonces la terna de Tipo 2 $\{\infty,(n+a,b-1),(a,b)\}$ contiene a ∞ y (a, b).
- si $n+1 \leq a \leq 2n$ entonces la terna de Tipo 2 $\{\infty,(a,b),(a-n,b+1)\}$ contiene a ∞ y (a, b).

Sean (a, b) y (c, d) elementos distintos de S.

- Si $a = c$, entonces la terna de Tipo 1 $\{(a,1),(a,2),(a,3)\}$ contiene a la pareja (a, b) y (c, d).
- Si $b = d$, entonces la terna de Tipo 3 $\{(i,b),(j,b),(i \circ j, b+1)\}$ contiene a la pareja (a, b) y (c, d).
- Si $a \neq c$ y $b \neq d$.
  Sea $\Phi : \{\infty\} \bigcup (Q \times \{1,2,3\}) \to \{\infty\} \bigcup (Q \times \{1,2,3\})$ donde
  $\infty \mapsto \infty$ y $(a, b) \mapsto (a, b+1)$ un automorfismo de T. Sin perdida de generalidad podemos suponer que $b = 1$ y $d = 2$.

- Si $c \in \{1, 2, \ldots, n\}$ y como $a \neq c$
  - Sea $a = n + c$, entonces la terna de Tipo 2 $\{\infty, (n + c, 1), (c, 2)\} \in T$ contiene al par $(n + 1, 1)$ y $(c, 2)$.
  - Sea $a \neq n + c$, entonces la terna $\{(a, 1), (x, 1), (c, 2)\} \in T$ contiene al par $(a, 1)$ y $(c, 2)$.
- Si $c \notin \{1, 2, \ldots, n\}$, entonces por ser Q idempotente existe $x \neq a$ tal que $a \circ x = c$, luego la terna $\{(a, 1), (x, 1), (c, 2)\} \in T$ contiene al par $(a, 1)$ y $(c, 2)$.

□

Ejemplo 2.4.2. *Usamos el Método de Skolem para construir un STS de orden 13.*

Tenemos que $v = 19 = 6(3) + 1$*, entonces* $n = 3$ *,* $Q = \{1, 2, 3, 4, 5, 6\}$ *y el cuasigrupo de orden* $2(3) = 6$ *es*

$\circ$	*1*	*2*	*3*	*4*	*5*	*6*
1	*1*	*3*	*4*	*2*	*5*	*6*
2	*3*	*2*	*5*	*4*	*6*	*1*
3	*4*	*5*	*3*	*6*	*1*	*2*
4	*2*	*4*	*6*	*1*	*3*	*5*
5	*5*	*6*	*1*	*3*	*2*	*4*
6	*6*	*1*	*2*	*5*	*4*	*3*

Las ternas de Tipo 1 son

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

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

Las ternas de Tipo 2 son

i=1	$\{\infty,(4,1),(1,2)\}$	$\{\infty,(4,2),(1,3)\}$	$\{\infty,(4,3),(1,1)\}$
i=2	$\{\infty,(5,1),(2,2)\}$	$\{\infty,(5,2),(2,3)\}$	$\{\infty,(5,3),(2,1)\}$
i=3	$\{\infty,(6,1),(3,2)\}$	$\{\infty,(6,2),(3,3)\}$	$\{\infty,(6,3),(3,1)\}$

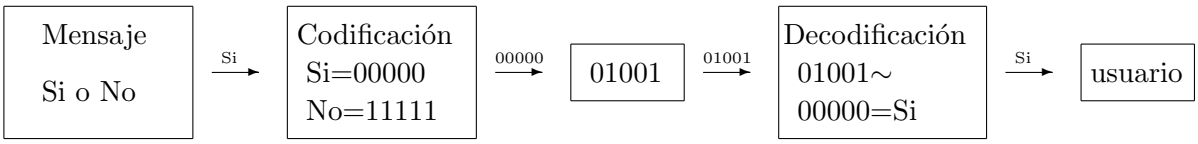
y algunas de las ternas de Tipo 3 son

Para i=1 y j=2	$\{(1,1),(2,1),(3,2)\}$	$\{(1,2),(2,2),(3,3)\}$	$\{(1,3),(2,3),(3,1)\}$
Para i=1 y j=3	$\{(1,1),(3,1),(4,2)\}$	$\{(1,2),(3,2),(4,3)\}$	$\{(1,3),(3,3),(4,1)\}$
Para i=1 y j=4	$\{(1,1),(4,1),(2,2)\}$	$\{(1,2),(4,2),(2,3)\}$	$\{(1,3),(4,3),(2,1)\}$
Para i=1 y j=5	$\{(1,1),(5,1),(5,2)\}$	$\{(1,2),(5,2),(5,3)\}$	$\{(1,3),(5,3),(5,1)\}$
Para i=1 y j=6	$\{(1,1),(6,1),(6,2)\}$	$\{(1,2),(6,2),(6,3)\}$	$\{(1,3),(6,3),(6,1)\}$

2.5. Corrección de Errores

En esta sección mostraremos el uso de los cuadrados latinos ortogonales en la construcción de códigos correctores de errores, basándonos en [4].

Los códigos correctores de errores son usados como su nombre lo indica, para corregir errores cuando se transmiten mensajes a través de un canal de comunicación ruidoso. Por ejemplo, si se quiere enviar un dato binario a través de un canal ruidoso lo más rápido y de la manera más confiable como sea posible. El canal puede ser una línea de teléfono, una estación de radio de alta frecuencia, entre otros. El ruido puede ser un error humano, imperfecciones en el equipo, ruido térmico, etc. lo que da lugar a que el dato recibido sea distinto al enviado. El objetivo de un código corrector de errores es codificar el mensaje, mediante la adición de una cierta cantidad de redundancia al mismo, de tal manera que el mensaje original se pueda recuperar si se han producido errores durante su trans-



misión.
En el ejemplo anterior ocurren dos errores, entonces el decodificador debe decodificar el vector recibido 01001 con la palabra más cercana, respecto a la distancia de Hamming, que es 00000 o Si.

Un **código q-ario** es un conjunto de secuencias de símbolos donde cada símbolo es elegido de un conjunto $F_q = \{\lambda_1, \lambda_2, \ldots, \lambda_q\}$ de q distintos elementos. El conjunto F_q es llamado el alfabeto y a menudo se considera el conjunto $Z_q = \{0, 1, 2, \ldots, q-1\}$. Sea $(F_q)^n$ el conjunto de todas la *n-uplas* $a = a_1 a_2 \cdots a_n$ donde cada $a_i \in F_q$. Los elementos de $(F_q)^n$ son llamados **vectores** o **palabras**. El orden del conjunto $(F_q)^n$ es q^n. Un código q-ario de longitud n es un subconjunto de $(F_q)^n$. Un **código-**(n, M, d) es un código de longitud n que contiene M palabras y tiene distancia mínima d. Como habíamos mencionado, esta distancia es respecto a la distancia de Hamming que se define como sigue.

