ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA INFORMÁTICA

Trabajo fin de Grado

Grado en I.I. - Tecnologías Informáticas

ESTUDIO DE CUADRADOS LATINOS PARA SU APLICACIÓN EN UN PROTOCOLO CRIPTOGRÁFICO DE COMPARTICIÓN DE SECRETOS

Realizado por
Manuel González Regadera

Dirigido por
María Dolores Frau García
Raúl Manuel Falcón Ganfornina

Departamento
Matemática Aplicada I

Sevilla, junio de 2022

Resumen

Por norma general, el acceso a un sistema de información está garantizado mediante el uso de una clave, una contraseña, etc. Si esta clave se divide y comparte con varios participantes con el objetivo de que sólo ciertos grupos autorizados puedan acceder al sistema, podemos afirmar que nos encontramos ante un sistema de seguridad compartida.

El presente estudio busca desarrollar una nueva versión para el esquema de compartición de secretos propuesto en (Cooper, Donovan, y Seberry, 1994) mediante la aplicación de propiedades relativas a cuadrados latinos y autotopismos asociados a estos, incluyendo, además, un estudio estadístico sobre el tamaño de los conjuntos críticos basados en autotopismos no triviales relativos a cuadrados latinos de orden seis.

Abstract

As a general rule, access to an information system is guaranteed through the use of a key, a password, etc. If this key is divided and shared with several participants so that only certain authorized groups can access the system, we can say that we are dealing with a shared security system.

The present study seeks to develop a new version for the secret sharing scheme proposed in (Cooper y cols., 1994) by applying properties related to Latin squares and autotopisms associated with them, including, in addition, a statistical study on the size of the critical sets based on non-trivial autotopisms relative to Latin squares of order six.

Agradecimientos

Me gustaría dedicar, en este pequeño espacio, unas palabras para todos aquellos que, de alguna manera, me han acompañado durante esta gran y maravillosa aventura que es la vida. Gracias a todos aquellos que me apoyaron y que confiaron en mí desde el primer momento.

Quisiera hacer una mención especial a mis padres: Eva y Manuel, por ser los pilares fundamentales de mi vida, por impulsarme siempre a perseguir y conseguir todos y cada uno de mis sueños, por mostrarme el significado del amor incondicional. A mis hermanos: Darío y Lucas, por enseñarme cada día a disfrutar de los pequeños detalles que nos regala la vida, por obligarme a ser un niño otra vez, por ser mi principal motivación para que, algún día, puedan estar tan orgullosos de mí como yo lo estoy de ellos. A mis abuelos y al resto de mi familia, porque el amor que siento por ellos es tal, que si lo defino, lo limito.

También quisiera dar las gracias a mis *Tóxicos*: María, Manuel y Jesús, por enseñarme a confiar de nuevo en la gente, por aportar esa pizca de locura que tanto necesitaba en mi vida, por cada aventura que hemos vivido y por todas las que nos quedan por vivir, porque más que amigos, os considero hermanos. A mi grupo *Intoxicación Koreana*: Alicia, Santiago, Almudena, Paula, Juan, Raúl y Rubén, por acogerme como a uno más desde el momento en que les conocí, por todas las charlas que terminaban de madrugada, por enseñarme el significado de la vida universitaria. A mi grupo *El Garito*: Fran, Cris, Rocío J., Rocío C., Alex, Cristina, porque, a pesar de la distancia, cada vez que quedamos parece que no hubiera pasado el tiempo.

Sin duda, y aunque los haya dejado para el final, a dos de las personas que más debo agradecer su apoyo incondicional, su ayuda y su paciencia a lo largo de todo este tiempo es a mis profesores y tutores de este trabajo: Loli y Raúl, porque no sólo me han introducido en el maravilloso mundo de las matemáticas sino que, al igual que la familia, han sabido guiarme por el camino correcto, velando por mí en cada momento. Espero que este proyecto sea sólo el principio de una vida dedicada a la investigación.

En definitiva, a todos aquellos que me enseñaron, a los que me dieron ánimos, a los que ya no están.

A todos ellos, gracias.

Índice general

Índice general **IV**

Índice de cuadros **VI**

Índice de figuras **VII**

1 Definición de objetivos **1**

2 Estudio de viabilidad **3**

3 Estado del arte **4**
3.1 Contexto 4
3.2 Preliminares 6
3.2.1 Cuadrados latinos 6
3.2.2 Cuadrados latinos parciales 6
3.2.3 Conjunto crítico de un cuadrado latino 7
3.2.4 Isotopismos 8
3.2.5 Conjuntos críticos basados en autotopismos de cuadrados latinos 9
3.2.6 Orbitas basadas en autotopismos de cuadrados latinos 9
3.2.7 Aplicación de cuadrados latinos al proceso de compartición de secretos 11
3.3 Resultados previos 12

4 Análisis de antecedentes y aportación realizada **16**
4.1 Análisis de antecedentes 16
4.1.1 Protocolo para la compartición de secretos basado en cuadrados latinos 16
4.1.2 Análisis de los conjuntos críticos basados en autotopismos no triviales de cuadrados latinos de hasta orden 5 17
4.2 Aportación realizada 19
4.2.1 Aportación al protocolo de compartición de secretos mediante cuadrados latinos 19
4.2.2 Aportación al estudio del tamaño de los conjuntos críticos basados en autotopismos no triviales de cuadrados latinos 23

5 Análisis temporal y costes de desarrollo **71**
5.1 Actividades, tareas e hitos 71
5.1.1 Distribución de roles y responsabilidades 72
5.1.2 Cronograma 73
5.2 Costes de desarrollo 74
5.2.1 Coste relativo al salario 74
5.3 Desarrollo real del proyecto 74

6 Análisis de requisitos **75**
6.1 Requisitos sobre el algoritmo 75
6.2 Requisitos temporales 75

7 Manual **76**

8 Comparación con otras alternativas **78**
8.1 Comparación con el esquema de compartición de secretos desearrollado por Cooper, Donovan y Seberry. 78
8.2 Comparación con estudios de conjuntos críticos basados en autotopismos no triviales de cuadrados latinos. 79

9 Plan de Riesgos **80**
9.1 Identificación de riesgos 80
9.2 Planes de contingencia 80

10 Plan de Calidad **81**
10.1 Indicadores 81
10.2 Plan de mejora 81

11 Plan de Comunicaciones **82**

12 Conclusiones y desarrollos futuros **83**

Referencias **85**

Índice de cuadros

3.1 Cantidad de cuadrados latinos en función de su tamaño n 6
3.2 Autotopismos relativos a cuadrados latinos L_2–$L_{5,2}$. 15

4.1 Autotopismos de $L_{6,1}$–$L_{6,12}$. 70

8.1 Comparativa entre protocolos de compartición de secretos 79

Índice de figuras

3.1 Cuadrado Latino desarrollado por Ahmad al-Buni (Fuente: (al Buni, 1980)) . . . 4
3.2 Cuadrado Latino desarrollado Ramón Llull (Fuente: Ars Demostrativa de la edición latina de Maguncia, 1722, vol.III) . . . 5
3.3 Cuadrado greco-latino (Fuente: Wikipedia) . . . 5
3.4 Cuadrado latino de orden 4 en forma estándar. . . . 6
3.5 Cuadrado latino parcial de orden 4 . . . 7
3.6 Conjunto crítico mínimo para un cuadrado latino de orden 4 . . . 7

4.1 Estudio estadístico Ejemplo 4.1 (Fuente: Elaboración propia) . . . 25
4.2 Estudio estadístico Ejemplo 4.2 (Fuente: Elaboración propia) . . . 26
4.3 Estudio estadístico Ejemplo 4.3 (Fuente: Elaboración propia) . . . 27
4.4 Estudio estadístico Ejemplo 4.4 (Fuente: Elaboración propia) . . . 28
4.5 Estudio estadístico Ejemplo 4.5 (Fuente: Elaboración propia) . . . 29
4.6 Estudio estadístico Ejemplo 4.6 (Fuente: Elaboración propia) . . . 30
4.7 Estudio estadístico de $L_{5,1}$ y Θ_1 (Fuente: Elaboración propia) . . . 31
4.8 Estudio estadístico $L_{5,1}$ y Θ_2 (Fuente: Elaboración propia) . . . 32
4.9 Estudio estadístico $L_{5,1}$ y Θ_3 (Fuente: Elaboración propia) . . . 32
4.10 Estudio estadístico $L_{5,2}$ y Θ_1 (Fuente: Elaboración propia) . . . 33
4.11 Estudio estadístico $L_{6,1}$ y Θ_1 (Fuente: Elaboración propia) . . . 34
4.12 Estudio estadistico $L_{6,1}$ y Θ_2 (Fuente: Elaboración propia) . . . 35
4.13 Estudio estadístico $L_{6,1}$ y Θ_3 (Fuente: Elaboración propia) . . . 35
4.14 Estudio estadístico $L_{6,2}$ y Θ_1 (Fuente: Elaboración propia) . . . 36
4.15 Estudio estadístico $L_{6,2}$ y Θ_2 (Fuente: Elaboración propia) . . . 37
4.16 Estudio estadístico $L_{6,2}$ y Θ_3 (Fuente: Elaboración propia) . . . 37
4.17 Estudio estadístico $L_{6,2}$ y Θ_4 (Fuente: Elaboración propia) . . . 38
4.18 Estudio estadístico $L_{6,2}$ y Θ_5 (Fuente: Elaboración propia) . . . 39
4.19 Estudio estadístico $L_{6,2}$ y Θ_6 (Fuente: Elaboración propia) . . . 39
4.20 Estudio estadístico $L_{6,2}$ y Θ_7 (Fuente: Elaboración propia) . . . 40
4.21 Estudio estadístico $L_{6,2}$ y Θ_8 (Fuente: Elaboración propia) . . . 40
4.22 Estudio estadístico $L_{6,2}$ y Θ_9 (Fuente: Elaboración propia) . . . 41
4.23 Estudio estadístico $L_{6,3}$ y Θ_1 (Fuente: Elaboración propia) . . . 42
4.24 Estudio estadístico $L_{6,3}$ y Θ_2 (Fuente: Elaboración propia) . . . 43
4.25 Estudio estadístico $L_{6,3}$ y Θ_3 (Fuente: Elaboración propia) . . . 43
4.26 Estudio estadístico $L_{6,3}$ y Θ_4 (Fuente: Elaboración propia) . . . 44
4.27 Estudio estadístico $L_{6,3}$ y Θ_5 (Fuente: Elaboración propia) . . . 44
4.28 Estudio estadístico $L_{6,4}$ y Θ_1 (Fuente: Elaboración propia) . . . 45
4.29 Estudio estadístico $L_{6,4}$ y Θ_2 (Fuente: Elaboración propia) . . . 46
4.30 Estudio estadístico $L_{6,4}$ y Θ_3 (Fuente: Elaboración propia) . . . 46
4.31 Estudio estadístico $L_{6,4}$ y Θ_4 (Fuente: Elaboración propia) . . . 47
4.32 Estudio estadístico $L_{6,4}$ y Θ_5 (Fuente: Elaboración propia) . . . 47

4.33 Estudio estadístico $L_{6,4}$ y Θ_6 (Fuente: Elaboración propia) 48
4.34 Estudio estadístico $L_{6,4}$ y Θ_7 (Fuente: Elaboración propia) 48
4.35 Estudio estadístico $L_{6,4}$ y Θ_8 (Fuente: Elaboración propia) 49
4.36 Estudio estadístico $L_{6,5}$ y Θ_1 (Fuente: Elaboración propia) 50
4.37 Estudio estadístico $L_{6,5}$ y Θ_2 (Fuente: Elaboración propia) 51
4.38 Estudio estadístico $L_{6,5}$ y Θ_3 (Fuente: Elaboración propia) 51
4.39 Estudio estadístico $L_{6,5}$ y Θ_4 (Fuente: Elaboración propia) 52
4.40 Estudio estadístico $L_{6,5}$ y Θ_5 (Fuente: Elaboración propia) 52
4.41 Estudio estadístico $L_{6,6}$ y Θ_1 (Fuente: Elaboración propia) 53
4.42 Estudio estadístico $L_{6,6}$ y Θ_2 (Fuente: Elaboración propia) 54
4.43 Estudio estadístico $L_{6,6}$ y Θ_3 (Fuente: Elaboración propia) 54
4.44 Estudio estadístico $L_{6,6}$ y Θ_4 (Fuente: Elaboración propia) 55
4.45 Estudio estadístico $L_{6,6}$ y Θ_5 (Fuente: Elaboración propia) 55
4.46 Estudio estadístico $L_{6,6}$ y Θ_6 (Fuente: Elaboración propia) 56
4.47 Estudio estadístico $L_{6,7}$ y Θ_1 (Fuente: Elaboración propia) 57
4.48 Estudio estadístico $L_{6,7}$ y Θ_2 (Fuente: Elaboración propia) 58
4.49 Estudio estadístico $L_{6,7}$ y Θ_3 (Fuente: Elaboración propia) 58
4.50 Estudio estadístico $L_{6,7}$ y Θ_4 (Fuente: Elaboración propia) 59
4.51 Estudio estadístico $L_{6,7}$ y Θ_5 (Fuente: Elaboración propia) 59
4.52 Estudio estadístico $L_{6,8}$ y Θ_1 (Fuente: Elaboración propia) 60
4.53 Estudio estadístico $L_{6,8}$ y Θ_2 (Fuente: Elaboración propia) 61
4.54 Estudio estadístico $L_{6,8}$ y Θ_3 (Fuente: Elaboración propia) 61
4.55 Estudio estadístico $L_{6,9}$ y Θ_1 (Fuente: Elaboración propia) 62
4.56 Estudio estadístico $L_{6,10}$ y Θ_1 (Fuente: Elaboración propia) 63
4.57 Estudio estadístico $L_{6,10}$ y Θ_2 (Fuente: Elaboración propia) 64
4.58 Estudio estadístico $L_{6,11}$ y Θ_1 (Fuente: Elaboración propia) 65
4.59 Estudio estadístico $L_{6,12}$ y Θ_1 (Fuente: Elaboración propia) 66
4.60 Estudio estadístico $L_{6,12}$ y Θ_2 (Fuente: Elaboración propia) 67
4.61 Estudio estadístico $L_{6,12}$ y Θ_3 (Fuente: Elaboración propia) 67
4.62 Estudio estadístico $L_{6,12}$ y Θ_4 (Fuente: Elaboración propia) 68
4.63 Estudio estadístico $L_{6,12}$ y Θ_5 (Fuente: Elaboración propia) 68
4.64 Estudio estadístico $L_{6,12}$ y Θ_6 (Fuente: Elaboración propia) 69
4.65 Estudio estadístico $L_{6,12}$ y Θ_7 (Fuente: Elaboración propia) 69

5.1 Tareas cronograma 73
5.2 Diagrama de Gantt 73
5.3 Tiempo dedicado a cada tarea (Fuente: Toggl Track) 74
5.4 Gráfico tiempo dedicado a cada tarea (Fuente: Toggl Track) 74

CAPÍTULO 1

Definición de objetivos

El objetivo principal de este trabajo consiste en implementar un algoritmo que permita obtener el secreto para un protocolo de compartición de secretos basado en cuadrados latinos y sus autotopismos, así como las posibles sombras a repartir entre los participantes. Dicho secreto será un cuadrado latino y las sombras se obtendrán a partir de sus Θ-conjuntos críticos, siendo Θ un autotopismo del mismo.

Como objetivo secundario se plantea realizar un estudio estadístico del tamaño de los Θ-conjuntos críticos de cuadrados latinos de orden seis con el fin de aplicarlos al sistema de compartición de secretos para mejorar su seguridad. Estos mínimos y máximos constituyen actualmente un problema abierto en la teoría de cuadrados latinos. En la literatura sólo se conocen dichos tamaños mínimos y máximos para cuadrados latinos de orden hasta cinco (Falcón, Johnson, y Perkins, 2020).

El algoritmo a desarrollar seguirá las siguientes etapas:

1. Debe elegir aleatoriamente:
   a) Un cuadrado latino L representante de una clase principal de tamaño n dado.
   b) Una simetría (autotopismo) Θ del cuadrado latino L.
2. Debe describir las órbitas en el conjunto de entradas del cuadrado latino L que son generadas por el autotopismo Θ.
3. Debe encontrar algún Θ-conjunto crítico. Su tamaño estará comprendido entre el mínimo $\mathrm{scs}(n)$ y el máximo $\mathrm{lcs}(n)$ posibles para cuadrados latinos de orden n. Para ello, debe tomar x entradas *aleatorias* del cuadrado latino L hasta dar con un Θ-conjunto crítico. Cada entrada puede elegirse como primer elemento de una órbita, por lo que realmente se eligen x órbitas aleatoriamente. Este procedimiento requiere estudiar si el conjunto elegido es Θ-conjunto crítico o no. Para ello, el algoritmo debe chequear que, para dicho conjunto, el cuadrado latino parcial vinculado se completa de forma única a L, y que ningún subconjunto del mismo cumple dicha propiedad.
4. Debe aplicar un isotopismo (aleatorio) Θ_1 al cuadrado latino L para obtener otro cuadrado latino L' de la misma clase de equivalencia.
5. Debe calcular el autotopismo Θ' de L' que es equivalente por conjugación del autotopismo Θ de L.
6. Debe obtener los Θ'-conjuntos críticos de L' a partir de los Θ-conjuntos críticos de L encontrados previamente.

El secreto para el protocolo de compartición de secretos será el cuadrado L', mientras que las sombras a repartir entre los participantes se obtendrán de entre los elementos de los Θ'- conjuntos críticos de L'. Serán públicos tanto el orden del cuadrado latino elegido, como secreto como el autotopismo Θ' que permitirá recuperar el secreto una vez que estén reunidos los participantes necesarios.