La **distancia de Hamming** entre dos vectores x y y de $(F_q)^n$ denotada por $d(x, y)$ es el número de lugares en donde los vectores difieren. Esta distancia satisface las siguientes condiciones:

(i) $d(x, y) = 0$ si y sólo si $x = y$.

(ii) $d(x, y) = d(y, x)$ para todo $x, y \in (F_q)^n$.

(iii) $d(x, y) \leq d(x, z) + d(z, y)$ para todo $x, y, z \in (F_q)^n$.

La **distancia mínima** de un código C se define como

$$d(C) = \text{mín}\{d(x, y)|x, y \in C, x \neq y\}.$$

No debemos pasar por alto los siguientes resultados de los códigos correctores.

Teorema 2.5.1. *Para un código C se tiene que*

(i) C puede detectar hasta s errores en cualquier palabra si $d(C) \geq s + 1$.

(ii) C puede corregir hasta t errores en cualquier palabra si $d(C) \geq 2t + 1$.

Corolario 2.5.1. *Si un código C tiene distancia mínima d, entonces C se puede utilizar*

(i) para detectar hasta $d - 1$ errores.

(ii) para corregir hasta $\lfloor (d - 1)/2 \rfloor$ errores en cualquier palabra.

Se dice que un código-(n, M, d) es bueno, cuando n es pequeño (para transmitir mensajes de forma rápida), M es grande (permite transmitir una gran variedad de mensajes) y d grande (permite corregir muchos errores). De tal manera que el problema principal de la Teoría de Códigos es optimizar uno de los parámetros n, M, d para valores dados de los otros dos. El problema mas común es encontrar el código más grande, dada la longitud de las palabras y la distancia mínima entre ellas.

Denotaremos a $A_q(n, d)$ como el valor más grande de M para el cual existe un código-(n, M, d) q-ario. Sobre un alfabeto arbitrario, vamos a considerar el problema más común de la Teoría de Codificación para los códigos de tamaño 4 y distancia mínima 3, es decir, el problema de encontrar el valor de $A_q(4, 3)$. El siguiente teorema nos da una cota superior para tal valor.

Teorema 2.5.2. *$A_q(4, 3) \leq q^2$, para todo q.*

Demostración. Supongamos que C es un código-$(4, M, 3)$ q-ario y sean $x = x_1x_2x_3x_4$ y $y = y_1y_2y_3y_4$ palabras distintas de C. Entonces $(x_1x_2) \neq (y_1y_2)$, ya que de otro modo x y y podrían diferir en los últimos dos lugares, contradiciendo el hecho que $d(C) = 3$. Así los M pares ordenados obtenidos por suprimir las dos últimas coordenadas de C son todos vectores distintos de $(F_q)^2$ y así $M \leq q^2$. □

Ahora, haremos uso de los cuadrados latinos ortogonales para la construcción de los códigos $(4, M, 3)$ q-arios.

Teorema 2.5.3. *Existe un código-$(4, q^2, 3)$ si y sólo si existe un par de $MOLS$ de orden q.*

Demostración. Mostraremos que un código

$$C = \{(i, j, a_{ij}, b_{ij}) | (i, j) \in (F_q)^2\}$$

es un código-$(4, q^2, 3)$ si y sólo si $A = (a_{ij})$ y $B = (b_{ij})$ forman un par de $MOLS$ de orden q.

La distancia mínima de C es 3 si y sólo si para cada par de posiciones coordenadas, los pares ordenados que aparecen en esas posiciones son distintos.

Ahora, los q^2 pares (i, a_{ij}) son distintos y los q^2 pares (j, a_{ij}) son distintos si y sólo si A es un cuadrado latino. De manera similar los q^2 pares (i, b_{ij}) son distintos y los q^2 pares (j, b_{ij}) son distintos si y sólo si B es un cuadrado latino. Finalmente los q^2 pares (a_{ij}, b_{ij}) son distintos si y sólo si A y B son mutuamente ortogonales. □

El teorema anterior nos muestra que $A_q(4, 3) = q^2$ si y sólo si existe un par de $MOLS$ de orden q.

Ejemplo 2.5.1. *Construyamos el código-$(4, q^2, 3)$ con $q = 4$. Por el teorema anterior, necesitamos un par de cuadrados latinos de orden 4 ortogonales para construir tal código.*

Sean

$$A = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 3 & 2 & 1 & 0 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \end{pmatrix} \text{ y } B = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \\ 1 & 0 & 3 & 2 \end{pmatrix}$$

cuadrados latinos ortogonales de orden 4. De tal manera que los elementos del código definidos como

$$C = \{(i, j, a_{ij}, b_{ij}) | (i, j) \in (F_4)^2\}$$

son

i	j	a_{ij}	b_{ij}
0	*0*	*0*	*0*
0	*1*	*1*	*1*
0	*2*	*2*	*2*
0	*3*	*3*	*3*
1	*0*	*3*	*2*
1	*1*	*2*	*3*
1	*2*	*1*	*0*
1	*3*	*0*	*1*
2	*0*	*1*	*3*
2	*1*	*0*	*2*
2	*2*	*3*	*1*
2	*3*	*2*	*0*
3	*0*	*2*	*1*
3	*1*	*3*	*0*
3	*2*	*0*	*3*
3	*3*	*1*	*2*

Como vimos en la sección 1.6, tenemos que para todo $q \neq 2, 6$ existe un par de $MOLS$ de orden q. De tal manera que el siguiente corolario es consecuencia de tal afirmación.

Corolario 2.5.2. $A_q(4,3) = q^2$ *para todo* $q \neq 2, 6$.

Ahora, para $q = 2$ Tenemos que $A_2(4,3) = 2$

0	0	0	0
0	1	1	1

y para $q = 6$ se tiene

Teorema 2.5.4. $A_6(4,3) = 34$

Demostración. Las matrices

$$A = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 1 & 0 & 3 & 2 & 5 & 4 \\ 2 & 3 & 5 & 4 & 0 & 1 \\ 3 & 2 & 4 & 5 & 1 & 0 \\ 4 & 5 & 1 & 0 & 3 & 2 \\ 5 & 4 & 0 & 1 & 2 & 3 \end{pmatrix} \text{ y } B = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 0 & 1 \\ 1 & 0 & 3 & 2 & 5 & 4 \\ 5 & 4 & 0 & 1 & 3 & 2 \\ 3 & 2 & 5 & 4 & 1 & 0 \\ 4 & 5 & 1 & 0 & 2 & 3 \end{pmatrix}$$

forman un par de cuadrados latinos de orden 6, los cuales están lo mas cercano posible a ser ortogonales, ya que solo fallan en $(a_{65}, b_{65}) = (a_{13}, b_{13})$ y $(a_{66}, b_{66}) = (a_{14}, b_{14})$. Así el código

$$\{(i, j, a_{ij}, b_{ij}) | (i, j) \in (F_6)^2, (i, j) \neq (6, 5) \text{ o } (6, 6)\}$$

es un código-$(4, 34, 3)$. □

Recordemos que dado q, existen a lo más $q-1$ $MOLS$ de orden q y que para q potencia de un primo existen $q-1$ $MOLS$ de orden q. En 1964 Singleton da la siguiente cota

Teorema 2.5.5. $A_q(n,d) \leq q^{n-d+1}$.