CAPÍTULO 2

Estudio de viabilidad

Desde el **punto de vista teórico**, se abordará el estudio pertinente sobre cuadrados latinos a través de dos artículos de investigación, principalmente.

- El primero de ellos (Cooper y cols., 1994) muestra por primera vez en la literatura cómo los conjuntos críticos de un cuadrado latino pueden ser usados en esquemas de compartición de secretos.
- El segundo artículo (Falcón y cols., 2020) profundiza en el estudio de conjuntos críticos basados en autotopismos de cuadrados latinos, con particular interés en aquellos de orden inferior a seis. Particularmente, se demuestra en dicho artículo que los tamaños de estos conjuntos críticos solo dependen tanto de la clase principal del cuadrado latino como de la estructura cíclica del autotopismo en consideración.

Desde el **punto de vista técnico**, se utilizará un software de código abierto, JUPYTER NOTEBOOKS, una aplicación web que permite desarrollar y compartir documentos con código que registran todo el proceso de desarrollo. La razón principal de usar JUPYTER NOTEBOOKS radica en que, además de soportar diversos lenguajes de programación, este software facilita la compartición y ejecución de los proyectos. Además, JUPYTER NOTEBOOKS suele ser muy usado en entornos académicos y de investigación. Al presentar una arquitectura basada en módulos abiertos, es ampliamente usado para desarrollar todo tipo de soluciones y servicios.

En cuanto al lenguaje empleado, se hará uso de PYTHON 3.0, no sólo por la comodidad que aporta a la hora de desarrollar código o la facilidad de lectura que presenta, sino por ser un lenguaje versátil y sencillo de aprender que, gracias a su popularidad, cuenta con una gran comunidad de usuarios para resolver dudas o problemas que puedan surgir.

Desde el **punto de vista económico**, al tratarse de un proyecto relativamente teórico, no se preveen gastos fuera de los supuestos salarios relativos a los distintos roles que participarían en este proyecto.

No se preveen riesgos noticiables, más allá de:

1. Los eventuales retrasos que puedan derivarse de compatibilizar el desarrollo del proyecto con el resto de los estudios.
2. Dificultades en la implementación puntual de alguna parte del código.
3. Circunstancialmente, la saturación de los recursos del dispositivo mientras se ejecuta la aplicación.

CAPÍTULO 3

Estado del arte

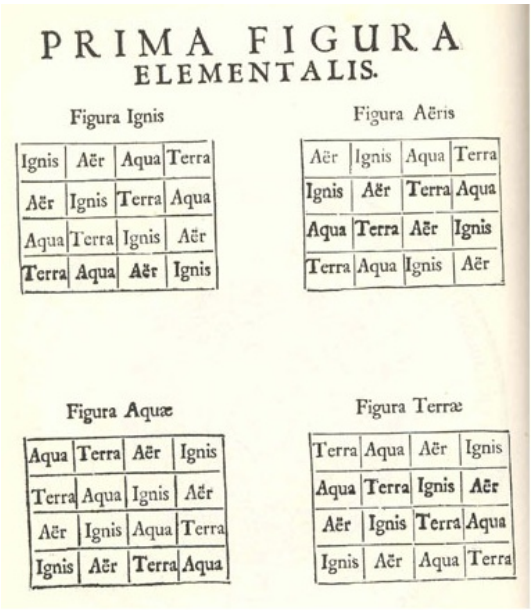
3.1– Contexto

El origen de los cuadrados latinos (Ibáñez, 2015) se remonta a los albores del segundo milenio, cuando las comunidades indias y árabes hacían uso de ellos, junto a los cuadrados mágicos[1], a modo de amuletos o talismanes. Hasta el momento, la primera publicación en la que aparecen cuadrados latinos atañe al libro *Shams al-Maárif al-Kubra*, del escritor y matemático árabe Ahmad al-Buni, quien construyó en el siglo XIII estas estructuras a partir de las letras de uno de los noventa y nueve nombres de Alá.

Figura 3.1: Cuadrado Latino desarrollado por Ahmad al-Buni (Fuente: (al Buni, 1980))

En el año 1232, en un intento de explicar el mundo a través de números combinatorios, se produce una aparición más moderna de los cuadrados latinos de la mano del filósofo castellano Ramón Llull, en su obra *Ars Demostrativa*, donde desarrolla cuadrados latinos de orden cuatro usando como símbolos Fuego, Aire, Agua y Tierra.

[1] Disposiciones numéricas en forma de matriz de *n x n* elementos conformadas por números naturales, de tal manera que con la suma de los elementos presentes en cada fila, columna o diagonal principal se obtiene el mismo resultado.



PRIMA FIGURA
ELEMENTALIS.

Figura Ignis

Ignis	Aër	Aqua	Terra
Aër	Ignis	Terra	Aqua
Aqua	Terra	Ignis	Aër
Terra	Aqua	Aër	Ignis

Figura Aëris

Aër	Ignis	Aqua	Terra
Ignis	Aër	Terra	Aqua
Aqua	Terra	Aër	Ignis
Terra	Aqua	Ignis	Aër

Figura Aquæ

Aqua	Terra	Aër	Ignis
Terra	Aqua	Ignis	Aër
Aër	Ignis	Aqua	Terra
Ignis	Aër	Terra	Aqua

Figura Terræ

Terra	Aqua	Aër	Ignis
Aqua	Terra	Ignis	Aër
Aër	Ignis	Terra	Aqua
Ignis	Aër	Aqua	Terra

Figura 3.2: Cuadrado Latino desarrollado Ramón Llull (Fuente: Ars Demostrativa de la edición latina de Maguncia, 1722, vol.III)

Sin embargo, la primera definición formal del concepto *cuadrado latino* fue dada por el matemático suizo Leonhard Euler en 1779 mientras intentaba dar solución al *Problema de los 36 oficiales* [2]. Euler hizo uso de letras provenientes del latín y el griego, otorgándole el nombre de *cuadrados greco-latinos* o *cuadrados latinos ortogonales* a estas figuras.

$A\alpha$	$B\gamma$	$C\beta$
$B\beta$	$C\alpha$	$A\gamma$
$C\gamma$	$A\beta$	$B\alpha$

Figura 3.3: Cuadrado greco-latino (Fuente: Wikipedia)

Euler demostró para estas estructuras que podían ser construidas siempre que su orden fuese impar o múltiplo de 4 y determinó que nunca se podían construir cuando el orden del cuadrado era par de clase impar, es decir, múltiplo de dos y no de cuatro. Sin embargo, los matemáticos Satyendra Nath Bose, Sharadchandra Shankar Shrikhande y Ernest Tilden Parker demostraron en (Bose, Parker, y Shrikhande, 1960) que la conjetura de Euler es falsa para todo cuadrado de orden igual o superior a diez. Como consecuencia, existen cuadrados greco-latinos de orden n para todo n mayor de dos, excepto para n igual a seis.

[2] En el Problema de los 36 oficiales se pretendía colocar en un cuadrado de tamaño 6x6 a treinta y seis militares de seis distintos regimientos y seis distintos rangos, de tal manera que ni regimiento ni rango se repitiesen por filas o columnas.

3.2– Preliminares

En esta sección, será introducida una serie de conceptos de la que se hará uso a lo largo de todo el trabajo de forma repetitiva.

3.2.1. Cuadrados latinos

Se denomina *cuadrado latino de orden n* a toda matriz cuadrada L de orden n cuyas entradas son tomadas de un conjunto *S* formado por *n* símbolos y que tiene la propiedad de que cada símbolo sólo aparece una vez en cada fila y sólo una vez en cada columna de L.

$$L \equiv \begin{array}{|c|c|c|c|}\hline 1 & 2 & 3 & 4 \\ \hline 2 & 1 & 4 & 3 \\ \hline 3 & 4 & 2 & 1 \\ \hline 4 & 3 & 1 & 2 \\ \hline \end{array}$$

Figura 3.4: Cuadrado latino de orden 4 en forma estándar.

Además, se dice que el cuadrado latino se encuentra en *forma estándar* si sus entradas toman como símbolos el conjunto de números naturales $\{1, 2, \ldots, n\}$ y las entradas de la primera fila y las de la primera columna de L aparecen en orden natural (ver Figura 3.4).

Como es de esperar, el número de cuadrados latinos crece enormemente a medida que aumenta su orden. Hasta ahora sólo se conoce exactamente el número de cuadrados latinos de orden hasta 11 (Hulpke, Kaski, y Östergård, 2011; Kolesova, Lam, y Thiel, 1990; McKay, Meynert, y Myrvold, 2007) (ver Cuadro 3.1).

Cuadro 3.1: Cantidad de cuadrados latinos en función de su tamaño n

n	Cantidad de cuadrados
1	1
2	2
3	12
4	576
5	161280
6	812851200
7	61479419904000
8	108776032459082956800
9	5524751496156892842531225600
10	9982437658213039871725064756920320000
11	776966836171770144107444346734230682311065600000

3.2.2. Cuadrados latinos parciales

De forma análoga a la definición de cuadrado latino, un *cuadrado latino parcial de orden* n se define como una matriz cuadrada *P* de orden n cuyas celdas pueden estar vacías o tomar el valor de algún símbolo del conjunto de símbolos *S* previamente mencionado, de tal forma que cada símbolo aparece a lo más una vez en cada fila, y a lo más una vez en cada columna. El número total de celdas no vacías constituye el *tamaño* del cuadrado parcial. Si dicho tamaño toma el valor de n^2, entonces P es un cuadrado latino de orden *n*. Así, por ejemplo, la Figura 3.5 muestra un cuadrado latino de orden y tamaño cuatro.

De ahora en adelante, denominaremos PLS_n y LS_n a los conjuntos de cuadrados latinos parciales y de cuadrados latinos de orden *n*, respectivamente, ambos teniendo el conjunto $[n] := \{1, \ldots, n\}$ como conjunto de símbolos S.

$P \equiv$

1		3	
		2	
	3		

Figura 3.5: Cuadrado latino parcial de orden 4

Todo cuadrado latino parcial $P = (p_{i,j}) \in \mathrm{PLS}_n$ viene unívocamente determinado por su conjunto de entradas

$$\mathrm{Ent}(P) := \{(i, j, p_{i,j}) \colon i, j, p_{i,j} \in [n]\}\,.$$

Así, una entrada de P es un triple $(i, j, p_{i,j})$ donde $p_{i,j}$ es el símbolo que aparece en la celda (i, j) de P. Es decir, en su fila i-ésima y en su columna j-ésima. Una *completación* de P es cualquier cuadrado latino L del mismo orden tal que el conjunto de entradas de P pertenece al conjunto de entradas de L. Es decir, $\mathrm{Ent}(P) \subseteq \mathrm{Ent}(L)$. Si se cumple esta condición, entonces podemos decir que P es *completable* a L. De existir un único cuadrado latino L con estas características, entonces P es considerado como un cuadrado latino parcial únicamente completable. El problema de decidir si un cuadrado latino parcial P es únicamente completable es NP-completo. Más aún, el problema de encontrar la existencia de una completación para P también es NP-completo.

3.2.3. Conjunto crítico de un cuadrado latino

En 1977, el científico británico John Ashworth Nelder (Nelder, 1977) introdujo el concepto de *conjunto crítico* de un cuadrado latino $L \in \mathrm{LS}_n$ como cualquier cuadrado latino parcial $P \in \mathrm{PLS}_n$ únicamente completable a L, de manera que, si $P' \in \mathrm{PLS}_n$ es tal que $\mathrm{Ent}(P') \subseteq \mathrm{Ent}(P)$, entonces P' no es únicamente completable a L.

Se dice que el conjunto crítico es *mínimo* si no existe otro conjunto crítico de L cuyo tamaño sea menor. De la misma manera, se dice que el conjunto crítico es *máximo* si no existe otro conjunto crítico de L cuyo tamaño sea mayor. De ahora en adelante, $\mathrm{scs}(n)$ y $\mathrm{lcs}(n)$ denotan, respectivamente, el tamaño mínimo y máximo de los conjuntos críticos de cualquier cuadrado latino de orden n. Además, un conjunto crítico es *fuerte* si su conjunto de entradas puede completarse de manera secuencial por una serie de *entradas forzadas*. Cabe indicar que una entrada forzada en un cuadrado latino parcial $P \in \mathrm{PLS}_n$ es una terna $(i, j, k) \in [n] \times [n] \times [n]$ de tal manera que la celda (i, j) se encuentra vacía en la i-ésima fila o la j-ésima columna, siendo el símbolo k el único que no aparece en dicha fila o columna. Así, por ejemplo, la entrada $(1, 3, 3)$ estaría forzada en el cuadrado latino parcial de la Figura 3.6.

$P \equiv$

1	2		
		4	
			2
	3		

Figura 3.6: Conjunto crítico mínimo para un cuadrado latino de orden 4

Nelder introdujo el problema relativo al cálculo del tamaño de los conjuntos críticos mínimo y máximo para cualquier cuadrado latino L dado. Dos años más tarde, el matemático Bohdan Smetaniuk (Smetaniuk, 1979) demostró que $\mathrm{scs}(2n) \leq \lfloor n^2/4 \rfloor$, asegurando además la existencia de dichos conjuntos inicialmente conjeturados por Nelder. Este hecho fue decubierto también por Donald Joseph Curran y Gerrit Hendrik Johannes Van Ree (Curran y Van Rees, 1979), quienes además demostraron la misma inecuación para el caso impar. Por otra parte, determinaron los valores de los conjuntos críticos mínimos para los cuadrados latinos de orden menor o igual a 5, y establecieron límites para el mayor y menor tamaño de conjunto crítico.

3.2.4. Isotopismos

El *grupo simétrico* S_n es el grupo de permutaciones del conjunto $[n]$. Toda permutación $\pi \in S_n$ puede descomponerse de forma única en producto de ciclos disjuntos. Su *estructura cíclica* z_π es la expresión $n^{d_n} \dots 1^{d_1}$, donde, para cada $\ell \in \{1, \dots, n\}$, el valor d_ℓ denota el número de ciclos de longitud ℓ en la citada descomposición de π en ciclos disjuntos. En la práctica, si $d_\ell = 1$, no suele incluirse el exponente d_ℓ en la expresión z_π. Así, por ejemplo, la permutación $(123)(45)(67)(8) \in S_8$ tiene estructura cíclica 32^21.

Un *isotopismo* de un cuadrado latino parcial $P \in \mathrm{PLS}_n$ es una terna $\Theta = (\alpha, \beta, \gamma) \in S_n \times S_n \times S_n$. Si aplicamos este isotopismo sobre P obtenemos un nuevo cuadrado latino parcial P^Θ que surge como consecuencia de aplicar la permutación α (respectivamente, β y γ) sobre las filas (respectivamente, columnas y símbolos) de P. En otras palabras,

$$\mathrm{Ent}(P^\Theta) = \{(\alpha(i),\, \beta(j),\, \gamma(k))\colon\ (i,j,k) \in \mathrm{Ent}(P)\}.$$

La *estructura cíclica* de Θ se define como la terna $z_\Theta = (z_\alpha,\, z_\beta,\, z_\gamma)$. Así, por ejemplo, la estructura cíclica del isotopismo $((123)(45)(6),\, (12)(34)(56), (123456)) \in S_6 \times S_6 \times S_6$ es la terna $(321, 2^3, 6)$. Por otra parte, para cada permutación $\pi \in S_3$ se obtiene el cuadrado latino parcial $P^\pi \in \mathrm{PLS}_n$, *conjugado* de P, donde:

$$\mathrm{Ent}(P^\pi) = \{(i_{\pi(1)}, i_{\pi(2)}, i_{\pi(3)})\colon\ (i_1,i_2,i_3) \in \mathrm{Ent}(P)\}$$

Se dice que la permutación π es un *paratrofismo* que lleva P a P^π. Se trata de una simple permutación en el orden en el que aparecen las filas, columnas y símbolos en las distintas entradas de P. Así por ejemplo, $P^{(12)}$ es la traspuesta de P, que también constituye un cuadrado latino parcial.

Ejemplo 3.1. Consideremos el siguiente cuadrado latino L de orden cuatro usado anteriormente, y el isotopismo $\Theta = ((12)(34), (1234), (123))$:

$$L \equiv \begin{array}{|c|c|c|c|}\hline 1 & 2 & 3 & 4 \\ \hline 2 & 1 & 4 & 3 \\ \hline 3 & 4 & 1 & 2 \\ \hline 4 & 3 & 2 & 1 \\ \hline \end{array}$$

Los cambios que se deben realizar son:

1. Filas:
   - Sustituir la fila 1 por la 2 y viceversa.
   - Sustituir la fila 3 por la 4 y viceversa.
2. Columnas:
   - Sustituir la columna 1 por la 2.
   - Sustituir la columna 2 por la 3.
   - Sustituir la columna 3 por la 4.
   - Sustituir la columna 4 por la 1.
3. Símbolos:
   - Sustituir el símbolo 1 por el 2.
   - Sustituir el símbolo 2 por el 3.
   - Sustituir el símbolo 3 por el 1.

$\triangleleft$

Entonces, si aplicamos el isotopismo sobre el cuadrado L:

$$L^{\Theta} \equiv \begin{array}{|c|c|c|c|}\hline 2 & 3 & 1 & 4 \\ \hline 3 & 2 & 4 & 1 \\ \hline 1 & 4 & 2 & 3 \\ \hline 4 & 1 & 3 & 2 \\ \hline \end{array}$$

Dos cuadrados latinos parciales son *paratópicos* o se encuentran en la *misma clase principal* si y solo si el primero de ellos es isotópico al conjugado del segundo. Es decir, si, aplicando un isotopismo al primero, podemos obtener el conjugado del segundo.

Cuando aplicamos un isotopismo Θ podemos encontrar casos en los que obtengamos el cuadrado latino parcial original P. Esto es, $P^{\Theta} = P$. Este isotopismo Θ se denomina *autotopismo* de P. El conjunto de autotopismos de un cuadrado latino L constituye un grupo, que se denota $\mathrm{Atop}(L)$. En la actualidad, el estudio de los grupos de autotopismos de cuadrados latinos parciales es un área activa de investigación, poniendo especial énfasis en la descripción de nuevos invariantes que faciliten su cálculo mediante computación, así como su posible aplicación en criptografía y teoría de códigos. Nuestro trabajo, como ya mencionamos al comienzo del documento, se centrará en el estudio de cuadrados latinos para su aplicación a un protocolo criptográfico de compartición de secretos.

3.2.5. Conjuntos críticos basados en autotopismos de cuadrados latinos

En 2006, el concepto de completabilidad de cuadrados latinos parciales fue generalizado (Falcón, 2006) (ver también (Falcón, 2011)), dando lugar a la $\mathfrak{F}$-completabilidad, siendo $\mathfrak{F}$ cualquier conjunto de isotopismos relativos a un cuadrado latino. Concretamente, un cuadrado latino parcial $P \in \mathrm{PLS}_n$ se denomina $\mathfrak{F}$-completable si y solo si existe una completación $L \in \mathrm{LS}_n$ de este, de tal manera que $\Theta \in \mathrm{Atop}(L)$, para todo $\Theta \in \mathfrak{F}$. De existir una única completación, P se denomina *únicamente $\mathfrak{F}$-completable*. De la misma manera, se denomina *$\mathfrak{F}$-conjunto crítico* de L si esta propiedad no se mantiene para ningún cuadrado latino parcial $Q \in \mathrm{PLS}_n$ tal que $\mathrm{Ent}(Q) \subset \mathrm{Ent}(P)$. En el caso de que $\mathfrak{F}$ esté conformado por un único isotopismo Θ, entonces se denota *Θ-conjunto crítico*. De igual forma, se hace uso del término *únicamente Θ-completable*.

Sean $L \in \mathrm{LS}_n$ y $\Theta \in \mathrm{Atop}(L)$. De ahora en adelante, denotaremos el conjunto de Θ-conjuntos criticos del cuadrado latino L como $CS_{\theta}(L)$. Además, $\mathrm{scs}_{\Theta}(L)$ y $\mathrm{lcs}_{\Theta}(L)$ denotarán, respectivamente, el menor y mayor tamaño de Θ-conjunto crítico de L.

3.2.6. Orbitas basadas en autotopismos de cuadrados latinos

Supongamos un cuadrado latino $L \in \mathrm{LS}_n$ y un autotopismo $\Theta(\alpha, \beta, \gamma) \in \mathrm{Atop}(L)$. Para cada entrada $(i, j, k) \in \mathrm{Ent}(L)$ se define su *órbita* respecto a Θ como el conjunto de entradas de L tales que, al aplicar Θ sobre alguna de ellas podemos obtener otra sucesivamente hasta obtener la entrada por la que comenzamos. Más concretamente:

$$\mathrm{Orb}_{\Theta}((i, j, k)) := \bigcup_{m \in \mathbb{N}} \{(\alpha^m(i),\, \beta^m(j), \gamma^m(k))\} \subseteq \mathrm{Ent}(L).$$

Si dicho conjunto está formado por una única terna, la órbita se dice *trivial*. Esto ocurre cuando $\alpha^2(i) = i$, $\beta^2(j) = j$ y $\gamma^2(k) = k$, para todos $i, j, k \in [n]$. Si este no es el caso, entonces la órbita se llama

- *Principal*, si todo par de entradas (i_1, j_1, k_1) e (i_2, j_2, k_2) en la órbita verifican que $i_1 \neq i_2$, $j_1 \neq j_2$ y $k_1 \neq k_2$.

- *Secundaria*, si contiene dos entradas con una componente común. En dicho caso, la órbita se dice *monótona por filas* (respectivamente, *por columnas*) si todas sus entradas están en la misma fila (respectivamente, columna). Más aún, dos órbitas monótonas por filas (respectivamente, por columnas) se dicen *paralelas* si los correspondientes conjuntos de columnas y símbolos (respectivamente, filas y símbolos) de sus entradas coinciden.

  Por su parte, una órbita secundaria se dice *monótona por símbolos* si todas sus entradas tienen el mismo símbolo. Más aún, dos órbitas monótonas por símbolos se dicen *paralelas* si los correspondientes conjuntos de filas y comlumnas de sus entradas coinciden.

  Finalmente, si una órbita secundaria no es monótona por filas, columnas of símbolos, entonces se dice que es *no monótona*.

Las entradas de L pueden pues clasificarse atendiendo a sus respectivas órbitas. Es así que el conjunto $\mathrm{Orb}_\Theta(L)$ de órbitas de L respecto a Θ constituye una partición del conjunto de entradas $\mathrm{Ent}(L)$.

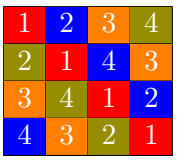
Ejemplo 3.2. Consideremos el siguiente cuadrado latino L de orden cuatro usado anteriormente y uno de sus autotopismos $\Theta = ((1234), (1234), (24)) \in \mathrm{Atop}(L)$:

$$L \equiv \begin{array}{|c|c|c|c|}\hline 1&2&3&4\\\hline 2&1&4&3\\\hline 3&4&1&2\\\hline 4&3&2&1\\\hline\end{array}$$

Se tiene entonces que $\mathrm{Orb}_\Theta(L) = \{O_1, O_2, O_3, O_4\}$, donde

- $O_1 = \{(1,1,1), (2,2,1), (3,3,1), (4,4,1)\}$.
- O_2: $\{(1,2,2), (2,3,4), (3,4,2), (4,1,4)\}$.
- O_3: $\{(1,3,3), (2,4,3), (3,1,3), (4,2,3)\}$.
- O_4: $\{(1,4,4), (2,1,2), (3,2,4), (4,3,2)\}$.

De manera visual, obtenemos lo que se denomina una Θ-*coloración* del cuadrado latino L:



◁

Cabe destacar que el número total de órbitas asociadas a un autotopismo Θ de un cuadrado latino $L \in \mathrm{LS}_n$ marca el límite superior del tamaño de cualquiera de sus Θ-conjuntos críticos. Téngase en cuenta para ello que, a partir de una única entrada a la que se aplica de forma iterativa Θ, se puede determinar todas aquellas entradas que pertenecen a su misma órbita. Dicho número de órbitas asociada a un autotopismo depende exclusivamente de la estructura cíclica del mismo. Más concretamente, dado un autotopismo $\Theta = (\alpha, \beta, \gamma)$ de un cuadrado latino $L \in \mathrm{LS}_n$, sea $z_\pi = n^{d_n^\pi} \ldots 1^{d_1^\pi}$ la estructura cíclica de la permutación $\pi \in \{\alpha, \beta, \gamma\}$. El número total de órbitas asociada a Θ en L es

$$|\mathrm{Orb}_\Theta(L)| = \sum_{1 \le i,j \le n} \frac{i \cdot d_i^\alpha \cdot j \cdot d_j^\beta}{\mathrm{m.c.m.}(i,j)}, \tag{3.1}$$

donde $\mathrm{m.c.m.}$ denota el mínimo común múltiplo. Así, el número de órbitas en el Ejemplo 3.2 es

$$\frac{4 \cdot 1 \cdot 4 \cdot 1}{4} = 4.$$

3.2.7. Aplicación de cuadrados latinos al proceso de compartición de secretos

Hoy en día, en los sistemas de información, es normal encontrarnos con el hecho de que se nos requiera realizar ciertas operaciones con el objetivo de mantener la confidencialidad y la integridad de la información.

Por norma general, el acceso a un sistema está garantizado mediante el uso de una clave, una contraseña, etc. Si esta clave se divide y comparte con varios participantes con el objetivo de que sólo ciertos grupos autorizados puedan acceder al sistema, podemos afirmar que nos encontramos ante un sistema de seguridad compartida. En la práctica, aparece la necesidad de implementar jerarquía dentro de estos grupos con el fin de que si uno de sus miembros se encuentra incapacitado, este pueda ser sustituido por otros de un nivel inferior. Es aquí donde debemos introducir el concepto de *esquema de compartición de secretos*.

Se denomina *esquema de compartición de secretos* (Cooper y cols., 1994) al procedimiento de dividir una *clave* o *secreto* K en n piezas de información llamadas *sombras* entre un conjunto $\mathcal{P}$ de participantes de tal forma que el acceso sólo está permitido a ciertos grupos de participantes. El conjunto de dichos grupos es un subconjunto del conjunto de partes de $\mathcal{P}$. Se denomina *estructura de acceso* y suele denotarse como Γ.

Los primeros esquemas de compartición de secretos (Villar, 2017) vinieron de la mano de Blackley (Blakley, 1979) y Shamir (Shamir, 1979) de manera independiente. En el esquema de Shamir, por ejemplo, se le asignaba a cada participante un fragmento $s_i = r(x_i)$ relativo a un secreto S, donde x_i representa un elemento único y no nulo del cuerpo $\mathbb{Z}_p$, con p un número primo, y $r(x)$ hace referencia a un polinomio interpolador de grado $t-1$, donde t es un entero tal que $1 \leq t \leq |\mathcal{P}|$.

Un ejemplo más actual, y en el que nos basaremos para el desarrollo de nuestro propio esquema de compartición de secretos, es el propuesto en (Cooper y cols., 1994) donde se usa un cuadrado latino como clave. El proceso que se sigue es el siguiente:

1. Seleccionar un cuadrado latino L de tal manera que su orden se hace público pero el cuadrado será privado, pues representa la clave del sistema.
2. Seleccionar un conjunto S formado por la unión de varios conjuntos críticos relativos a L.
3. Cada entrada $e \in \mathrm{Ent}(L)$ que esté incluida en un conjunto crítico en S constituye una sombra e de la clave y es asignada a un participante.
4. Cuando un grupo de participantes conforman un conjunto crítico con las sombras que les han sido asignadas, pueden reconstruir la clave del sistema y acceder al mismo. Dicho grupo forma parte por tanto de la estructura de acceso Γ del esquema.

Ejemplo 3.3. Supongamos el siguiente cuadrado latino L considerado como clave del sistema de compartición de secretos que queremos desarrollar.

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

El siguiente paso es encontrar un conjunto formado por la unión de varios conjuntos críticos relativos al cuadrado latino que se ha tomado como clave. Una posibilidad podría ser:

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

Las sombras generadas son repartidas entre los participantes y se forman los grupos autorizados que podrán reconstruir la clave original. Algunos ejemplos de reparto pueden ser:

- $A_1 = \{(1,1,1),(1,2,2),(2,4,3),(3,2,4),(4,3,2)\}$.
- $A_2 = \{(1,1,1),(1,3,3),(2,4,3),(3,2,4),(4,3,2)\}$.
- $A_3 = \{(1,1,1),(1,4,4),(2,4,3),(3,2,4),(4,3,2)\}$.
- $A_4 = \{(1,3,3),(1,4,4),(2,2,1),(3,4,2),(4,1,4)\}$.
- ...

$\triangleleft$

3.3– Resultados previos

En esta sección se describirán algunos de los lemas, teoremas y proposiciones que se han usado durante el trabajo:

Lema 3.4. *(Falcón y cols., 2020) Consideremos un isotopismo $\Theta = (\delta_1, \delta_2, \delta_3) \in S_n \times S_n \times S_n$ y una permutación $\pi \in S_3$. Definimos el isotopismo*

$$\Theta^\pi := (\delta_{\pi(1)}, \delta_{\pi(2)}, \delta_{\pi(3)}) \in S_n \times S_n \times S_n.$$

Entonces, $(P^\pi)^{\Theta^\pi} = (P^\Theta)^\pi$, para todo cuadrado latino parcial $P \in \mathrm{PLS}_n$.

Lema 3.5. *(Falcón y cols., 2020) Existe una correspondencia uno a uno entre los grupos de autotopismos de cualquier par de cuadrados latinos parciales que sean paratópicos entre sí.*

Demostración. Suponemos $P_1, P_2 \in \mathrm{PLS}_n$ dos cuadrados latinos parciales paratópicos. Entonces, existe una permutación $\pi \in S_3$ y un isotopismo $\Theta \in S_n \times S_n \times S_n$ tal que $P_2 = ((P_1)^\pi)^\Theta$. Entonces, el resultado puede obtenerse directamente del Lema 3.4. Concretamente, si $\Theta_1 \in \mathrm{Atop}(P_1)$, entonces $\Theta\Theta_1^\pi\Theta^{-1} \in \mathrm{Atop}(P_2)$. $\square$

Proposición 3.6. *(Falcón y cols., 2020) Sean $L_1, L_2 \in \mathrm{LS}_n$ dos cuadrados latinos paratópicos tales que $L_2 = ((L_1)^\pi)^\Theta$, para cierta permutación $\pi \in S_3$ y cierto isotopismo $\Theta \in S_n \times S_n \times S_n$. Sean además $\Theta_1 \in \mathrm{Atop}(L_1)$ y $\Theta_2 = \Theta\Theta_1^\pi\Theta^{-1} \in \mathrm{Atop}(L_2)$. Entonces hay una correspondencia uno a uno entre ambos conjuntos $\mathrm{CS}_{\Theta_1}(L_1)$ and $\mathrm{CS}_{\Theta_2}(L_2)$ de tal manera que $\mathrm{scs}_{\Theta_1}(L_1) = \mathrm{scs}_{\Theta_2}(L_2)$ y $\mathrm{lcs}_{\Theta_1}(L_1) = \mathrm{lcs}_{\Theta_2}(L_2)$.*

Demostración. Podemos obtener el resultado atendiendo a la demostración del Lema 3.5. Concretamente, si $P \in \mathrm{CS}_{\Theta_1}(L_1)$, entonces $(P^\pi)^\Theta \in \mathrm{CS}_{\Theta_2}(L_2)$. $\square$

Estos resultados nos permiten trabajar con representantes de las clases principales de cuadrados latinos de orden n dado. Por ejemplo, para $n \in \{2,3,4,5\}$, podemos tomar los siguientes representantes:

$$L_2 \equiv \begin{array}{|c|c|}\hline 1&2\\\hline 2&1\\\hline\end{array} \qquad L_3 \equiv \begin{array}{|c|c|c|}\hline 1&2&3\\\hline 2&3&1\\\hline 3&1&2\\\hline\end{array} \qquad L_{4,1} \equiv \begin{array}{|c|c|c|c|}\hline 1&2&3&4\\\hline 2&1&4&3\\\hline 3&4&1&2\\\hline 4&3&2&1\\\hline\end{array} \qquad L_{4,2} \equiv \begin{array}{|c|c|c|c|}\hline 1&2&3&4\\\hline 2&1&4&3\\\hline 3&4&2&1\\\hline 4&3&1&2\\\hline\end{array}$$

$$L_{5,1} \equiv \begin{array}{|c|c|c|c|c|}\hline 1&2&3&4&5\\\hline 2&3&4&5&1\\\hline 3&4&5&1&2\\\hline 4&5&1&2&3\\\hline 5&1&2&3&4\\\hline\end{array} \qquad L_{5,2} \equiv \begin{array}{|c|c|c|c|c|}\hline 1&2&3&4&5\\\hline 2&1&4&5&3\\\hline 3&4&5&1&2\\\hline 4&5&2&3&1\\\hline 5&3&1&2&4\\\hline\end{array} \tag{3.2}$$

En la práctica no es preciso conocer el grupo completo de autotopismos de un cuadrado latino L para conocer el tamaño de sus conjuntos Θ-criticos para todo $\Theta \in \mathrm{Atop}(L)$. De hecho, es suficiente con que se centre la atención en un representante de cada clase conjugada[3] del grupo de autotopismos. Cabe observar aquí que todos los autotopismos relativos a la misma clase conjugada, tienen la misma estructura cíclica.

Lema 3.7. *(Falcón y cols., 2020) Supongamos Θ_1 y Θ_2 dos autotopismos conjugados en el grupo de autotopismos del cuadrado latino $L \in \mathrm{LS}_n$. Entonces, existe una correspondencia uno a uno entre los conjuntos críticos $\mathrm{CS}_{\Theta_1}(L)$ y $\mathrm{CS}_{\Theta_2}(L)$ de tal manera que $\mathrm{scs}_{\Theta_1}(L) = \mathrm{scs}_{\Theta_2}(L)$ y $\mathrm{lcs}_{\Theta_1}(L) = \mathrm{lcs}_{\Theta_2}(L)$.*

Proposición 3.8. *Si $L \in \mathrm{LS}_n$ y $\Theta = (\alpha, \beta, \gamma) \in \mathrm{Atop}(L)$, entonces ningún Θ-conjunto crítico de L tendrá más de una entrada en la misma órbita. Como consecuencia:*

$$0 < \mathrm{scs}_\Theta(L) \leq \mathrm{lcs}_\Theta(L) \leq |\mathrm{Orb}_\Theta(L)|.$$

Este hecho es fácilmente verificable si atendemos a las definiciones descritas en el apartado anterior. Puesto que las entradas de un cuadrado latino está compuesto por el conjunto de sus órbitas y cada órbita puede obtenerse completamente a partir de una de sus entradas, un cuadrado latino será únicamente completable a partir del conjunto resultante de tomar un elemento de cada órbita.