Demostración. Supongamos que C es un código-(n, M, d). Entonces suprimimos las últimas $d-1$ coordenadas para cada palabra del código. De tal manera que las cadenas M de tamaño $n-d+1$, así obtenidos deben de ser distintos y por lo tanto $M \leq q^{n-d+1}$. □

El siguiente teorema nos dice que existe una equivalencia entre los $MOLS$ y los códigos correctores de errores.

Teorema 2.5.6. *Un código-$(n, q^2, n-1)$ sobre F_q es equivalente a un conjunto de $n-2$ $MOLS$.*

Demostración. Un código-$(n, q^2, n-1)$ C sobre F_q tiene la forma

$$\{(i, j, a_{ij}^{(1)}, a_{ij}^{(2)}, \ldots, a_{ij}^{(n-2)}) | (i,j) \in (F_q)^2\}$$

Mostremos que $d(C) = (n-1)$ si y sólo si $A_1, A_2, \ldots, A_{n-2}$ donde $A_k = (a_{ij}^{(k)})$ forman un conjunto de $MOLS$ de orden q.

$d(C) = n-1$ si y sólo si en cada par de posiciones coordenadas, los pares ordenados que aparecen en esas posiciones son distintos. Ahora los q^2 pares $(i, a_{ij}^{(k)})$ y los q^2 pares $(j, a_{ij}^{(k)})$ son distintos si y sólo si A_k es un cuadrado latino, para $k = 1, 2, \ldots, n-2$.

Para $k \neq r$. Los q^2 pares $(a_{ij}^{(k)}, a_{ij}^{(r)})$ son distintos si y sólo si A_k y A_r son mutuamente ortogonales con $k, r = 1, \ldots, n-2$. Esto se cumple si y sólo si $A_1, A_2, \ldots, A_{n-2}$ es un conjunto de $n-2$ $MOLS$ de orden q. □

Corolario 2.5.3. $A_q(3,2) = q^2$ *para todo entero positivo q.*

Demostración. Un código-$(3, q^2, 2)$ sobre F_q es equivalente a tener un cuadrado latino de orden q, el cual sabemos existe para cualquier q. Sea

$$C = \{(i, j, a_{ij}) | (i,j) \in (F_q)^2\}.$$

Los q^2 pares (i, a_{ij}) y los q^2 pares (j, a_{ij}) son distintos si y sólo si $A = (a_{ij})$ es un cuadrado latino. □

El siguiente corolario se deriva de los resultados anteriores.

Corolario 2.5.4. *Si q es potencia de un primo y $n \leq q+1$, entonces*

$$A_q(n, n-1) = q^2.$$

Ejemplo 2.5.2. *Construyamos el código-$(5, 15, 4)$ sobre F_4. Sean*

$$A_1 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{pmatrix}, A_2 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 3 & 2 & 1 & 0 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \end{pmatrix}, A_3 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \\ 1 & 0 & 3 & 2 \end{pmatrix}$$

3 MOLS de orden 4. Entonces el código

$$C = \{(i, j, a_{ij}^{(1)}, a_{ij}^{(2)}, a_{ij}^{(3)}) | (i, j) \in (F_4^2)\}$$

es

i	j	a_{ij}^1	a_{ij}^2	a_{ij}^3
0	*0*	*0*	*0*	*0*
0	*1*	*1*	*1*	*1*
0	*2*	*2*	*2*	*2*
0	*3*	*3*	*3*	*3*
1	*0*	*1*	*3*	*2*
1	*1*	*0*	*2*	*3*
1	*2*	*3*	*1*	*0*
1	*3*	*2*	*0*	*1*
2	*0*	*2*	*1*	*3*
2	*1*	*3*	*0*	*2*
2	*2*	*0*	*3*	*1*
2	*3*	*1*	*2*	*0*
3	*0*	*3*	*2*	*1*
3	*1*	*2*	*3*	*0*
3	*2*	*1*	*0*	*3*
3	*3*	*0*	*1*	*2*

2.6. Criptología

En esta sección mostramos algunas de las maneras en que los cuadrados latinos son usados en la criptología. Para el desarrollo de la primera subsección nos apoyamos en [1].

La **criptología** (del griego krypto y logos, estudio de lo oculto, lo escondido) es la ciencia que trata los problemas teóricos relacionados con la seguridad en el intercambio de mensajes en clave entre un emisor y un receptor a través de un canal de comunicaciones. Esta ciencia está dividida en dos grandes ramas: **la criptografía**, ocupada de encriptar y desencriptar, o lo que es lo mismo, cifrar y descifrar mensajes, y el **criptoanálisis**, que trata de descifrar los mensajes sin tener la autorización, rompiendo así el criptosistema.

Para establecer un criptosistema, necesitamos una **clave** K, un mensaje M, un esquema de cifrado E_k para encriptar el mensaje M y formar un texto cifrado C y un esquema de descifrado D_k para desencriptar el texto cifrado. De tal manera que dado un mensaje M este es cifrado como $C = E_k(M)$ y el texto cifrado C es trasmitido. El esquema de descifrado obtiene el mensaje original M vía el calculo de $D_k(C) = M$.

Con el fin de poder recuperar el mismo mensaje M que fue enviado, la función del mensaje E_k debe ser 1-1 tal que los mensajes distintos son mensajes cifrados dentro de textos cifrados distintos.

Una forma sencilla de utilizar a los cuadrados latinos para ocultar información es la siguiente.

Recordemos que en un sistema de encriptación se requiere esencialmente que los usuarios mantengan una clave (secreta) que solo ellos conocen o tienen acceso. Si la clave es interceptada el sistema debe ser considerado inseguro.

Supongamos que tenemos un conjunto $\{L_1, L_2, \ldots, L_k\}$ de $MOLS$ de orden n y que las partes están de acuerdo en tener como clave a los cuadrados latinos L_c y L_d con $c \neq d$.

Supongamos que nuestro mensaje en texto en claro es (i, j) y es cifrado como (α, β) que es el par que se encuentra en la intersección del renglón i y la columna j de los cuadrados latinos L_c y L_d. Para descifrar el texto cifrado simplemente se exploran los cuadrados L_c y L_d hasta que el par (α, β) es encontrado y por la ortogonalidad de los cuadrados latinos el par (α, β) aparecerá solo en las coordenadas (i, j) donde (i, j) es el mensaje original.

Ejemplo 2.6.1. *Sea el conjunto de 3 MOLS de orden 4*

$$L_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{pmatrix}, L_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \end{pmatrix}, L_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

Supongamos que Alice y Bob acuerdan que su clave secreta esta dada por los cuadrados L_2 y L_3, entonces si Alice quiere enviar el mensaje $(2, 4)$ a Bob, ella cifra el mensaje señalando que en los cuadrados L_2 y L_3 el par $(\alpha, \beta) = (2, 1)$ aparece en las coordenadas $(2, 4)$. Así $(2, 4)$ es cifrado como $(2, 1)$ el cual es enviado a Bob. Para descifrar Bob explora los cuadrados L_2 y L_3 y encuentra el

par $(2,1)$ *en la posición* $(2,4)$ *de los cuadrados y por lo tanto se sabe que el mensaje original es* $(2,4)$.

Notemos que al tener k $MOLS$, tenemos $\binom{k}{2}$ posibles claves y existen n^2 posibles mensajes.

Ahora, consideremos una ligera variación, definamos a las siguientes matrices

$$A = \begin{pmatrix} L_1 & L_1 \\ L_1 & L_1 \end{pmatrix}, B = \begin{pmatrix} L_2 & L_2 \\ L_2 & L_2 \end{pmatrix}, C = \begin{pmatrix} 1 & 2 & 3 & 4 & 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 & 4 & 3 & 2 & 1 \\ 4 & 3 & 2 & 1 & 3 & 4 & 1 & 2 \\ 2 & 1 & 4 & 3 & 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 & 4 & 3 & 2 & 1 \\ 1 & 2 & 3 & 4 & 2 & 1 & 4 & 3 \\ 2 & 1 & 4 & 3 & 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 & 3 & 4 & 1 & 2 \end{pmatrix}$$

Las matrices A, B, C son 3-ortogonales, es decir, cualesquiera de las 64 posibles tercias (i,j,k) con $1 \leq i,j,k \leq 4$ aparece en exactamente una posición. Por ejemplo, la terna $(1,4,3)$ aparece únicamente en la posición $(2,6)$. En una analogía en la manera en como Alice y Bob pueden comunicarse usando estas matrices. Podemos enviar el mensaje $(2,6)$, Alice podría cifrar como $(1,4,3)$ y enviar esto a Bob. Bob puede descifrar mediante la exploración de las matrices hasta que el encuentre la única posición $(2,6)$ que contiene la terna $(1,4,3)$.

2.6.1. Esquema de Secreto Compartido

La integridad de un sistema de información puede consistir en exigir que determinadas operaciones solo pueden ser llevadas acabo por una o mas personas que tienen derechos de acceso. El acceso a este sistema es a menudo adquirida a través de una clave, cuyo uso se rige por un sistema de gestión de claves.

En particular si el esquema tiene k participantes, un (t,k)**-esquema de secreto compartido** es un sistema donde k piezas de información llamadas **acciones** de una llave secreta K son distribuidas de modo que cada participante tiene una acción, tal que

1. La llave K puede ser reconstruida a partir del conocimiento de cualesquiera t o mas acciones.
2. La llave K no puede reconstruirse a partir del conocimiento de menos de t acciones.

Ahora, presentamos un esquema de secreto compartido que utiliza cuadrados latinos. Para esto definimos un nuevo tipo de cuadrado latino.

Un **cuadrado latino parcial** de orden n es una matriz de tamaño $n \times n$ con las entradas elegidas del conjunto $\{1,2,\ldots,n\}$, tal que ningún elemento aparece dos veces en cualquier fila o columna.

La diferencia entre un cuadrado latino y un cuadrado latino parcial, es que este último puede tener posiciones vacías. Smetaniuk mostró que cualquier cuadrado latino parcial de orden n con a lo más $n-1$ posiciones llenas puede ser completado a un cuadrado latino de orden n. De otra manera, si colocamos $n-1$ unos en las primeras $n-1$ posiciones de la diagonal principal del cuadrado y un 2 en la última posición de la diagonal obtenemos un cuadrado latino parcial de orden n con n posiciones llenas que no puede ser completado a un cuadrado latino de orden n.

Ejemplo 2.6.2. *Por ejemplo , el siguiente cuadrado latino parcial de orden 3 con 3 posiciones llenas como se describió antes*

$$\begin{pmatrix} 1 & * & * \\ * & 1 & * \\ * & * & 2 \end{pmatrix}$$

al tratar de completarlo obtendríamos

$$\begin{pmatrix} 1 & 2 & 3 \\ * & 1 & * \\ * & 3 & 2 \end{pmatrix}$$

lo siguiente sería poner un 1 en la posición $(2,3)$ *y en la posición* $(3,1)$ *pero este ya no seria un cuadrado latino de orden 3. Por lo que el cuadrado latino parcial no lo podemos completar a un cuadrado latino.*

Un cuadrado latino de orden n es por supuesto un cuadrado latino parcial de orden n sin posiciones vacías.

Un **conjunto crítico** C en un cuadrado latino L de orden n es el conjunto

$$C = \{(i,j,k) | i,j,k \in \{1,2,\ldots,n\}\}$$

que cumple las siguientes dos propiedades

1. L es el único cuadrado latino de orden n que tiene el símbolo k en la posición (i,j), esto se cumple para todo elemento de C.
2. Ningún subconjunto propio de C tiene la propiedad 1.

Un conjunto crítico es llamado **mínimo** si es un conjunto crítico de cardinalidad mínima posible para L.

Ejemplo 2.6.3. *Un conjunto crítico mínimo C para el cuadrado latino*

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & * & * \\ * & * & * & 3 \\ * & 4 & * & * \\ * & * & 2 & * \end{pmatrix}$$

es

$$C = \{(1,1;1),(1,2;2),(2,4;3),(3,2;4),(4,3;2)\}$$

Teniendo estas herramientas ya podemos describir el esquema de secreto compartido. La llave secreta K se toma como un cuadrado latino L cuyo orden n se le permite ser público, aunque L se mantiene como privado, S es la unión de conjuntos críticos de L. A cada participante se le da una acción que es un elemento $(i, j; k)$ de C distribuidos de forma segura. Cuando un grupo de participantes cuyas acciones forman un conjunto crítico C de L se reúnen pueden reconstruir el cuadrado latino L abriendo la llave secreta $K = L$.

Ejemplo 2.6.4. *Con*

$$L = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix}$$

y $S = \{(2, 1; 2), (3, 2; 1), (1, 3; 3)\}$ *tenemos un* $(2, 3)$*-esquema de secreto compartido, ya que dos participantes combinando sus acciones* $\in S$ *pueden reconstruir de forma única el cuadrado latino* L*.*

Regresando al ejemplo 2.6.3 y con

$$S = \{(1, 1; 1), (1, 2; 2), (2, 4; 3), (3, 2; 4), (4, 3; 2), (1, 3; 3), (1, 4; 4), (2, 2; 1), (3, 4; 2), (4, 1, 4)\}$$

se da a cada participante una acción $(i, j; k) \in S$. Dado que cualquier conjunto crítico permite la reconstrucción del cuadrado latino completo, los participantes se reunirán de tal modo que sus acciones formen un conjunto crítico.

Ahora, lo que se quiere es un sistema donde las acciones de algunos participantes tengan mas peso que otros. En este caso se requiere que una acción para el participante i pueda ser reemplazada por una colección de acciones de participantes de menor peso. Este sistema es llamado a menudo **Esquema Multinivel**.