Proposición 3.9. *(Falcón y cols., 2020) Supongamos el cuadrado latino $L \in \mathrm{LS}_n$ y el autotopismo $\Theta \in \mathrm{Atop}(L)$. Si existen m órbitas secundarias paralelas del mismo tipo, es decir, monótonas por filas, columnas o símbolos, entonces cada Θ-conjunto crítico de L contiene, al menos, $m-1$ entradas. Por tanto:*

$$\mathrm{scs}_\Theta(L) \geq m - 1.$$

Lema 3.10. *(Falcón y cols., 2020) Consideremos un cuadrado latino $L \in \mathrm{LS}_n$, un par de isotopismos $\Theta_1 \in \mathrm{Atop}(L)$ y $\Theta_2 \in S_n \times S_n \times S_n$, y una permutación $\pi \in S_3$. Si $(L^\pi)^{\Theta_2} = L$, entonces existe una correspondencia uno a uno entre ambos conjuntos $CS_{\Theta_1}(L)$ y $CS_{\Theta_2\Theta_1^\pi\Theta_2^{-1}}(L)$, de tal manera que $\mathrm{scs}_{\Theta_1}(L) = \mathrm{scs}_{\Theta_2\Theta_1^\pi\Theta_2^{-1}}(L)$ y $\mathrm{lcs}_{\Theta_1}(L) = \mathrm{lcs}_{\Theta_2\Theta_1^\pi\Theta_2^{-1}}(L)$.*

[3]Dos elementos a y b relativos a un grupo G se dice que son conjugados si y solo si existe un tercer elemento c que también pertenece a G de tal manera que $b = cac^{-1}$.

Teorema 3.11. *(Falcón y cols., 2020) Sea $L \in \mathrm{LS}_n$ y $\Theta = (\alpha, \beta, \mathrm{Id}_n) \in \mathrm{Atop}(L)$. Si $z_\alpha = z_\beta = n$, entonces se cumplen las siguientes afirmaciones.*

a) $\mathrm{scs}_\Theta(L) = \mathrm{lcs}_\Theta(L) = n - 1$.

b) $|CS_\Theta(L)| = n^n$.

Proposición 3.12. *(Falcón y cols., 2020) Supongamos P y Q dos subcuadrados latinos parciales (no necesariamente distintos) relativos a un cuadrado latino $L \in \mathrm{LS}_n$ de tal manera que se cumpla una de las siguientes condiciones:*

- $\mathrm{Filas}(P) = \mathrm{Filas}(Q)$.
- $\mathrm{Columnas}(P) = \mathrm{Columnas}(Q)$.
- $\mathrm{Simbolos}(P) = \mathrm{Simbolos}(Q)$.

Además, supongamos un autotopismo $\Theta \in \mathrm{Atop}(L)$ tal que $P^\Theta = Q$ and $Q^\Theta = P$. Entonces:

$$(\mathrm{Ent}(P) \cup \mathrm{Ent}(Q)) \cap \mathrm{Orb}_\Theta(R) \neq \emptyset$$

para cualquier Θ-conjunto crítico relativo a L.

De esta manera, aplicando los resultados anteriores, se puede simplificar el número de autotopismos a considerar en el análisis de los tamaños posibles para los Θ-conjuntos críticos. El Cuadro 3.2 muestra los tamaños máximo y mínimo de los Θ-conjuntos críticos asociados a los cuadrados latinos de orden $n \in \{2, 3, 4, 5\}$, para los autotopismos correspondientes.

Cuadro 3.2: Autotopismos relativos a cuadrados latinos L_2–$L_{5,2}$.

L	$\Theta \in \mathrm{Atop}(L)$	z_Θ	$\lvert\mathrm{CS}_\Theta(L)\rvert$	$\mathrm{scs}_\Theta(L)$	$\mathrm{lcs}_\Theta(L)$
L_2	$(\mathrm{Id}_2, \mathrm{Id}_2, \mathrm{Id}_2)$	$(1^2, 1^2, 1^2)$	4	1	1
	$((12), (12), \mathrm{Id}_2)$	$(2, 2, 1^2)$	4	1	1
L_3	$(\mathrm{Id}_3, \mathrm{Id}_3, \mathrm{Id}_3)$	$(1^3, 1^3, 1^3)$	27	2	3
	$((12), (12), (13))$	$(21, 21, 21)$	14	1	2
	$((123), (132), \mathrm{Id}_3))$	$(3, 3, 1^3)$	27	2	2
	$((123), (123), (132))$	$(3, 3, 3)$	9	1	1
$L_{4,1}$	$(\mathrm{Id}_4, \mathrm{Id}_4, \mathrm{Id}_4)$	$(1^4, 1^4, 1^4)$	576	5	7
	$((12)(34), (12)(34), \mathrm{Id}_4)$	$(2^2, 2^2, 1^4)$	192	4	4
	$((23), (14), (14))$	$(21^2, 21^2, 21^2)$	256	4	4
	$((12)(34), (13)(24), (14)(23))$	$(2^2, 2^2, 2^2)$	256	3	3
	$((243), (134), (134))$	$(31, 31, 31)$	90	2	2
	$((1234), (1234), (24))$	$(4, 4, 21^2)$	64	2	2
$L_{4,2}$	$(\mathrm{Id}_4, \mathrm{Id}_4, \mathrm{Id}_4)$	$(1^4, 1^4, 1^4)$	736	4	6
	$((12)(34), (12)(34), \mathrm{Id}_4)$	$(2^2, 2^2, 1^4)$	192	4	4
	$((13)(24), (14)(23), (34))$	$(2^2, 2^2, 21^2)$	224	3	3
	$((12), (12), (34))$	$(21^2, 21^2, 21^2)$	256	4	4
	$((1324), (1324), (12)(34))$	$(4, 4, 2^2)$	64	2	2
	$((1423), (1324), \mathrm{Id}_4)$	$(4, 4, 1^4)$	256	3	3
$L_{5,1}$	$(\mathrm{Id}_5, \mathrm{Id}_5, \mathrm{Id}_5)$	$(1^5, 1^5, 1^5)$	53250	6	10
	$((12)(35), (13)(45), (14)(23))$	$(2^21, 2^21, 2^21)$	3088	3	5
	$((2354), (1243), (1243))$	$(41, 41, 41)$	832	3	3
	$((12345), (15432), \mathrm{Id}_5)$	$(5, 5, 1^5)$	3125	4	4
	$((12345), (12345), (13524))$	$(5, 5, 5)$	250	2	2
$L_{5,2}$	$(\mathrm{Id}_5, \mathrm{Id}_5, \mathrm{Id}_5)$	$(1^5, 1^5, 1^5)$	48462	7	11
	$((13)(45), (25)(34), (13)(45))$	$(2^21, 2^21, 2^21)$	2896	3	5
	$((345), (345), (345))$	$(31^2, 31^2, 31^2)$	8424	5	6

CAPÍTULO 4

Análisis de antecedentes y aportación realizada

Como ya se mencionó al comienzo del proyecto, el objetivo principal de este trabajo será desarrollar un algoritmo que permita obtener el secreto para un protocolo de compartición de secretos basado en cuadrados latinos, así como las posibles sombras a repartir entre los participantes. Dicho secreto será un cuadrado latino y las sombras se obtendrán a partir de los Θ-conjuntos críticos asociados a dicho cuadrado latino.

De manera paralela al estudio de dicho protocolo, se realizará un análisis estadístico sobre los tamaños de Θ-conjuntos críticos de cuadrados latinos de orden seis, de los que, hasta la fecha, el conocimiento que se tiene es prácticamente nulo. Debemos ser conscientes de que, si se consigue conocer Θ-conjuntos críticos de cuadrados latinos de órdenes superiores, se produciría un aumento en la seguridad del protocolo de compartición de secretos. Esto se debe a que la fuerza bruta se vuelve una opción cada vez menos viable para la obtención de la clave atendiendo al incremento exponencial de la cantidad de cuadrados latinos a medida que crece su orden (ver Cuadro 3.1).

4.1– Análisis de antecedentes

4.1.1. Protocolo para la compartición de secretos basado en cuadrados latinos

Tal y como se ha indicado en la Subsección 3.2.7, los principales precursores del uso de cuadrados latinos en el ámbito de la criptografía fueron J. Cooper, Diane Donovan y Jennifer Seberry (Cooper y cols., 1994). Las versiones derivadas de este sistema son muy diversas. Una de ellas, por ejemplo, es (Ashwini, Venkaiah, y Bhukya, 2021) en la cual, los autores aprovechan las propiedades de los cuadrados latinos y los autotopismos relativos a estos para reducir el problema de disponibilidad de la clave. Para ello se trabaja con divisiones del autotopismo Θ sobre grupos reducidos de participantes de tal manera que cualquiera de estos grupos puede reconstruir la clave. Otro posible ejemplo es (Stones, Su, Liu, Wang, y Lin, 2015), en el que se toma un autotopismo como clave en lugar de un cuadrado latino.

El sistema que se desarrollará en este trabajo estará basado en el esquema de compartición de secretos de J. Cooper, Diane Donovan y Jennifer Seberry (Cooper y cols., 1994), al que se le añadirán modificaciones basadas en el uso de autotopismos de cuadrados latinos para dificultar la obtención de la clave por parte de terceros no implicados.

Como podrá comprobarse en secciones posteriores, la novedad del sistema aquí desarrollado radica en el uso de Θ-conjuntos críticos como sombras que permitirán recuperar el secreto, que será su cuadrado latino asociado. El verdadero potencial radica en el hecho de emplear cuadrados latinos de órdenes superiores a los ya estudiados, pues, como mencionábamos anteriormente, el número de cuadrados latinos aumenta enormemente a medida que incrementamos el órden de

estos, haciendo del ataque por fuerza bruta algo prácticamente inservible. Esta es la razón principal por la que se realiza, de manera paralela, una investigación sobre los Θ-conjuntos críticos basados en autotopismos de cuadrados latinos de orden superior a cinco. Concretamente, nuestro trabajo de campo versará sobre los tamaños de conjuntos críticos basados en autotopismos no triviales de cuadrados latinos de orden seis, aunque es aplicable a cualquier orden mayor.

4.1.2. Análisis de los conjuntos críticos basados en autotopismos no triviales de cuadrados latinos de hasta orden 5

Hace poco menos de dos años, Raúl M. Falcón, Laura Johnson y Stephanie Perkins (Falcón y cols., 2020) introdujeron todos los conceptos que mencionamos en el Capítulo 3 acerca de conjuntos críticos basados en autotopismos de cuadrados latinos. En particular, realizaron un censo de los conjuntos críticos basados en autotopismos no triviales de cuadrados latinos de orden menor que seis. Para ello, llevaron a cabo un estudio sobre autotopismos representantes de cada clase conjugada y cuadrados latinos representantes de cada clase principal. Para cada autotopismo Θ del cuadrado latino L bajo estudio, los autores indicaron los tamaños mínimo ($\mathrm{scs}_\Theta(L)$) y máximo ($\mathrm{lcs}_\Theta(L)$) que toman sus Θ-conjuntos críticos. Con vistas a ilustrar dicho estudio, mostramos aquí un ejemplo para cada representante descrito en (3.2). Cada representante se muestra ya coloreado atendiendo al autotopismo correspondiente.

Ejemplo 4.1. (Falcón y cols., 2020) Consideramos el autotopismo $\Theta = ((12), (12), \mathrm{Id}_2)$ para el cuadrado latino

$$L_2 \equiv \begin{array}{|c|c|}\hline 1 & 2 \\ \hline 2 & 1 \\ \hline \end{array}$$

Según la Proposición 3.8, $\mathrm{lcs}_\Theta(L_2) \leq 2$, el número de órbitas. Como cada entrada de L_2 es Θ-forzada por cualquier otra entrada,

$$\mathrm{scs}_\Theta(L_2) = \mathrm{lcs}_\Theta(L_2) = 1.$$

$\triangleleft$

Ejemplo 4.2. (Falcón y cols., 2020) Consideremos el autotopismo $\Theta = ((123), (132), \mathrm{Id}_3)$ del cuadrado latino

$$L_3 \equiv \begin{array}{|c|c|c|}\hline 1 & 2 & 3 \\ \hline 2 & 3 & 1 \\ \hline 3 & 1 & 2 \\ \hline \end{array}$$

Dado que el conjunto de órbitas $\mathrm{Orb}_\Theta(L_3)$ está formado por tres órbitas paralelas monótonas por símbolos, las Proposiciones 3.8 y 3.9 implican que $2 \leq \mathrm{scs}_\Theta(L_3) \leq \mathrm{lcs}_\Theta(L_3) \leq 3$. De hecho, como cada entrada de L_3 es Θ-forzada por dos entradas cualesquiera que pertenezcan a dos órbitas secundarias distintas, resulta que

$$\mathrm{scs}_\Theta(L_3) = \mathrm{lcs}_\Theta(L_3) = 2.$$

$\triangleleft$

Ejemplo 4.3. (Falcón y cols., 2020) Consideremos el autotopismo $\Theta = ((1234), (1234), (24))$ para el cuadrado latino

$$L_{4,1} \equiv \begin{array}{|c|c|c|c|}\hline 1 & 2 & 3 & 4 \\ \hline 2 & 1 & 4 & 3 \\ \hline 3 & 4 & 1 & 2 \\ \hline 4 & 3 & 2 & 1 \\ \hline \end{array}$$

Dado que el conjunto de órbitas $\mathrm{Orb}_\Theta(L_{4,1})$ está conformado por dos órbitas paralelas monótonas por símbolos y dos órbitas no monótonas, la Proposición 3.9 implica que cada Θ-conjunto crítico de $L_{4,1}$ contiene una entrada relativa a una de las órbitas monótonas por símbolos y una relativa a una órbita no monótona. Por tanto:

$$\mathrm{scs}_\Theta(L_{4,1}) = \mathrm{lcs}_\Theta(L_{4,1}) = 2.$$

$\triangleleft$

Ejemplo 4.4. (Falcón y cols., 2020) Consideremos el autotopismo $\Theta = ((1324), (1324), (12)(34))$ para el cuadrado latino

$$L_{4,2} \equiv \begin{array}{|c|c|c|c|}\hline 1&2&3&4\\\hline 2&1&4&3\\\hline 3&4&2&1\\\hline 4&3&1&2\\\hline\end{array}$$

Dado que el conjunto de órbitas $\mathrm{Orb}_\Theta(L_{4,2})$ está formado por cuatro órbitas no monótonas, la Proposición 3.12 implica que

$$\mathrm{scs}_\Theta(L_{4,2}) = \mathrm{lcs}_\Theta(L_{4,2}) = 2$$

$\triangleleft$

Ejemplo 4.5. (Falcón y cols., 2020) Consideremos el autotopismo $\Theta = ((12345), (12345), (13524))$ para el cuadrado latino

$$L_{5,1} \equiv \begin{array}{|c|c|c|c|c|}\hline 1&2&3&4&5\\\hline 2&3&4&5&1\\\hline 3&4&5&1&2\\\hline 4&5&1&2&3\\\hline 5&1&2&3&4\\\hline\end{array}$$

El conjunto de órbitas $\mathrm{Orb}_\Theta(L_{5,1})$ se compone de cinco órbitas principales. Un estudio sencillo de los casos posibles, puede asegurar que cada entrada del cuadrado latino propuesto es Θ-forzada por cualquier otro par de entradas de órbitas diferentes. Por tanto:

$$\mathrm{scs}_\Theta(L_{5,1}) = \mathrm{lcs}_\Theta(L_{5,1}) = 2$$

$\triangleleft$

Ejemplo 4.6. (Falcón y cols., 2020) Consideremos el autotopismo $\Theta = ((345), (345), (345))$ para el cuadrado latino

$$L_{5,2} \equiv \begin{array}{|c|c|c|c|c|}\hline 1&2&3&4&5\\\hline 2&1&4&5&3\\\hline 3&4&5&1&2\\\hline 4&5&2&3&1\\\hline 5&3&1&2&4\\\hline\end{array}$$

Atendiendo a la fórmula descrita en (3.1), el número de órbitas asociadas a Θ es

$$\frac{1\cdot 2\cdot 1\cdot 2}{1} + \frac{1\cdot 2\cdot 3\cdot 1}{3} + \frac{3\cdot 1\cdot 1\cdot 2}{3} + \frac{3\cdot 1\cdot 3\cdot 1}{3} = 11.$$

Más concretamente, el conjunto de órbitas $\mathrm{Orb}_\Theta(L_{5,2})$ está formado por una órbita principal, dos órbitas paralelas monótonas por filas, dos órbitas paralelas monótonas por columnas, dos órbitas

paralelas monótonas por símbolos y cuatro órbitas triviales. Además, el autotopismo Θ mantiene los dos subcuadrados latinos parciales siguientes:

1	2			
2	1			

			1	2
		2		1
		1	2	

.

Luego, la Proposición 3.12 implica que cada Θ-conjunto crítico de $L_{5,2}$ contiene, al menos, una entrada de cada uno de los subcuadrados latinos parciales anteriores. Además, la Proposición 3.9 implica que dicho Θ-conjunto crítico también contiene una entrada de una órbita monótona por filas y una de una órbita monotona por columnas. A pesar de esto, estas cuatro entradas no constituyen un Θ-conjunto crítico para $L_{5,2}$ por sí solas. A modo de aclaración, los siguientes cuadrados latinos contienen a Θ en su correspondiente grupo de autotopismos. Destacamos en cada caso las órbitas comunes con $L_{5,2}$.

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

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

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

Un estudio sencillo de los casos posibles puede asegurar que cada Θ-conjunto crítico de $L_{5,2}$ es:

- Un cuadrado latino parcial de tamaño cinco que contiene exactamente una entrada de cada uno de los cinco tipos de órbitas; o bien
- Un cuadrado latino parcial de tamaño seis que contiene una órbita trivial, una entrada de un par de órbitas del mismo tipo, y cuatro entradas que procedan de órbitas secundarias de los dos tipos de órbitas secundarias restantes.