Ejemplo 2.6.5. *Supongamos que en un banco, se quiere tener una firma válida para la transferencia de* $1,000,000,000$ *solo si la acción de dos cajeros y un vicepresidente o dos vicepresidentes son enterados.*

Usando el cuadrado latino

$$L = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix}$$

y considerando los siguientes conjuntos críticos de L

$$A_1 = \{(1, 1; 1), (1, 2; 2), (2, 1; 2)\}, A_2 = \{(1, 1; 1), (1, 2; 2), (3, 2; 1)\}, A_3 = \{(3, 2; 1), (2, 1; 2)\}$$

tenemos que

1. *L puede reconstruirse con* $(2, 1; 2)$ *y* $(3, 2; 1)$

2. *Cualesquiera de estas dos acciones puede ser reemplazada por las dos acciones* $(1,1;1)$ *y* $(1,2;2)$

El sistema puedes ser construido por dar a los cajeros $(1,1;1)$ *y* $(1,2;2)$ *y asignando las acciones* $(2,1;2)$ *y* $(3,2;1)$ *a los vicepresidentes.*

Ahora, consideremos la siguiente situación.

Supongamos que el administrador de un hospital requiere acceso a varios archivos restringidos de departamentos diferentes, por ejemplo, archivos de datos de pacientes, recursos hospitalarios y datos del banco de trasplante de órganos.

Si tres esquemas de secreto compartido fueran usados, el administrador tendría que recordar y usar 3 acciones diferentes, una para cada esquema. Una forma de construir varios esquemas que tengan una llave común que sirva para desbloquearlos es

Sea L un cuadrado latino de orden 5

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \\ 3 & 5 & 1 & 2 & 4 \\ 4 & 3 & 5 & 1 & 2 \\ 5 & 4 & 2 & 3 & 1 \end{pmatrix}$$

. Este cuadrado tiene 41 conjuntos críticos mínimos, tres de ellos son:

$$A_1 = \{(1,1;1),(2,5;3),(3,5;4),(4,2;3),(4,3;5),(5,1;5),(5,3;2)\}$$
$$A_2 = \{(1,1;1),(1,5;5),(3,2;5),(3,5;4),(4,2;3),(5,3;2),(5,4;3)\}$$
$$A_3 = \{(1,1;1),(1,5;5),(3,4;2),(4,2;3),(4,5;2),(5,2;4),(5,4;3)\}$$

Consideremos el cuadrado latino parcial de orden 5

$$\begin{pmatrix} * & * & * & * & 5 \\ * & * & * & * & 3 \\ * & 5 & * & 2 & 4 \\ * & 3 & 5 & * & 2 \\ 5 & 4 & 2 & 3 & * \end{pmatrix}$$

Notemos que cada uno de los elementos de cada uno de los conjuntos críticos A_1, A_2, A_3 de L es un elemento del cuadrado latino parcial dado. Los elementos de este cuadrado latino parcial no forman un conjunto crítico de L, dado que este cuadrado parcial tiene cinco completaciones distintas. Sin embargo cada departamento reconstruirá la misma clave secreta L y cada departamento tiene un conjunto distinto de claves para esta llave secreta.

2.6.2. Cuadrados Latinos y Cuasigrupos

En esta sección presentamos el uso de los cuasigrupos en la codificación de datos y por tanto, aplicaciones potenciales en la criptografía simétrica (se usa la misma clave para cifrar y descifrar mensajes) basándonos en [5].

el propósito del scrambler (Codificación pseudoaleatoria) es maximizar la entropía en la salida, incluso cuando la entrada sea constante.

La salida del encriptador propuesto depende del número de índices y de los ordenes de las matrices (r, s) que son enviados por una autoridad de confianza. La encriptación también depende de elementos multiplicadores que son generados por un algoritmo secreto basado en el número de índices, el orden de las matrices que se estén considerando y del *nonce* (número aleatorio generado por la autoridad de confianza). Esta clave se actualiza por la red de forma regular.

Recordemos que un cuasigrupo es un sistema binario $(Q, *)$ que satisface las condiciones

- Para cualquier $a, b \in Q$ existe un único $x \in Q$ tal que $a * x = b$.

- Para cualquier $a, b \in Q$ existe un único $y \in Q$ tal que $y * a = b$.

Escribimos a los elementos x y y como $a \setminus b$ y b/a, a estas nuevas operaciones las llamaremos **división izquierda** y **división derecha** de b sobre a. Estas operaciones binarias dan nuevos cuasigrupos sobre el conjunto Q.

El dual de un sistema binario $(Q, *)$ es un sistema binario $(Q, \circ)$ cuya operación se define como $a \circ b = b * a$. Este será un cuasigrupo si $(Q, *)$ lo es.

Un elemento a de un cuasigrupo $(Q, *)$ es **idempotente** si $a * a$. a será llamada **identidad izquierda** si $a * x = x$ para todo $x \in Q$, **identidad derecha** si $x * a = x$ para todo $x \in Q$ e **identidad** si es derecha e izquierda.

Un **lazo** (loop) es un cuasigrupo que tiene un elemento identidad. Este elemento es necesariamente único. Si a es identidad izquierda y b identidad derecha, entonces
$a = a * b = b$. Mas aún, un cuasigrupo no puede tener dos diferentes identidades izquierdas ya que si $a * x = x = b * x$ entonces $a = b$ por cancelación.

Si escribimos la tabla de Cayley de un lazo de tal manera que el primer elemento sea la identidad, entonces los elementos en el primer renglón son los mismos que las etiquetas del renglón y de manera similar para la primer columna. En particular si usamos la etiquetas $1, 2, \ldots, n$ el cuadrado latino resultante es reducido. De tal manera que un lazo es un cuasigrupo cuya tabla de Cayley es un cuadrado latino reducido.

Codificación

Sea Q un cuasigrupo tal que $a_1, a_2, \ldots, a_n \in Q$, entonces la operación de codificación QE definida sobre $(a_1, a_2, \ldots, a_n)$ asignandolo a otro vector $(b_1, b_2, \ldots, b_n)$ tal que los elementos del vector resultante también pertenezcan al mismo cuasigrupo.

La ecuación matemática usada para la codificación es

$$E_a(a_1, a_2, a_3, \ldots, a_n) = (b_1, b_2, b_3, \ldots, b_n)$$

donde la secuencia de salida esta definida por
$b_1 = a * a_1$
$b_i = b_{i-1} * a_i$
donde $2 \leq i \leq n$ y a es la **clave oculta**.