Por tanto:

$$\mathrm{scs}_{\Theta}(L_{5,2}) = 5 < 6 = \mathrm{lcs}_{\Theta}(L_{5,2}).$$

$\triangleleft$

Como hemos podido comprobar, en cada uno de los ejemplos anteriores se realiza un estudio matemático exhaustivo para conocer en torno a qué tamaño se sitúan los conjuntos críticos de un cuadrado latino dado uno de sus autotopismos. En nuestro caso, el estudio que se aporta será estadístico, llevando a cabo múltiples intentos con conjuntos de distinto tamaño para cada cuadrado latino y para cada uno de los atotopismo relativos a él.

4.2– Aportación realizada

4.2.1. Aportación al protocolo de compartición de secretos mediante cuadrados latinos

Como ya comentábamos anteriormente, la propuesta desarrollada está basada en el esquema de compartición de secretos descrito en (Cooper y cols., 1994). El verdadero potencial de este nuevo esquema se basa en el hecho de emplear cuadrados latinos de órdenes superiores a los ya estudiados pues el número de cuadrados latinos aumenta enormemente a medida que incrementamos el órden de estos, provocando que un ataque por fuerza bruta sea inviable para conocer la clave.

Los pasos a seguir que marca el nuevo protocolo desarrollado son los siguientes:

1. Dado un número l de participantes, se obtienen todos los posibles pares *representante - autotopismo*, donde *representante* hace referencia a un cuadrado latino L representante de una clase principal y *autotopismo* hace referencia a un autotopismo $\Theta \in Atop(L)$, que satisface que el tamaño de algún Θ-conjunto crítico $S \in Ent(L)$ es igual al número de participantes.

2. Una vez tenemos una lista formada por los pares mencionados anteriormente, tomaremos aquellos cuyo representante tenga mayor orden. En caso de existir más de una posibilidad, se tomará una nueva lista formada por los casos seleccionados y se elegirá uno aleatoriamente.

3. Conociendo el representante y el autotopismo que se usará, el siguiente paso es encontrar un Θ-conjunto crítico de L basándonos en el autotopismo Θ.

4. Después de conseguir el conjunto crítico, se debe generar aleatoriamente un isotopismo Θ_1 que será aplicado a L para conseguir un nuevo cuadrado latino L', equivalente a L y clave del esquema de compartición de secretos. De la misma manera, el isotopismo Θ_1 será aplicado al Θ-conjunto crítico calculado anteriormente para obtener las sombras que serán repartidas entre los participantes.

5. Por último, calculamos el autotopismo conjugado Θ' a partir del isotopismo generado aleatoriamente Θ_1, su inverso Θ^{-1} y el autototopismo inicial Θ. Más concretamente,

$$\Theta' \equiv \Theta'_1 * \Theta * \Theta^{-1}$$

   Mediante este nuevo autotopismo Θ' se podrá recuperar la clave L' a partir de las sombras repartidas a los participantes.

Ilustramos dicho esquema con un ejemplo.

Ejemplo 4.7. Tres amigos: Alicia, Almudena y Santiago, deciden comprar caramelos. Llegado un punto de la tarde, Santiago debe volver a casa, sin embargo aún quedan caramelos. Alicia y Almudena insisten en que los guardarán para la próxima vez que estén juntos pero Santiago, no fiándose de la palabra de ambas, les propone guardarlos en una caja fuerte especial que tiene su padre. Esta caja no revelaría la clave a ninguno de los tres, sino que les daría pequeñas subclaves a cada uno, de manera que, cuando volviesen a estar juntos, la caja se abriría. Reflejamos, entonces, el proceso que siguió la caja para llevar a cabo la compartición de la clave:

1. Conociendo que el número de participantes era tres, la caja decidió que el par representante-autotopismo seleccionado debía ser:

$$L_{5,1} \equiv \begin{array}{|c|c|c|c|c|}\hline 1 & 2 & 3 & 4 & 5 \\ \hline 2 & 3 & 4 & 5 & 1 \\ \hline 3 & 4 & 5 & 1 & 2 \\ \hline 4 & 5 & 1 & 2 & 3 \\ \hline 5 & 1 & 2 & 3 & 4 \\ \hline \end{array} \qquad \Theta \equiv ((2354), (1243), (1243))$$

2. Seguidamente calculó un Θ-conjunto crítico de tamaño 3 relativo al cuadrado latino y autotopismo generados:

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

3. Una vez la caja tenía el Θ-conjunto crítico, generó un isotopismo aleatorio:

$$\Theta_1 \equiv ((45213), (312), (54))$$

4. Aplicó el isotopismo aleatorio al representante $L_{5,1}$ y el Θ-conjunto crítico S_Θ, obteniendo así la clave L' y las sombras S'_Θ que repartió entre los tres amigos:

$$L' \equiv \begin{array}{|c|c|c|c|c|}\hline 3&2&4&5&1\\\hline 2&5&1&4&3\\\hline 4&1&2&3&5\\\hline 5&4&3&1&2\\\hline 1&3&5&2&4\\\hline\end{array} \qquad S'_\Theta \equiv \{(1,3,4),(1,4,5),(1,5,1)\}$$

5. Por último, la caja calculó Θ'como el autotopismo que aplicado a las sombras y completando forzosamente cuando sea necesario, da como resultado la clave:

$$\Theta' \equiv \Theta'_1 * \Theta * \Theta^{-1} \equiv ((1425),(1234),(1234))$$

$\lhd$

Llegados a este punto puede que al lector le aborde una pregunta: *¿Qué sucede si alguno de los participantes no se encuentra presente?*

En el esquema de compartición de secretos que se propone en (Cooper y cols., 1994) se solventa el problema planteado considerando varios conjuntos críticos que necesariamente contengan una o varias entradas en común. Las sombras repartidas en ese caso son los distintos elementos de los conjuntos críticos elegidos. De esta manera, no se necesita reunir a todos los participantes para recuperar el secreto, sino que ciertos conjuntos de participantes, integrados todos ellos en la estructura de acceso del esquema, son suficientes para llevar a cabo la tarea. Con este esquema lo que se permite es que existan varios grupos distintos de participantes (algunos comunes) que puedan reunirse para recuperar la clave, sin necesidad de reunirlos a todos. Nótese que no es posible recuperar la clave con cualquier conjunto (de un mínimo cardinal) de participantes reunidos.

La propuesta a presentar en este trabajo se podría hacer exactamente igual, simplemente considerando Θ-conjuntos críticos asociados al cuadrado latino y autotopismo correspondiente, en lugar de a conjuntos críticos (sin considerar simetría). Sin embargo, el sistema presentado aquí permite dar respuesta al problema planteado anteriormente sin necesidad de buscar distintos conjuntos críticos con entradas comunes, lo que simplificar la solución, sobre todo, pensando en órdenes superiores. Aunque en el sistema básico aquí propuesto requiere repartir tantas sombras como participantes haya, necesitándolos a todos para poder obtener la clave, existe una opción alternativa que consiste en considerar un esquema de compartición de secretos con sustitutos. En este caso, el conjunto de sombras consistiría en un Θ-conjunto crítico de tamaño estrictamente menor que el número de participantes, al que se le añadiría algún elemento más de las órbitas implicadas en dicho conjunto crítico. Los participantes que tengan elementos de una misma órbita podrían sustituirse entre sí. De esta manera existirían varios conjuntos válidos para la recuperación del secreto, similar al esquema que proponen en el artículo citado anteriormente, pero sin la necesidad de tener que buscar Θ-conjuntos críticos que compartan elementos. Veamos un ejemplo que aclare esta idea:

Ejemplo 4.8. Suponemos que, en un banco, existen cuatro empleados y un único director. Para abrir la caja fuerte se propone como requisito que siempre se encuentren dos empleados y el director, por lo que deciden dividir la clave de la caja mediante un esquema de compartición de secretos. Para ello, el sistema determina que se buscarán conjuntos críticos de tres entradas, una para el director y dos para dos de los empleados. Estos serán, entonces, los participantes. Los trabajadores restantes serán considerados sustitutos de los empleados participantes, por lo que se les asignarán entradas redundantes de las órbitas usadas con los otros empleados. Así:

1. Conociendo que el número de participantes era tres, el algoritmo decidió que el par representante-autotopismo seleccionado debía ser:

$$L_{5,2} \equiv \begin{array}{|c|c|c|c|c|}\hline 1&2&3&4&5\\\hline 2&1&4&5&3\\\hline 3&4&5&1&2\\\hline 4&5&2&3&1\\\hline 5&3&1&2&4\\\hline\end{array} \qquad \Theta \equiv ((13)(45),(25)(34),(13)(45))$$

2. Seguidamente calculó un Θ-conjunto crítico de tamaño 3 relativo al cuadrado latino y autotopismo generados:

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

3. Una vez la caja tenía el Θ-conjunto crítico, generó un isotopismo aleatorio:

$$\Theta_1 \equiv ((2435),(341),(51243))$$

4. Aplicó el isotopismo aleatorio al representante $L_{5,2}$ y el Θ-conjunto crítico S_Θ, obteniendo así la clave L' y las sombras S'_Θ que repartió entre los tres trabajadores:

$$L' \equiv \begin{array}{|c|c|c|c|c|}\hline 3&4&2&5&1\\\hline 4&5&1&2&3\\\hline 5&1&3&4&2\\\hline 1&2&4&3&5\\\hline 2&3&5&1&4\\\hline\end{array} \qquad S'_\Theta \equiv \{(1,1,3),(3,2,1),(3,1,5)\}$$

   Otorgó las sombras de la siguiente manera:

   - El director recibió la sombra (1,1,3).
   - El empleado 1 recibió la sombra (3,2,1).
   - El empleado 2 recibió la sombra (3,1,5).

   Además, para contemplar que hubiese sustitutos para los empleados 1 y 2, al resto de trabajadores se les entregaron las siguientes sombras:

   - El empleado 3 recibió la sombra (1,5,3), que sería sustituto del empleado 1.
   - El empleado 4 recibió la sombra (1,1,4), que sería sustituto del empleado 2.

5. Por último, la caja calculó Θ'como el autotopismo conjugado de Θ que, aplicado a las sombras y completando forzosamente cuando sea necesario, da como resultado la clave. Esto es,

$$\Theta' \equiv \Theta'_1 * \Theta * \Theta^{-1} \equiv ((15)(23),(14)(25),(13)(25))$$

   De esta manera, las estructuras de acceso serían:

   - Director + empleado 1 + empleado 2.
   - Director + empleado 1 + empleado 4.
   - Director + empleado 2 + empleado 3.
   - Director + empleado 3 + empleado 4.

◁

Por otro lado, en el esquema propuesto en (Cooper y cols., 1994) se incluye una modificación para adaptarlo a un sistema multinivel. Para ello se consideran varios conjuntos críticos de distinto tamaño tales que compartan algunos elementos. Los elementos comunes serían considerados sombras de mayor jerarquía, puesto que en el caso de reunirse los participantes de estos elementos se necesitarían menos sombras (de menor jerarquía) para completar el secreto.

El esquema básico de compartición de secretos que se presenta en este trabajo puede ser considerado un esquema rudimentario multinivel si se consideran casos en los que los tamaños de las órbitas correspondientes a las sombras seleccionadas son diferentes, ya que aquellos participantes cuya sombra derive en una órbita más larga tienen más información del secreto que aquellos que presenten órbitas menores, y por tanto, podrían ser considerados de una jerarquía superior. En este sentido, se puede tomar como ejemplo el cuadrado latino representante $L_{5,2}$ y el autotopismo $\Theta \equiv ((345), (345), (345))$ en el que se obtienen cuatro órbitas con tres entradas cada una y una órbita con una única entrada. Las órbitas con mayor número de entradas podrían ser asignadas a un orden superior, mientras que la órbita trivial pertenecería a un orden inferior.

En la mayor parte de los ejemplos obtenidos en estos primeros órdenes de cuadrados latinos empleados, los Θ-conjuntos críticos están formados por órbitas de igual tamaño, por lo que en la mayoría de los ejemplos que se pueden crear en estos órdenes bajos serían esquemas mononivel.

En este sentido, sería interesante realizar un estudio para conocer si en órdenes superiores de cuadrados latinos existen otros ejemplos que nos brinden otras posibilidades para este caso.

Otra opción para transformar el sistema propuesto aquí en un esquema multinivel, más en la línea propuesta en (Cooper y cols., 1994), sería crear las sombras de tamaños diferentes, de modo que las órbitas no triviales produzcan distintas sombras para tener sustitutos. Y dejar algunas órbitas (podrían ser triviales o no) que sólo den lugar a una sombra. Estas últimas sombras harían irreempazables a los participantes que las tuviesen asignadas (que serían los de mayor jerarquía), mientras que las otras serían asociadas a personas de menor jerarquía, puesto que podrían ser reemplazados por otros participantes que tuvieran en su poder elementos de la misma órbita. Con esta propuesta también se evitaría tener que buscar distintos conjuntos críticos para un mismo cuadrado que, además, según el esquema de (Cooper y cols., 1994), tendrían que compartir entradas, tarea complicada en el caso de órdenes superiores.

Cabe destacar que este algoritmo es aplicable a cualquier tamaño de conjunto de participantes, siempre y cuando se conozcan conjuntos críticos de dicho tamaño para algún orden de cuadrados latinos.

4.2.2. Aportación al estudio del tamaño de los conjuntos críticos basados en autotopismos no triviales de cuadrados latinos

Hasta el momento se conoce la clasificación de tamaños de conjuntos críticos basados en autotopismos de cuadrados latinos de hasta orden cinco gracias al artículo (Falcón y cols., 2020). En esta sección se pretende llevar a cabo un estudio estadístico sobre el tamaño de conjuntos críticos basados en autotopismos de cuadrados latinos de orden superior a cinco, concretamente de orden 6 (aunque se puede ampliar al resto de órdenes). Para ello, realizaremos una división bipartita del contenido de la sección. En la primera parte se demostrará, a partir de los ejemplos expuestos en la Sección 4.1.2, que el algoritmo empleado para el estudio estadístico funciona correctamente, comparando las salidas del mismo con los resultados expuestos en el artículo . En cuanto a la segunda parte, llevaremos a cabo análisis estadísticos sobre el tamaño de los conjuntos críticos de las distintas clases principales de cuadrados latinos de orden seis.

El algoritmo desarrollado presenta el siguiente funcionamiento. Dado un cuadrado latino L y un autotopismo Θ relativo al mismo:

1. Se hallan las Θ-órbitas de L.

2. Se itera sobre los distintos posibles valores para el tamaño de cada conjunto crítico. Estos valores irán desde el mínimo, en este caso 1, y el máximo, que por la Proposición 3.8 conocemos que es el número de órbitas, aunque podríamos reducir dicho valor en una unidad, pues la última órbita podría obtenerse de manera forzada a partir de las anteriores.

3. Para cada tamaño de conjunto n, el algoritmo tomará todas las combinaciones de n órbitas y formará un conjunto C a partir de una de las combinaciones tomada aleatoriamente. Para ello seleccionará el primer elemento de cada órbita. Recordamos que en la Sección 3.2.6 se veía que si se aplicaba un isotopismo Θ sobre un elemento cualquiera de la Θ-órbita, podíamos obtener todas las entradas incluidas en ella.

4. Una vez se tiene el conjunto C se comprueba si el cuadrado latino parcial P formado por las entradas de C es únicamente completable a L. En caso de serlo, se realiza la misma comprobación para todos los subconjuntos que podemos formar con $n-1$ elementos de C. Si alguno de los cuadrados latinos parciales formados por los subconjuntos mencionados devuelve que es únicamente completable a L, entonces C no será un Θ-conjunto crítico de L. En caso contrario, C se contemplará como un Θ-conjunto crítico de L.

5. Para cada tamaño de conjunto, el proceso se repite un número de veces determinado (actualmente mil veces), de tal manera que, cada vez que el algoritmo encuentre un Θ-conjunto crítico de L de dicho tamaño, anotará un acierto. En caso contrario, anotará un fallo.

Comprobación de la bondad del algoritmo

- Caso 1 (Ejemplo 4.1): El par representante - atotopismo usado es:

$$L_2 \equiv \begin{array}{|c|c|}\hline 1 & 2 \\ \hline 2 & 1 \\ \hline \end{array} \qquad \Theta = ((12), (12), \mathrm{Id}_2)$$

Para este caso, el artículo expone que los conjuntos críticos tienen tamaño 1. Comprobamos este hecho con el algoritmo desarrollado:

```
graficaEstudioEstadístico(representante_L2,autotopismos_L2[1])
```

```
Con el tamaño:  1 , hay:  1000  aciertos.
Con el tamaño:  2 , hay:  0  aciertos.
```

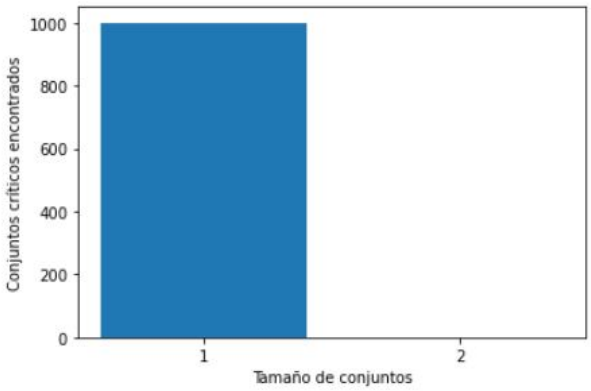


Figura 4.1: Estudio estadístico Ejemplo 4.1 (Fuente: Elaboración propia)

Podemos comprobar que los resultados obtenidos coinciden con los expuestos en el Ejemplo 4.1. Además observamos que se produce un 100 % de aciertos en todas las ejecuciones que ha llevado a cabo el algoritmo. Realmente, con cuatro casillas, dar un único valor deja determinado el cuadrado, por eso es lógico que todas las iteraciones con tamaño uno hayan obtenido aciertos.

- Caso 2 (Ejemplo 4.2): El par representante - atotopismo usado es:

$$L_3 \equiv \begin{array}{|c|c|c|}\hline 1 & 2 & 3 \\ \hline 2 & 3 & 1 \\ \hline 3 & 1 & 2 \\ \hline \end{array} \qquad \Theta = ((123), (132), \mathrm{Id}_3)$$

Para este caso, el artículo expone que los conjuntos críticos tienen tamaño 2. Comprobamos este hecho con el algoritmo desarrollado:

```
graficaEstudioEstadístico(representante_L3,autotopismos_L3[2])
```

```
Con el tamaño:  1 , hay:  0  aciertos.
Con el tamaño:  2 , hay:  1000  aciertos.
Con el tamaño:  3 , hay:  0  aciertos.
```

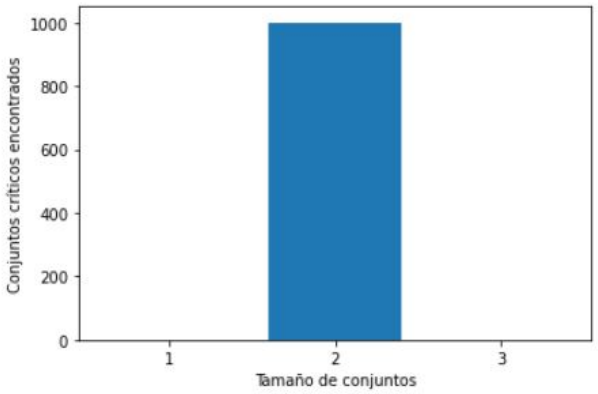


Figura 4.2: Estudio estadístico Ejemplo 4.2 (Fuente: Elaboración propia)

Estadísticamente volvemos a recuperar el resultado esperado según el Ejemplo 4.2. Para este caso volvemos a tener un 100 % de éxitos en cada iteración. Esto se debe a que las tres $\Theta-$órbitas del cuadrado son principales y, por tanto, conociendo un elemento de dos de ellas, se puede comprobar fácilmente que se recupera el cuadrado.

- Caso 3 (Ejemplo 4.3): El par representante - atotopismo usado es:

$$L_{4,1} \equiv \begin{array}{|c|c|c|c|}\hline 1 & 2 & 3 & 4 \\ \hline 2 & 1 & 4 & 3 \\ \hline 3 & 4 & 1 & 2 \\ \hline 4 & 3 & 2 & 1 \\ \hline \end{array} \qquad \Theta = ((1234), (1234), (24))$$

Para este caso, el artículo expone que los conjuntos críticos tienen tamaño 2. Comprobamos este hecho con el algoritmo desarrollado:

```
graficaEstudioEstadístico(representante_L41,autotopismos_L41[5])
```

```
Con el tamaño:  1 , hay:  0  aciertos.
Con el tamaño:  2 , hay:  639  aciertos.
Con el tamaño:  3 , hay:  0  aciertos.
Con el tamaño:  4 , hay:  0  aciertos.
```

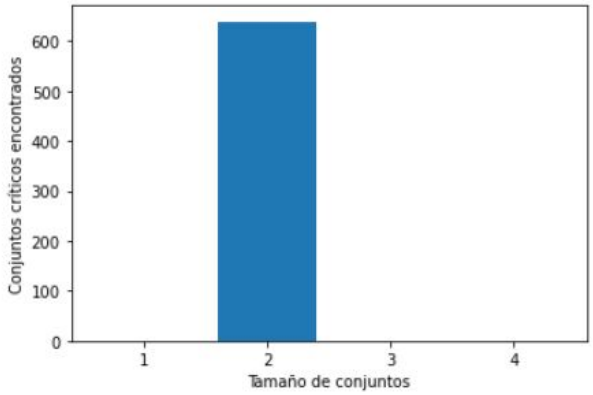


Figura 4.3: Estudio estadístico Ejemplo 4.3 (Fuente: Elaboración propia)

De nuevo, podemos observar que los resultados recogidos en el estudio estadístico reflejan los obtenidos en el Ejemplo 4.3. En este caso, podemos comprobar que el índice de acierto es del 63.9 %, es decir, por cada cien combinaciones de conjuntos de tamaño dos probados, en torno a sesenta y cuatro son clasificados como conjuntos críticos. Esto se debe a que se escogen órbitas al azar y, en muchas ocasiones, el conjunto formado no es conjunto crítico.

- Caso 4 (Ejemplo 4.4): El par representante - atotopismo usado es:

$$L_{4,2} \equiv \begin{array}{|c|c|c|c|}\hline 1 & 2 & 3 & 4 \\ \hline 2 & 1 & 4 & 3 \\ \hline 3 & 4 & 2 & 1 \\ \hline 4 & 3 & 1 & 2 \\ \hline \end{array} \qquad \Theta = ((1324), (1324), (12)(34))$$

Para este caso, el artículo expone que los conjuntos críticos tienen tamaño 2. Comprobamos este hecho con el algoritmo desarrollado:

```
graficaEstudioEstadístico(representante_L42,autotopismos_L42[4])
```

```
Con el tamaño:  1 , hay:  0  aciertos.
Con el tamaño:  2 , hay:  665  aciertos.
Con el tamaño:  3 , hay:  0  aciertos.
Con el tamaño:  4 , hay:  0  aciertos.
```

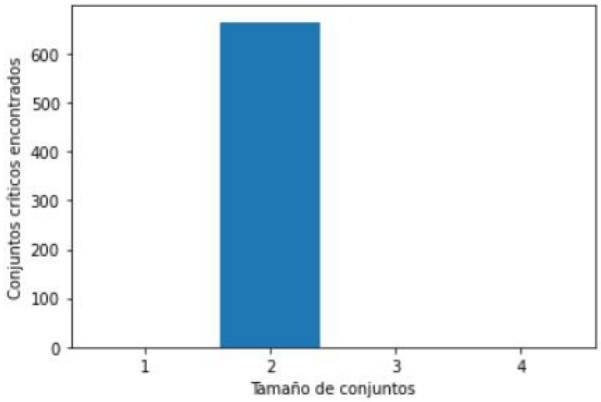


Figura 4.4: Estudio estadístico Ejemplo 4.4 (Fuente: Elaboración propia)

Podemos observar que el estudio realizado obtiene los mismos resultados que el Ejemplo 4.4. Al igual que en el ejemplo anterior, se obtienen menos aciertos que el número total de ejecuciones debido a que, como se ha mencionado antes, se escogen órbitas al azar y, en muchas ocasiones, el conjunto formado no es conjunto crítico.

- Caso 5 (Ejemplo 4.5) : El par representante - atotopismo usado es:

$$L_{5,1} \equiv \begin{array}{|c|c|c|c|c|}\hline 1&2&3&4&5\\\hline 2&3&4&5&1\\\hline 3&4&5&1&2\\\hline 4&5&1&2&3\\\hline 5&1&2&3&4\\\hline\end{array} \qquad \Theta = ((12345), (12345), (13524))$$

Para este caso, el artículo expone que los conjuntos críticos tienen tamaño 2. Comprobamos este hecho con el algoritmo desarrollado:

```
graficaEstudioEstadístico(representante_L51,autotopismos_L51[4])
```

```
Con el tamaño:  1 , hay:  0  aciertos.
Con el tamaño:  2 , hay:  1000  aciertos.
Con el tamaño:  3 , hay:  0  aciertos.
Con el tamaño:  4 , hay:  0  aciertos.
Con el tamaño:  5 , hay:  0  aciertos.
```

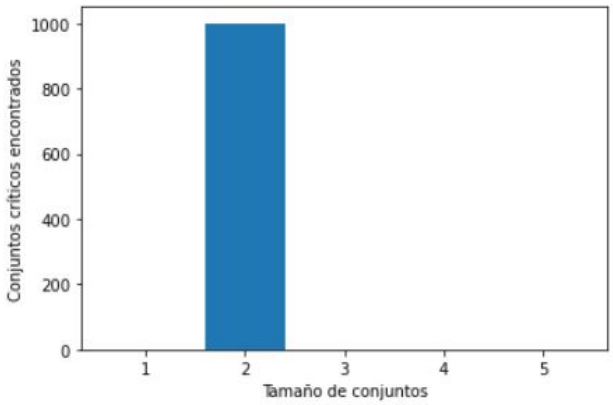


Figura 4.5: Estudio estadístico Ejemplo 4.5 (Fuente: Elaboración propia)

Además de observar que se obtienen los resultados esperados por el Ejemplo 4.5, se puede comprobar que se obtiene un 100 % de aciertos en las iteraciones realizadas. Esto se debe a que el autotopismo usado genera órbitas con un gran número de entradas y, por tanto, con tan solo dos entradas relativas a dichas Θ-órbitas podría comprobarse fácilmente que el cuadrado es únicamente completable.

- Caso 6 (Ejemplo 4.6): El par representante - atotopismo usado es:

$$L_{5,2} \equiv \begin{array}{|c|c|c|c|c|}\hline 1&2&3&4&5\\\hline 2&1&4&5&3\\\hline 3&4&5&1&2\\\hline 4&5&2&3&1\\\hline 5&3&1&2&4\\\hline\end{array} \qquad \Theta = ((345),(345),(345))$$

Para este caso, el artículo expone que los conjuntos críticos presentan un tamaño entre 5 y 6. Comprobamos este hecho con el algoritmo desarrollado:

```
graficaEstudioEstadístico(representante_L52,autotopismos_L52[2])
```

```
Con el tamaño:  1 , hay:  0  aciertos.
Con el tamaño:  2 , hay:  0  aciertos.
Con el tamaño:  3 , hay:  0  aciertos.
Con el tamaño:  4 , hay:  0  aciertos.
Con el tamaño:  5 , hay:  126  aciertos.
Con el tamaño:  6 , hay:  0  aciertos.
Con el tamaño:  7 , hay:  0  aciertos.
Con el tamaño:  8 , hay:  0  aciertos.
Con el tamaño:  9 , hay:  0  aciertos.
Con el tamaño:  10 , hay:  0  aciertos.
Con el tamaño:  11 , hay:  0  aciertos.
```

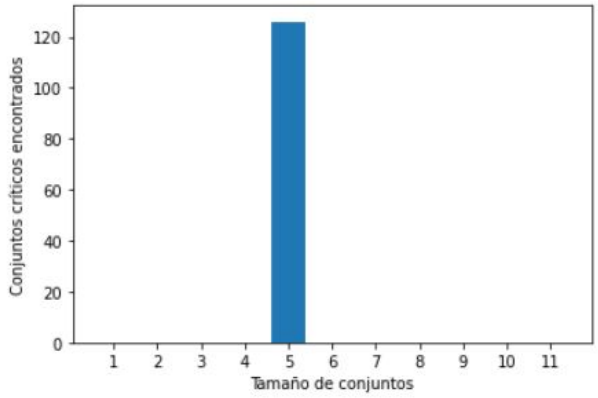


Figura 4.6: Estudio estadístico Ejemplo 4.6 (Fuente: Elaboración propia)

Podemos comprobar que se recogen conjuntos críticos de tamaño cinco pero no de tamaño seis. Tras comentarlo con ambos tutores del TFG, se ha llegado a la conclusión de que el artículo presenta un error, pues no existen conjuntos críticos de tamaño seis para la combinación representante - autotopismo establecida. Este hecho puede ser demostrado mediante un estudio de casos que trasciende los objetivos de este trabajo. De cualquier manera, destaca el hecho de que el algoritmo propuesto ha sido capaz de detectar dicho error.

Comprobación de la bondad del algoritmo (BIS). Cuadrados latinos de orden 5

En esta subsección se comprobará de manera mas exahustiva la bondad del algoritmo usado, aplicándolo a todos los casos de cuadrados latinos de orden cinco y sus respectivos autotopismos. Se recuerda que los tamaños de conjunto crítico para cada par representante - autotopismo pueden ser consultados en el Cuadro 3.2. Cabe destacar que, por economía del espacio, aquellos tamaños para los que no se obtengan conjuntos críticos, no aparecerán en la imagen (sí en la gráfica). Así:

Caso 1: Suponemos el cuadrado latino $L_{5,1}$:

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

Se realiza el estudio estadístico con cada uno de sus autotopismos:

1. Sea $\Theta_1 \equiv ((12)(35), (13)(45), (14)(23))$:

```
graficaEstudioEstadístico(representante_L51,autotopismos_L51[1])
```

```
Con el tamaño:  3  , hay:  6  aciertos.
Con el tamaño:  4  , hay:  47  aciertos.
Con el tamaño:  5  , hay:  59  aciertos.
```

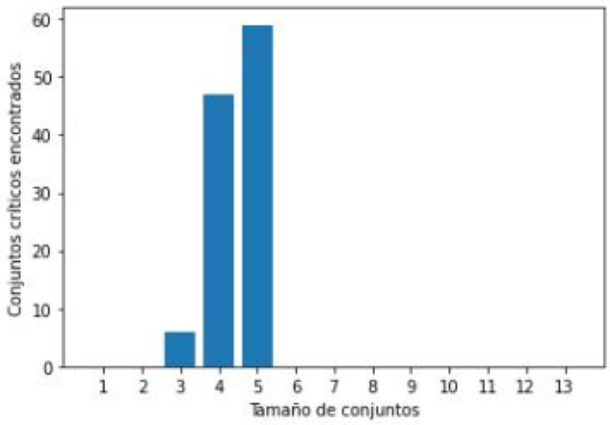


Figura 4.7: Estudio estadístico de $L_{5,1}$ y Θ_1 (Fuente: Elaboración propia)

2. Sea $\Theta_2 \equiv ((2354), (1243), (1243))$:

```
graficaEstudioEstadístico(representante_L51,autotopismos_L51[2])
```

```
Con el tamaño:  3  , hay:  460  aciertos.
```

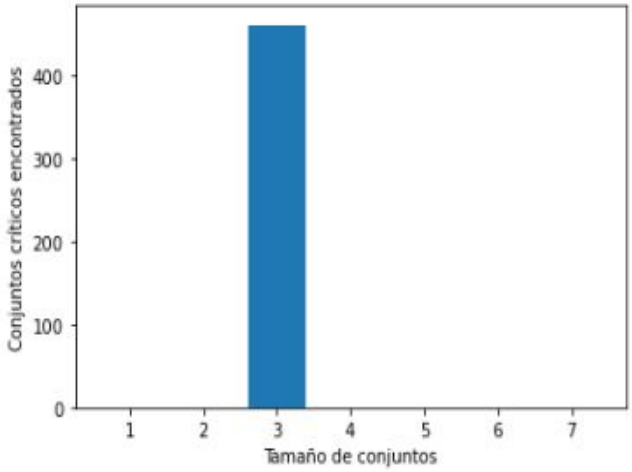


Figura 4.8: Estudio estadístico $L_{5,1}$ y Θ_2 (Fuente: Elaboración propia)

3. Sea $\Theta_3 \equiv ((12345), (15432), Id_5)$:

```
graficaEstudioEstadístico(representante_L51,autotopismos_L51[3])
```

```
Con el tamaño:  4  , hay:  1000  aciertos.
```

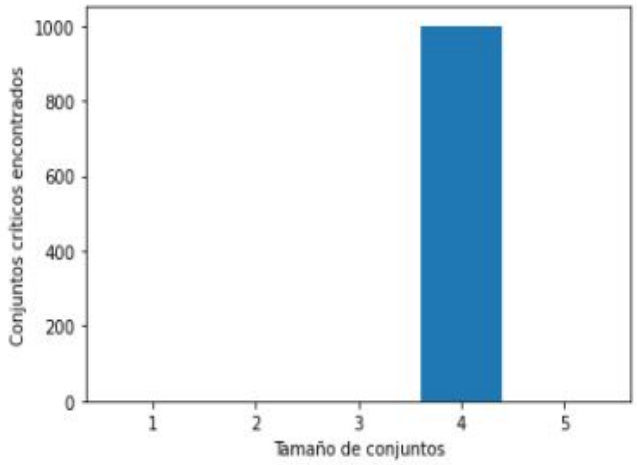


Figura 4.9: Estudio estadístico $L_{5,1}$ y Θ_3 (Fuente: Elaboración propia)

4. Sea $\Theta_4 \equiv ((12345), (12345), (13524))$: Consultar caso 5 en el punto 4.2.2.

Caso 2: Suponemos el cuadrado latino $L_{5,2}$:

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

Se realiza el estudio estadístico con cada uno de sus autotopismos:

1. Sea $\Theta_1 \equiv ((13)(45), (25)(34), (13)(45))$:

```
graficaEstudioEstadístico(representante_L52,autotopismos_L52[1])
```

```
Con el tamaño:  3  , hay:  12  aciertos.
Con el tamaño:  4  , hay:  64  aciertos.
Con el tamaño:  5  , hay:  51  aciertos.
```

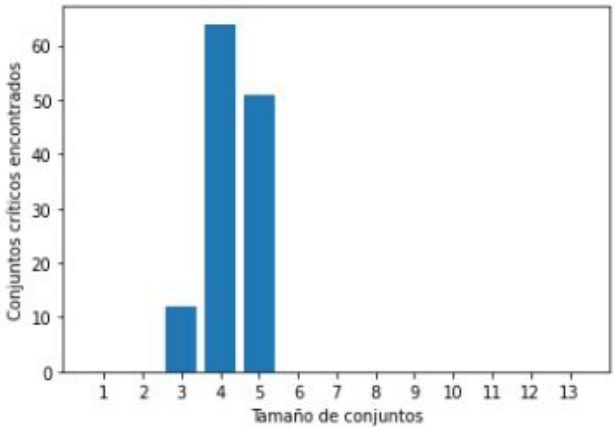


Figura 4.10: Estudio estadístico $L_{5,2}$ y Θ_1 (Fuente: Elaboración propia)

2. Sea $\Theta_2 \equiv ((345), (345), (345))$: Consultar caso 6 en el punto 4.2.2.

Como se puede observar, los resultados obtenidos siguen los datos recogidos en el Cuadro 3.2, hecho que nos confirma que el algoritmo funciona correctamente y, por tanto, sería recomendable realizar el estudio estadístico con cuadrados de orden superior a los ya estudiados, con el objetivo de que puedan ser aplicados al algoritmo de compartición de secretos desarrollado anteriormente.