Ejemplo 2.6.6. *Sea* $a = 2$ *y* $(a_1, a_2, a_3, \ldots, a_n) = (2, 4, 1, 2, 3, 3)$ *con tabla de Cayley*

$$\begin{pmatrix} * & 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 1 & 5 \\ 2 & 2 & 1 & 5 & 4 & 3 \\ 3 & 5 & 4 & 3 & 2 & 1 \\ 4 & 1 & 5 & 4 & 3 & 2 \\ 5 & 3 & 2 & 1 & 5 & 5 \end{pmatrix}$$

entonces
$b_1 = a * a_1 = 2 * 2 = 1$
$b_2 = b_1 * a_2 = 1 * 4 = 1$
$b_3 = b_2 * a_3 = 1 * 1 = 4$
$b_4 = b_3 * a_4 = 4 * 2 = 5$
$b_5 = b_4 * a_5 = 5 * 3 = 1$
$b_6 = b_5 * a_6 = 1 * 3 = 2$
de tal manera que $(b_1, b_2, b_3, \ldots, b_n) = (1, 1, 4, 5, 1, 2)$ *es el vector codificado.*

otra implementación es

$$E_{h_1, h_2, \ldots, h_n}(a_1, a_2, a_3, \ldots, a_n) = (e_1, e_2, \ldots, e_n)$$

donde
$b_1 = h_1 * a_1$ $b_2 = b_1 * a_2$ $\ldots b_n = b_{n-1} * a_n$
$c_1 = h_2 * b_1$ $c_2 = c_1 * b_2$ $\ldots c_n = c_{n-1} * b_n$
$\vdots$
$e_1 = h_n * s_1$ $e_2 = e_1 * s_2$ $\ldots e_n = e_{n-1} * s_n$

con $h_1, h_2, h_3, \ldots, h_n$ elementos multiplicadores.

El encriptador $MLI(Multi\ Level\ Indexed)$ es

$$QE^{I_r,I_s}_{h_1,h_2,\ldots,h_n}(a_1,a_2,a_3,\ldots,a_n)=(e_1,e_2,e_3,\ldots,e_n)$$

donde $(a_1,a_2,a_3,\ldots,a_n)$ es el vector de entrada , $(e_1,e_2,\ldots,e_n)$ el vector de salida y I_r y I_s son llamados **índices**

Ejemplo 2.6.7. *Sea* $a=2$ *y* $(a_1,a_2,a_3,a_4,a_5,a_6,a_7,a_8,a_9,a_{10})=(1,1,1,1,1,1,1,1,1,1)$ *Primero se cifra el vector con el siguiente cuasigrupo de orden 7*

$$\begin{pmatrix} * & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 6 & 5 & 2 & 3 & 4 & 1 & 7 \\ 2 & 4 & 3 & 7 & 1 & 2 & 6 & 5 \\ 3 & 7 & 6 & 3 & 4 & 5 & 2 & 1 \\ 4 & 1 & 7 & 4 & 5 & 6 & 3 & 2 \\ 5 & 2 & 1 & 5 & 6 & 7 & 4 & 3 \\ 6 & 3 & 2 & 6 & 7 & 1 & 5 & 4 \\ 7 & 5 & 4 & 1 & 2 & 3 & 7 & 6 \end{pmatrix}$$

el vector resultante es $(b_1,b_2,b_3,b_4,b_5,b_6,b_7,b_8,b_9,b_{10})=(4,1,6,3,7,5,2,4,1,6)$.

Nuevamente ciframos este último vector, pero ahora con el siguiente cuasigrupo de orden 9

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

De tal manera que el vector de salida es $(e_1,e_2,e_3,e_4,e_5,e_6,e_7,e_8,e_9,e_{10})=(1,8,2,9,5,7,3,4,1,5)$.

Decodificación

Este proceso es similar al de cifrado. El principal punto a destacar es la generación de la matriz inversa. La inversa izquierda es usada para la decodificación. La ecuación fundamental para este proceso es

$$D(e_1,e_2,\ldots,e_n)=(a_1,a_2,\ldots,a_n)$$

donde
$a_1=a\backslash e_1$
$a_i=e_{i-1}\backslash e_i$

Para llevar acabo el proceso de descifrado es necesario primero generar la matriz inversa del cuasigrupo dado.

Ejemplo 2.6.8. *Mostramos a un cuasigrupo de orden 7 y a su matriz inversa*

$$\begin{pmatrix} * & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 5 & 6 & 2 & 3 & 4 & 1 & 7 \\ 2 & 3 & 4 & 7 & 1 & 2 & 6 & 5 \\ 3 & 6 & 7 & 3 & 4 & 5 & 2 & 1 \\ 4 & 7 & 1 & 4 & 5 & 6 & 3 & 2 \\ 5 & 1 & 2 & 5 & 6 & 7 & 4 & 3 \\ 6 & 2 & 3 & 6 & 7 & 1 & 5 & 4 \\ 7 & 4 & 5 & 1 & 2 & 3 & 7 & 6 \end{pmatrix} \begin{pmatrix} \backslash & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 6 & 3 & 4 & 5 & 1 & 2 & 7 \\ 2 & 4 & 5 & 1 & 2 & 7 & 6 & 3 \\ 3 & 7 & 6 & 3 & 4 & 5 & 1 & 2 \\ 4 & 2 & 7 & 6 & 3 & 4 & 5 & 1 \\ 5 & 1 & 2 & 7 & 6 & 3 & 4 & 5 \\ 6 & 5 & 1 & 2 & 7 & 6 & 3 & 4 \\ 7 & 3 & 4 & 5 & 1 & 2 & 7 & 6 \end{pmatrix}$$

con estas tablas de Cayley y con $a = 6$ *codificaremos al vector* $(a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9) = (2, 3, 4, 4, 5, 5, 5, 5, 5)$ *es vector codificado es* $(2, 3, 4, 4, 5, 5, 5, 5, 5)$ *. Ahora mediante la matriz inversa dada, el mensaje original es recuperado* $(2, 3, 4, 4, 5, 5, 5, 5, 5)$

2.6.3. Isotopía de Cuadrados Latinos

Los cuadrados latinos tienen un gran potencial dentro de la Criptografía, sobre todo por la propiedad de Isotopía que existe entre ellos. Pero, ¿cómo saber cuando dos cuadrados latinos son isotópicos?. En esta sección mostramos dos teoremas importantes que responden a esa pregunta, basándonos en [19].

Dos cuadrados latinos $L = (l_{ij})$ y $M = (m_{ij})$ de orden n son llamados **isotópicos** si existe una tercia ordenada (θ, φ, ψ) de biyecciones tales que

$$\psi(l_{\theta(i)\varphi(j)}) = m_{ij} \text{ para } i, j = 1, 2, \ldots, n$$

es decir, si uno puede ser transformado en el otro por reordenamiento de renglones, reordenamiento de columnas y renombramientos de elementos.

El **Isotopismo** es una importante relación en un conjunto de cuadrados latinos de orden n al cual denotaremos como $\mathfrak{L}_n$. Mas aún, es una relación de equivalencia que da una partición de $\mathfrak{L}_n$ de **clases isotópicas** de cuadrados latinos.

Dados dos cuadrados latinos L y M de orden n ¿cómo poder decir que son isotópicos sin tener que dar las permutaciones de renglones, columnas y el renombramiento de elementos?.

El Teorema de Cayley dice que cualquier grupo $(G, *)$ es isomorfo a un subgrupo $\overline{G}$ de un grupo $Sym(G)$ (grupo simétrico de elementos en el conjunto X). Los elementos de $\overline{G}$ pueden representarse por traslaciones izquierdas de G. Una **Traslación izquierda** asociada a $a \in G$ se denota como L_a donde $L_a : G \to G$ definida como $L_a(x) = a * x$. Entonces un grupo G esta representado por el conjunto de sus traslaciones izquierdas $L_G \subseteq Sym(G)$.

Para un cuasigrupo Q se puede considerar de manera similar al conjunto de traslaciones izquierdas. Además el cuasigrupo es definido únicamente por L_Q. El siguiente teorema relaciona estas traslaciones con la isotopía de dos cuasigrupos.

Teorema 2.6.1. *Sea (θ, φ, ψ) un isotopismo de dos cuasigrupos $Q_1 = (Q, *_1), Q_2 = (Q, *_2)$ entonces para el conjunto de traslaciones L_{Q_1} y L_{Q_2} se cumple*

$$L_{Q_2} = \psi L_{Q_1} \varphi^{-1} \dots (1)$$

Con este teorema tenemos un método sencillo de como encontrar un isotopismo para dos cuasigrupos Q_1,Q_2.Sin embargo, es demasiado complejo, ya que se debe verificar (1) para todo $\varphi, \psi \in Sym(Q)$. El siguiente teorema es más práctico.

Teorema 2.6.2. *Sean $Q_1 = (Q, *_1)$ y $Q_2 = (Q, *_2)$ dos cuasigrupos y $p_2 \in L_{Q_2}$. Entonces Q_1 y Q_2 son isotópicos si y sólo si existen $p_1 \in L_{Q_1}$ y $p \in Sym(Q)$ tal que*

$$L_{Q_2} p_2^{-1} = p L_{Q_1} p_1^{-1} p^{-1}$$

Del teorema anterior los conjuntos de permutaciones $L_{Q_2} p_2^{-1}$ y $L_{Q_1} p_1^{-1}$ son conjugados por p. De tal manera que poseen la misma estructura cíclica.

2.7. Diseño de Experimentos

En esta sección mostramos el usó de los cuadrados latinos ortogonales en la construcción de diseños experimentales basándonos en [20, 21].

Un **experimento** se refiere a la creación y preparación de lotes de prueba que verifiquen la validez de las hipótesis establecidas sobre las causas de un determinado problema o defecto del objeto de estudio.

El **diseño de experimentos** es la metodología estadística destinada a la planificación y análisis de un experimento.

Un **diseño de cuadrado latino** es un diseño de bloque con un factor experimental y dos variables de bloqueo. En este tipo de diseño, la muestra de sujeto se estratifica un función de dos variables de clasificación y, posteriormente, se aplican los distintos tratamientos dentro de cada bloque. Este diseño es restrictivo porque requiere que el número de tratamientos, de renglones y de columnas sea igual.

El diseño de cuadrado latino tuvo sus orígenes en experimentos agrícolas, el uso de este diseño no se limita a esta situación, se ha utilizado en otras áreas diferentes a la agricultura, tales como la biología, estudio de mercados, procesos industriales, entre otros.

Los **Tratamientos** son el conjunto de circunstancias creados para el experimento, en respuesta a la hipótesis de investigación y son el centro de la misma.

Ejemplo 2.7.1. *Cuadrado latino reducido de orden 4*

$$\begin{pmatrix} A & B & C & D \\ B & C & D & A \\ C & D & A & B \\ D & A & B & C \end{pmatrix}.$$

El cuadrado latino reducido de orden 4 lo podemos aplicar al siguiente experimento.

Ejemplo 2.7.2. *Supongamos que cuatro automóviles y cuatro conductores se emplean en un estudio sobre las posibles diferencias entre cuatro aditivos de gasolina. Aunque los coches son modelos idénticos, es muy probable que ocurran ligeras diferencias sistemáticas en su comportamiento y aunque cada conductor intente llevar el automóvil como exige la prueba, pueden ocurrir ligeras diferencias sistemáticas de conductor a conductor. Será deseable eliminar tanto las diferencias de los automóviles como los de los conductores.*

El siguiente cuadrado latino de orden 4 permite analizar este problema bajo la hipótesis de que no existe interacción apreciable entre tratamientos, automóviles y conductores.

	Automóvil			
Conductor	*I*	*II*	*III*	*IV*
1	*A*	*B*	*C*	*D*
2	*B*	*C*	*D*	*A*
3	*C*	*D*	*A*	*B*
4	*D*	*A*	*B*	*C*

donde A, B, C y D son los aditivos.

Para tener mayor eficiencia en el diseño se requiere asignar de manera aleatoria a los tratamientos, por lo cual se require aleatorizar el cuadrado latino. Para aleatorizar un cuadrado latino de orden t se debe hacer lo siguiente

1. Partir de un cuadrado latino reducido del orden requerido por el experimento.
2. Aleatorizar todas las columnas del cuadrado elegido. Para este efecto existen tablas de permutaciones o simplemente se elige un orden aleatorio de las t columnas.
3. Aleatorizar las t filas del cuadrado obtenido en el paso 2.
4. Asignar aleatoriamente los tratamientos a las letras.

Aleatoricemos el cuadrado latino de orden 4 del experimento anterior.

Ejemplo 2.7.3. *1. Tenemos el cuadrado latino estándar de orden 4, que necesitamos para el experimento.*

$$\begin{pmatrix} A & B & C & D \\ B & C & D & A \\ C & D & A & B \\ D & A & B & C \end{pmatrix}$$

2. Ahora tenemos la siguiente permutación de columnas 1342, es decir, la primera columna permanece fija, la tercera columna ahora será la segunda, la cuarta columna será la tercera y la que era la segunda será la cuarta, quedando

$$\begin{pmatrix} A & C & D & B \\ B & D & A & C \\ C & A & B & D \\ D & B & C & A \end{pmatrix}.$$

3. Ahora aleatorizamos las filas del cuadrado latino obtenido en (2). Sea 3412 la permutación que aplicaremos a las filas. La fila 3, ahora sera la primera, la cuarta la segunda , la primera la tercera y la segunda ahora será la cuarta. El cuadrado aleatorizado obtenido es

$$\begin{pmatrix} C & A & B & D \\ D & B & C & A \\ A & C & D & B \\ B & D & A & C \end{pmatrix}.$$

4. Aleatorizamos los tratamientos.

Si tenemos un cuadrado grecolatino de orden k y permutamos ya sea filas o columnas, se sigue cumpliendo que el cuadrado es grecolatino.

Un cuadrado grecolatino de orden k, permite estudiar k tratamientos simultáneamente con tres variables diferentes de bloques.

Ejemplo 2.7.4. *El siguiente cuadrado grecolatino de orden 4 es una extensión del diseño de cuadrado latino del ejemplo anterior, en el que existe una variable de bloque adicional, los días α, β, γ y δ.*

	Automóvil			
Conductor	*I*	*II*	*III*	*IV*
1	$A\alpha$	$B\beta$	$C\gamma$	$D\delta$
2	$B\delta$	$A\gamma$	$D\beta$	$C\alpha$
3	$C\beta$	$D\alpha$	$A\delta$	$B\gamma$
4	$D\gamma$	$C\delta$	$B\alpha$	$A\beta$

donde A, B, C y D son los aditivos.

Notemos que la tercera variable de bloqueo que esta representada con las letras griegas α, β, γ y δ aparece una sola vez con cada tratamiento.

Si se tiene un conjunto de $A_1, A_2, \ldots, A_r$ $MOLS$ de orden n, con $r \leq n$, entonces si a cada A_i los representamos con alfabetos distintos para $i = 1, \ldots, r$. Al superponer al menos a tres $MOLS$ obtenemos un cuadrado **hipergrecolatino.**

Un cuadrado hipergrecolatino de orden k permite el estudio de k tratamientos con más de tres variables de bloques. Vamos a ilustrarlo con el siguiente ejemplo.

Ejemplo 2.7.5 (PROBADOR DE DESGASTE DE MATERIALES)**.** *Se utiliza esta máquina para ensayar la resistencia al desgaste de distintos tipos de tela u otros materiales parecidos y tiene la característica de poder analizar cuatro piezas a la vez en cada ensayo.*

La variable respuesta es la pérdida de peso, medida en décimas de miligramos, sufrida por la pieza sometida a ensayo, cuando roza contra una lija determinada durante 1000 revoluciones de la máquina. Se montan en cuatro soportes 1,2,3 y 4, las muestras de cuatro tipos de diferentes tejidos (tratamientos) A, B, C y D, cuya resistencia al desgaste queremos comparar.

Cada soporte puede estar en cualquiera de las posiciones P_1, P_2, P_3 y P_4 en la máquina. Cada hoja de papel de lija α, β, γ y δ se cortó en cuatro trozos, cada uno de los cuales se usó para hacer una observación. El cuadrado hipergrecolatino de orden 4 es

	Posiciones			
Ensayo	P_1	P_2	P_3	P_4
R_1	$\alpha A1$	$\beta B2$	$\gamma C3$	$\delta D4$
R_2	$\beta C4$	$\alpha D3$	$\delta A2$	$\gamma B1$
R_3	$\gamma D2$	$\delta C1$	$\alpha B4$	$\beta A3$
R_4	$\delta B3$	$\gamma A4$	$\beta D1$	$\alpha C2$

con Tratamientos: A, B, C, D; Soportes:1,2,3,4; Hojas de papel de lija:$\alpha, \beta, \gamma, \delta$.

CAPÍTULO 3

Conclusiones

En este trabajo se estudiaron con cierta profundidad algunas de las relaciones existentes entre los cuadrados latinos y distintas áreas de las matemáticas como son: teoría de diseños combinatorios, teoría de gráficas, álgebra, estadística y criptología. Incluso dedicamos un espacio para tratar la presencia de los cuadrados latinos en las Matemáticas Recreativas, concretamente los cuadrados mágicos y el juego Sudoku.

Se pretende que este trabajo sea una referencia introductoria para el estudio de los cuadrados latinos y que constituya una alternativa interesante a los textos que ya existen sobre el tema. Conviene destacar que el desarrollo de las secciones 1.1, 2.2 y 2.3.3 no los encontrará en ningún otro libro, solamente en artículos especializados.

Es importante mencionar uno de los resultados originales de la tesis. En la sección 2.3.3 desarrollamos la demostración dada por Jörgen Bierbrauer y Albrecht Brandis en 1985 sobre la mejor cota inferior que existe hasta el momento para el número de Ramsey de un árbol, cabe mencionar que lo que hace extensa esta prueba es la demostración de la existencia de cierto tipo de cuadrados latinos. Nosotros damos una prueba alternativa en donde hacemos uso de la equivalencia de los cuadrados latinos simétricos y unipotentes de orden n con las 1-factorizaciones de $\mathbb{K}_n$.

Bibliografía

[1] Laywine. Charles F., *Discrete Mathematics Using Latin Squares*, Wiley-Interscience Series in Discrete Mathematics and Optimization, 1998.

[2] Anderson. Ian., *Combinatorial Designs: Construction Methods*, Ellis Horwood Limited, 1990.

[3] Bierbrauer. Jörgen and Brandis. Albrecht., *On Generalized Ramsey Numbers For Trees*, Combinatorica 5 (2) (1985), pp. 95-107.

[4] Hill. Raymond., *A First Course in Coding Theory*, Oxford, 1994.

[5] Kartik Satti.Maturi Venkat., *A Quasigroup Based Cryptographic System.*

[6] Anges M. Herzberg and M. Ram Murty, *Sudoku Aquares and Chromatic Polynomials*, Notice of the AMS. Volume 54, Number 6, 2007.

[7] Richard M. Wilson, *Nonisomorphic Steiner Triple Systems*, Springer-Verlag, Volume 135, Number 4, pp. 303-313, 1974.

[8] Anderson. Ian. and Honkala Iiro., *A short course in combinatorial designs*, Spring, 1997.

[9] C.C. Lindner. and C. A. Rodger., *Design Theory*, Auburn University, CRC Press, 1997.

[10] Ryan M. Pedersen and Timothy L. Vis., *Sets of Mutually Orthogonal Sudoku Latin Squares*, College Mathematics Journal 40:3, pp. 174-180, 2009.

[11] Agnes M. Herzberg and M. Ram Murty., *Sudoku Squares and Chromatic Polynomials*,Notices of the AMS, Volume 54, Number 6, pp. 708-717, 2007.

[12] Czeslaw. Koscielny., *Generating Quasigroups for Cryptographic Applications*, Int. J. Appl. Math. Comput. Sci., Vol. 12, No.4, pp. 559-569, 2002.

[13] D. I. Falikman., *A proof of Van der Waerden"s conjecture on the permanent of a doubly stochastic matrix*, 1981.

[14] Alter. Ronald., *How many latin Square are there*, Computer Science Department, University of Kentucky, pp. 632-634, 1975.

[15] L. Brégman., *Some properties of nonnegative matrices and their permanents*, Soviet Math. Dokl. 14 (1973), pp. 945-949.

[16] Euler. Leonhard, *Recherches sur une nouvelle especе de quarres magiques*, Verh. Genootsch. der Wet. Vlissingen, 9, pp. 85-232, 1782.

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

[18] Tn. Skolem, *Some remarks on the triple systems of Steiner*, Math. Scand., 6 (1958), pp. 273-280.

[19] Grosek. Otokar. and Sýs. Marek., *Isotopy of latin squares in Cryptography*, Tatra Mt. Publi. 45, 2010, pp. 27-36.

[20] Robert O. Kuehl, *Diseño de Experimentos*, Segunda edición, Thomson , México, D.F., 2001.

[21] Douglas C. Montgomery, *Diseño y Análisis de Experimentos*, Segunda edición, Limusa wiley, México, 2008.