Aplicación del algoritmo a cuadrados latinos de orden superior a cinco

Como hemos podido observar a lo largo de esta sección, las ejecuciones del algoritmo diseñado para cuadrados latinos de orden cinco siguen fielmente los resultados obtenidos en el artículo (Falcón y cols., 2020) e incluso han detectado un error en dicho artículo. Sería entonces conveniente aplicar este algoritmo a ejemplos de cuadrados latinos de orden superior pues el verdadero potencial del esquema de compartición de secretos que se ha desarrollado en la sección anterior se basa en el uso de cuadrados latinos de órdenes superiores a los ya estudiados. Esto se debe a que el número de cuadrados latinos crece exponencialmente a medida que incrementamos el orden de estos, haciendo de un ataque por fuerza bruta algo impensable (ver Cuadro 3.1). Concretamente, el estudio estadístico se centrará en cuadrados latinos de orden seis. Así:

Caso 1: Suponemos el cuadrado latino $L_{6,1}$:

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

Se realiza el estudio estadístico con cada uno de sus autotopismos:

1. Sea $\Theta_1 \equiv ((36)(45), (36)(45), (36)(45))$:

```
graficaEstudioEstadístico(representante_L61,autotopismos_L61[1])
```

```
Con el tamaño:  7 , hay:  2  aciertos.
Con el tamaño:  8 , hay:  5  aciertos.
Con el tamaño:  9 , hay:  4  aciertos.
```

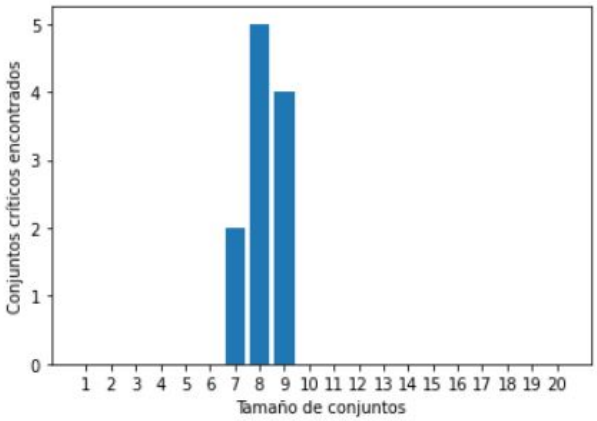


Figura 4.11: Estudio estadístico $L_{6,1}$ y Θ_1 (Fuente: Elaboración propia)

2. Sea $\Theta_2 \equiv ((12)(35)(46), (12)(34)(56), \mathrm{Id}_6)$:

```
graficaEstudioEstadístico(representante_L61,autotopismos_L61[2])
```

```
Con el tamaño:  9 , hay:  3  aciertos.
Con el tamaño:  10 , hay:  6  aciertos.
```

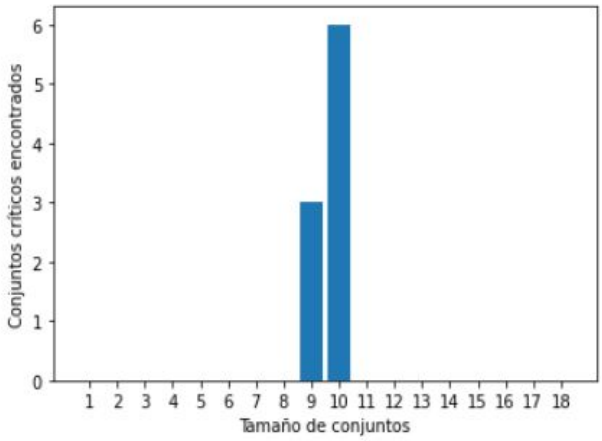


Figura 4.12: Estudio estadistico $L_{6,1}$ y Θ_2 (Fuente: Elaboración propia)

3. Sea $\Theta_3 \equiv ((12)(34)(56), (12)(35)(46), (36)(45))$:

```
graficaEstudioEstadístico(representante_L61,autotopismos_L61[3])
```

```
Con el tamaño:  7 , hay:  16  aciertos.
Con el tamaño:  8 , hay:  5  aciertos.
```

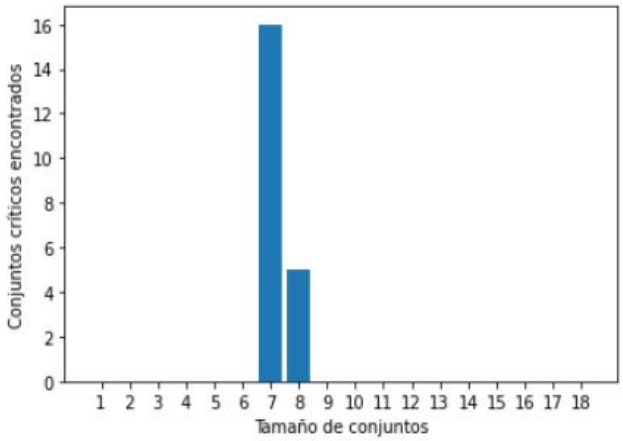


Figura 4.13: Estudio estadístico $L_{6,1}$ y Θ_3 (Fuente: Elaboración propia)

Caso 2: Suponemos el cuadrado latino $L_{6,2}$:

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

Se realiza el estudio estadístico con cada uno de sus autotopismos:

1. Sea $\Theta_1 \equiv ((23)(45), (23)(45), (23)(45))$:

```
graficaEstudioEstadístico(representante_L62,autotopismos_L62[1])
```

```
Con el tamaño:  7  , hay:  1  aciertos.
Con el tamaño:  8  , hay:  3  aciertos.
Con el tamaño:  9  , hay:  10  aciertos.
```

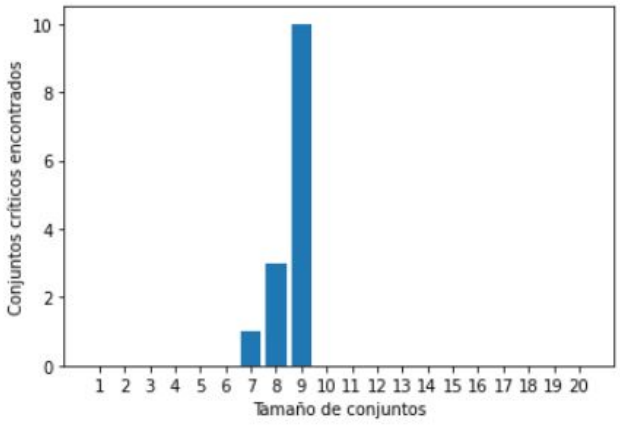


Figura 4.14: Estudio estadístico $L_{6,2}$ y Θ_1 (Fuente: Elaboración propia)

2. Sea $\Theta_2 \equiv ((14)(25)(36), (14)(26)(35), \mathrm{Id}_6)$:

```
graficaEstudioEstadístico(representante_L62,autotopismos_L62[2])
```

```
Con el tamaño:  9  , hay:  2  aciertos.
Con el tamaño:  10  , hay:  5  aciertos.
```

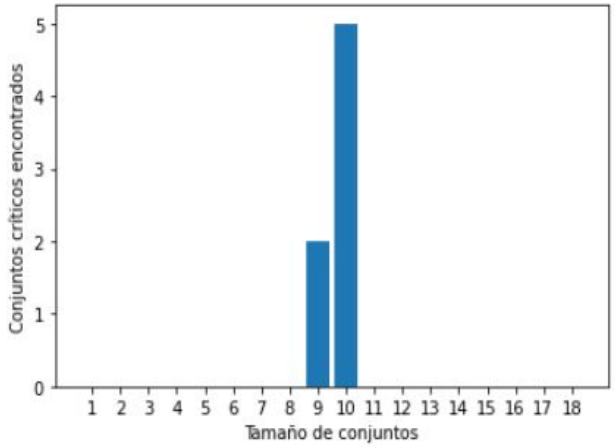


Figura 4.15: Estudio estadístico $L_{6,2}$ y Θ_2 (Fuente: Elaboración propia)

3. Sea $\Theta_3 \equiv ((14)(26)(35), (14)(25)(36), (23)(56))$:

```
graficaEstudioEstadístico(representante_L62,autotopismos_L62[3])
```

```
Con el tamaño:  7  , hay:  9  aciertos.
Con el tamaño:  8  , hay:  14  aciertos.
```

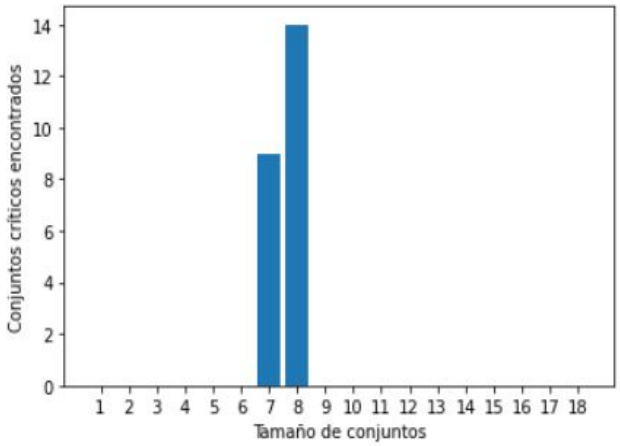


Figura 4.16: Estudio estadístico $L_{6,2}$ y Θ_3 (Fuente: Elaboración propia)

4. Sea $\Theta_4 \equiv ((456),(456),(456))$:

```
graficaEstudioEstadístico(representante_L62,autotopismos_L62[4])
```

```
Con el tamaño:  8  , hay:  6  aciertos.
Con el tamaño:  9  , hay:  8  aciertos.
```

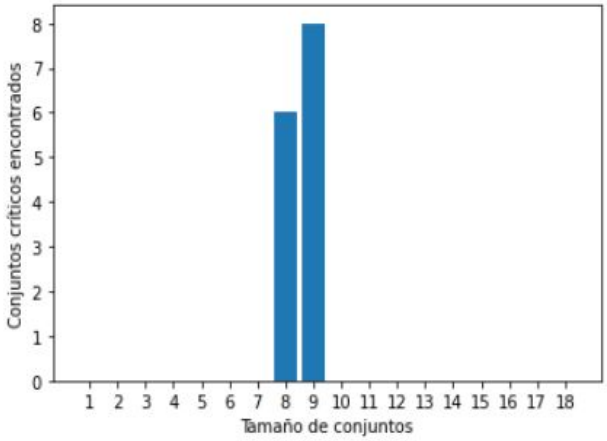


Figura 4.17: Estudio estadístico $L_{6,2}$ y Θ_4 (Fuente: Elaboración propia)

5. Sea $\Theta_5 \equiv ((123)(456), (15)(26)(34), (163524))$:

```
graficaEstudioEstadístico(representante_L62,autotopismos_L62[5])
```

```
Con el tamaño:  4  , hay:  396  aciertos.
```

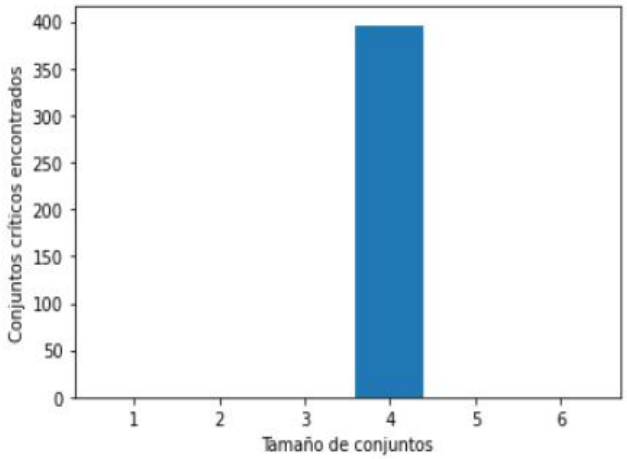


Figura 4.18: Estudio estadístico $L_{6,2}$ y Θ_5 (Fuente: Elaboración propia)

6. Sea $\Theta_6 \equiv ((132)(456), (123)(456), Id)$:

```
graficaEstudioEstadístico(representante_L62,autotopismos_L62[6])
```

```
Con el tamaño:  8  , hay:  145  aciertos.
```

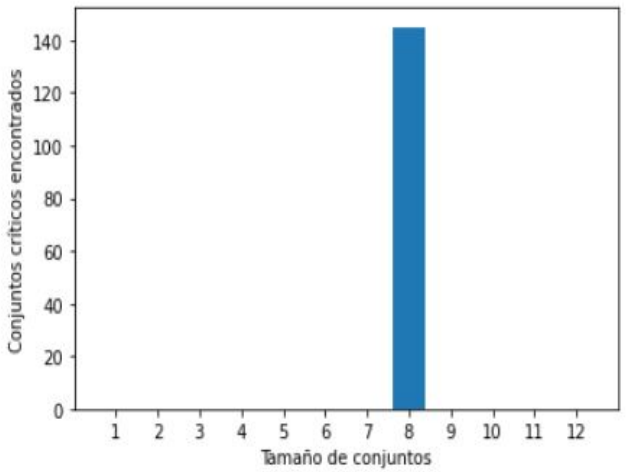


Figura 4.19: Estudio estadístico $L_{6,2}$ y Θ_6 (Fuente: Elaboración propia)

7. Sea $\Theta_7 \equiv ((123)(456), (132)(456), (465))$:

```
graficaEstudioEstadístico(representante_L62,autotopismos_L62[7])
```

```
Con el tamaño:  6  , hay:  53  aciertos.
Con el tamaño:  7  , hay:  21  aciertos.
```

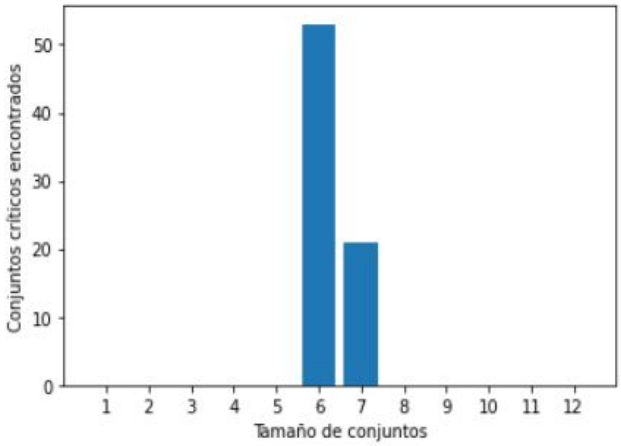


Figura 4.20: Estudio estadístico $L_{6,2}$ y Θ_7 (Fuente: Elaboración propia)

8. Sea $\Theta_8 \equiv ((142635), (153426), (13)(46))$:

```
graficaEstudioEstadístico(representante_L62,autotopismos_L62[8])
```

```
Con el tamaño:  4  , hay:  530  aciertos.
```

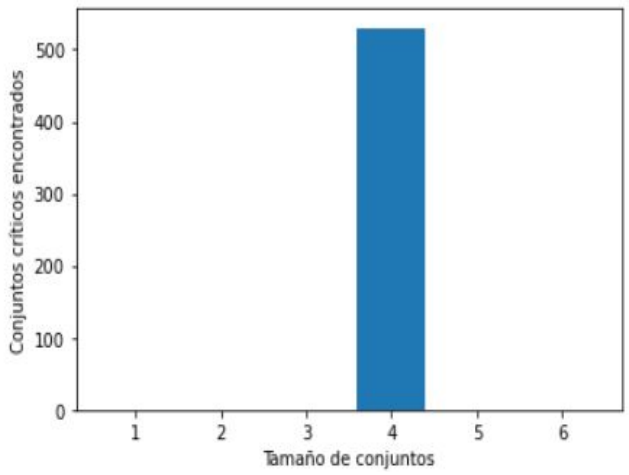


Figura 4.21: Estudio estadístico $L_{6,2}$ y Θ_8 (Fuente: Elaboración propia)

9. Sea $\Theta_9 \equiv ((142536), (143526), (456))$:

```
graficaEstudioEstadístico(representante_L62,autotopismos_L62[9])
```

```
Con el tamaño:  3  , hay:  164  aciertos.
```

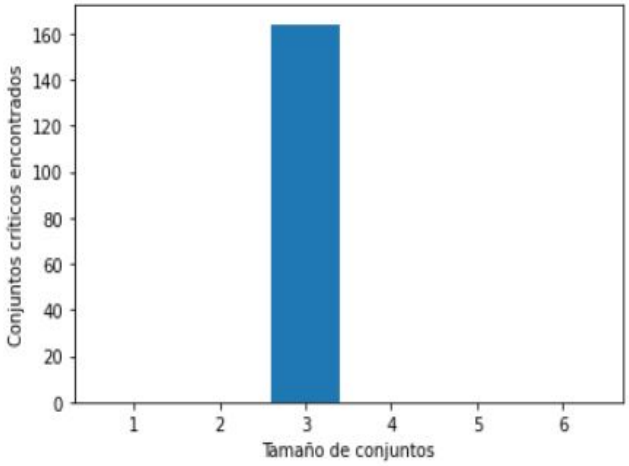


Figura 4.22: Estudio estadístico $L_{6,2}$ y Θ_9 (Fuente: Elaboración propia)

Caso 3: Suponemos el cuadrado latino $L_{6,3}$:

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

Se realiza el estudio estadístico con cada uno de sus autotopismos:

1. Sea $\Theta_1 \equiv ((456),(123),(123))$:

```
graficaEstudioEstadístico(representante_L63,autotopismos_L63[1])
```

```
Con el tamaño:  8  , hay:  3  aciertos.
Con el tamaño:  9  , hay:  9  aciertos.
```

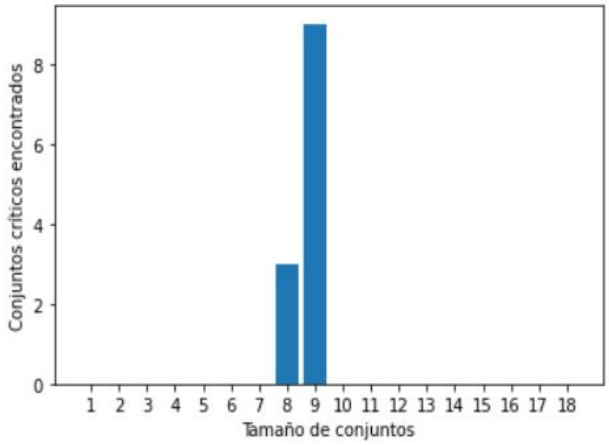


Figura 4.23: Estudio estadístico $L_{6,3}$ y Θ_1 (Fuente: Elaboración propia)

2. Sea $\Theta_2 \equiv ((14)(26)(35), (15)(26)(34), (12)(45))$:

```
graficaEstudioEstadístico(representante_L63,autotopismos_L63[2])
```

```
Con el tamaño:  6  , hay:  35  aciertos.
Con el tamaño:  7  , hay:  61  aciertos.
Con el tamaño:  8  , hay:  3  aciertos.
```

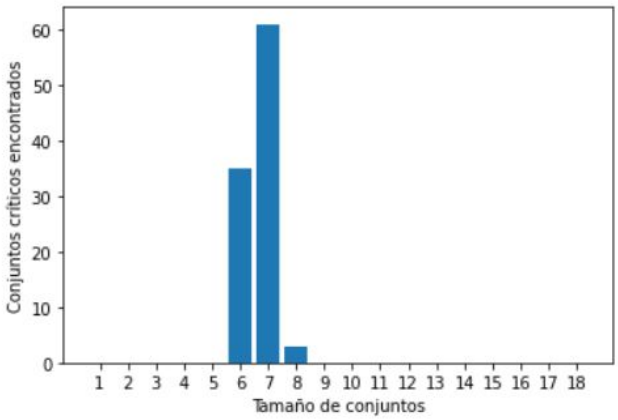


Figura 4.24: Estudio estadístico $L_{6,3}$ y Θ_2 (Fuente: Elaboración propia)

3. Sea $\Theta_3 \equiv ((123)(465), (132)(465), \mathrm{Id}_6)$:

```
graficaEstudioEstadístico(representante_L63,autotopismos_L63[3])
```

```
Con el tamaño:  8  , hay:  301  aciertos.
```

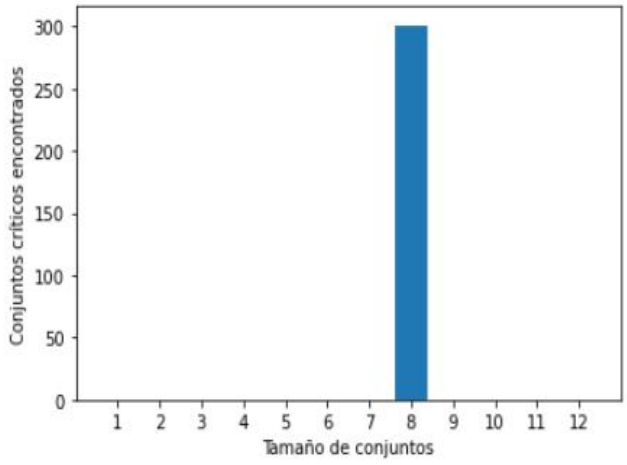


Figura 4.25: Estudio estadístico $L_{6,3}$ y Θ_3 (Fuente: Elaboración propia)

4. Sea $\Theta_4 \equiv ((123)(456), (123)(465), (132))$:

```
graficaEstudioEstadístico(representante_L63,autotopismos_L63[4])
```

```
Con el tamaño:  6  , hay:  157  aciertos.
```

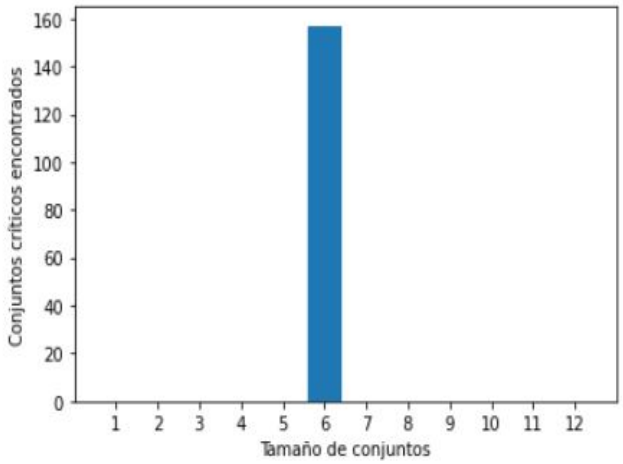


Figura 4.26: Estudio estadístico $L_{6,3}$ y Θ_4 (Fuente: Elaboración propia)

5. Sea $\Theta_5 \equiv ((153624), (152634), (13)(45))$:

```
graficaEstudioEstadístico(representante_L63,autotopismos_L63[5])
```

```
Con el tamaño:  4  , hay:  526  aciertos.
```

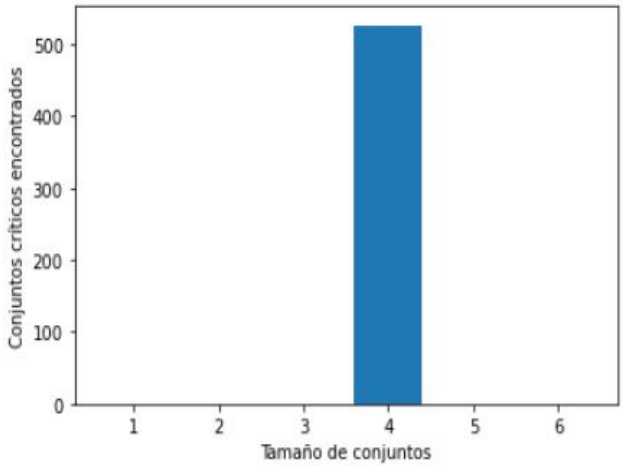


Figura 4.27: Estudio estadístico $L_{6,3}$ y Θ_5 (Fuente: Elaboración propia)

Caso 4: Suponemos el cuadrado latino $L_{6,4}$:

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

Se realiza el estudio estadístico con cada uno de sus autotopismos:

1. Sea $\Theta_1 \equiv ((23)(45)(23)(45)(23)(45))$:

```
graficaEstudioEstadístico(representante_L64,autotopismos_L64[1])
```

```
Con el tamaño:  7  , hay:  3  aciertos.
Con el tamaño:  8  , hay:  5  aciertos.
Con el tamaño:  9  , hay:  1  aciertos.
```

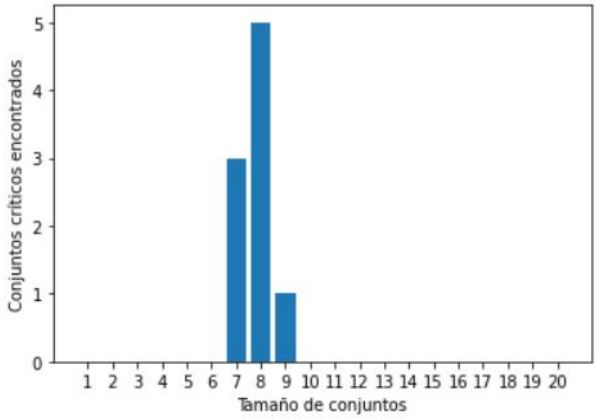


Figura 4.28: Estudio estadístico $L_{6,4}$ y Θ_1 (Fuente: Elaboración propia)

2. Sea $\Theta_2 \equiv ((16)(25)(34), (16)(25)(34), \mathrm{Id}_6)$:

```
graficaEstudioEstadístico(representante_L64,autotopismos_L64[2])
```

```
Con el tamaño:  9  , hay:  5  aciertos.
Con el tamaño:  10  , hay:  4  aciertos.
```

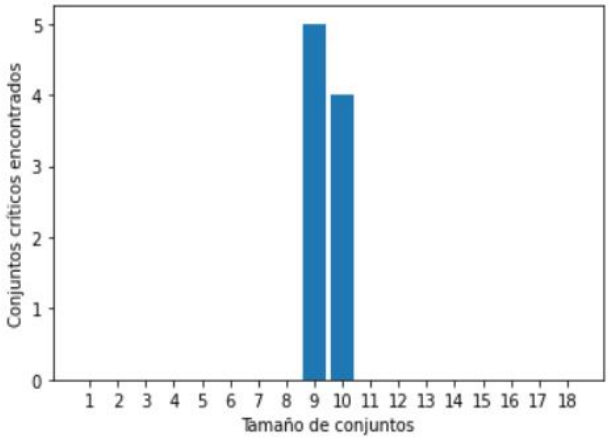


Figura 4.29: Estudio estadístico $L_{6,4}$ y Θ_2 (Fuente: Elaboración propia)

3. Sea $\Theta_3 \equiv ((14)(25)(36), (15)(26)(34), (23)(45))$:

```
graficaEstudioEstadístico(representante_L64,autotopismos_L64[3])
```

```
Con el tamaño:  6  , hay:  12  aciertos.
Con el tamaño:  7  , hay:  48  aciertos.
Con el tamaño:  8  , hay:  5  aciertos.
```

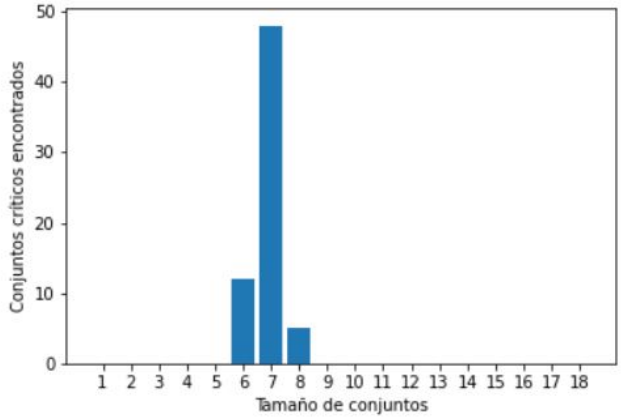


Figura 4.30: Estudio estadístico $L_{6,4}$ y Θ_3 (Fuente: Elaboración propia)

4. Sea $\Theta_4 \equiv ((123)(465), (16)(25)(34), (153624))$:

```
graficaEstudioEstadístico(representante_L64,autotopismos_L64[4])
```

```
Con el tamaño:  4  , hay:  400  aciertos.
```

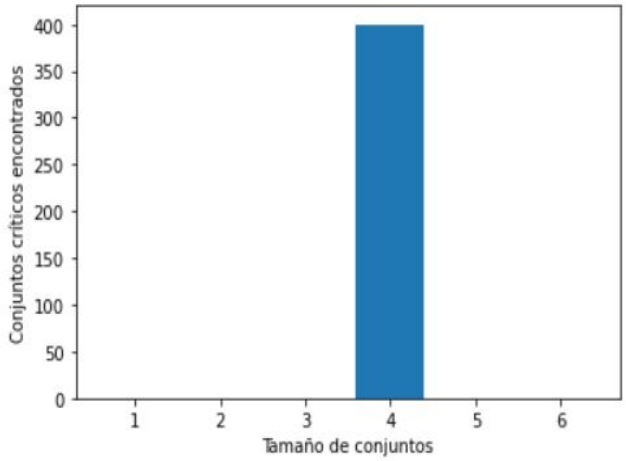


Figura 4.31: Estudio estadístico $L_{6,4}$ y Θ_4 (Fuente: Elaboración propia)

5. Sea $\Theta_5 \equiv ((123)(465), (132)(456), \mathrm{Id}_6)$:

```
graficaEstudioEstadístico(representante_L64,autotopismos_L64[5])
```

```
Con el tamaño:  8  , hay:  118  aciertos.
```

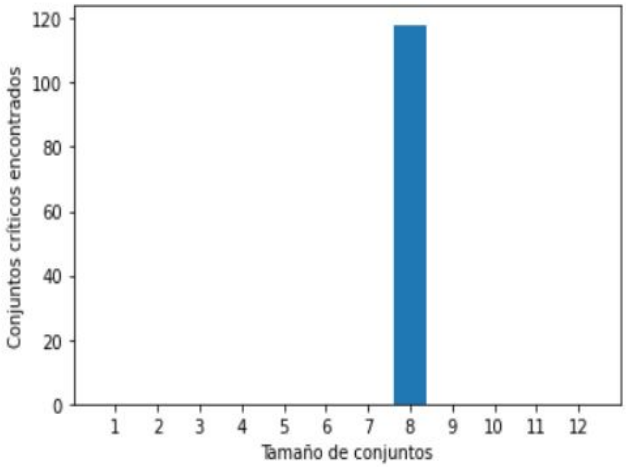


Figura 4.32: Estudio estadístico $L_{6,4}$ y Θ_5 (Fuente: Elaboración propia)

6. Sea $\Theta_6 \equiv ((123)(465), (123)(465), (132)(456))$:

```
graficaEstudioEstadístico(representante_L64,autotopismos_L64[6])
```

```
Con el tamaño:  4  , hay:  79  aciertos.
Con el tamaño:  5  , hay:  18  aciertos.
```

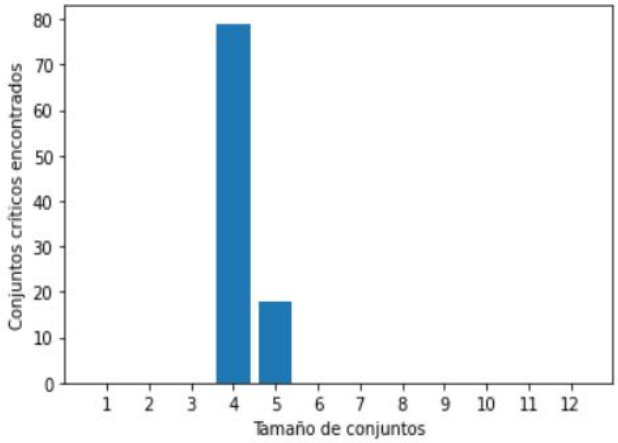


Figura 4.33: Estudio estadístico $L_{6,4}$ y Θ_6 (Fuente: Elaboración propia)

7. Sea $\Theta_7 \equiv ((142635), (153624), \mathrm{Id}_6)$:

```
graficaEstudioEstadístico(representante_L64,autotopismos_L64[7])
```

```
Con el tamaño:  5  , hay:  1000  aciertos.
```

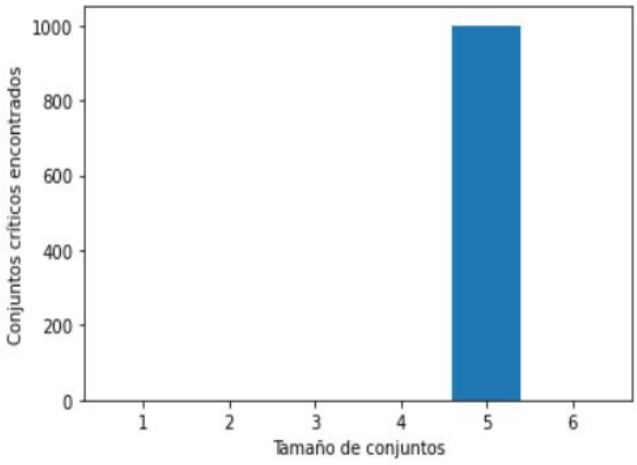


Figura 4.34: Estudio estadístico $L_{6,4}$ y Θ_7 (Fuente: Elaboración propia)

8. Sea $\Theta_8 \equiv ((142635), (142635), (123)(465))$:

```
graficaEstudioEstadístico(representante_L64,autotopismos_L64[8])
```

```
Con el tamaño:  3  , hay:  278  aciertos.
```

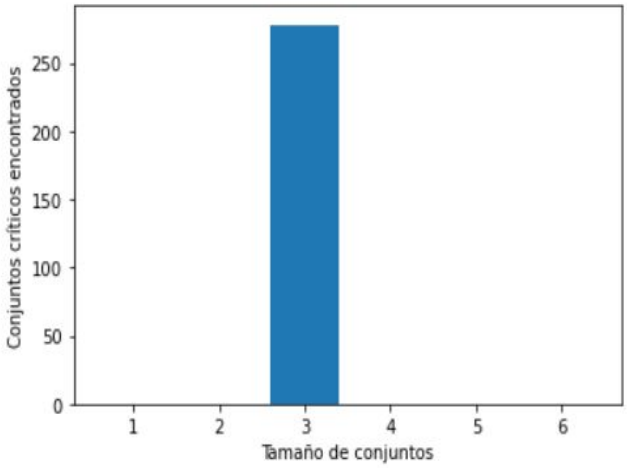


Figura 4.35: Estudio estadístico $L_{6,4}$ y Θ_8 (Fuente: Elaboración propia)

Caso 5: Suponemos el cuadrado latino $L_{6,5}$:

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

Se realiza el estudio estadístico con cada uno de sus autotopismos:

1. Sea $\Theta_1 \equiv (\mathrm{Id}_6, (15)(24)(36), (15)(24)(63))$:

```
graficaEstudioEstadístico(representante_L65,autotopismos_L65[1])
```

```
Con el tamaño:  9  , hay:  2  aciertos.
Con el tamaño:  10  , hay:  10  aciertos.
```

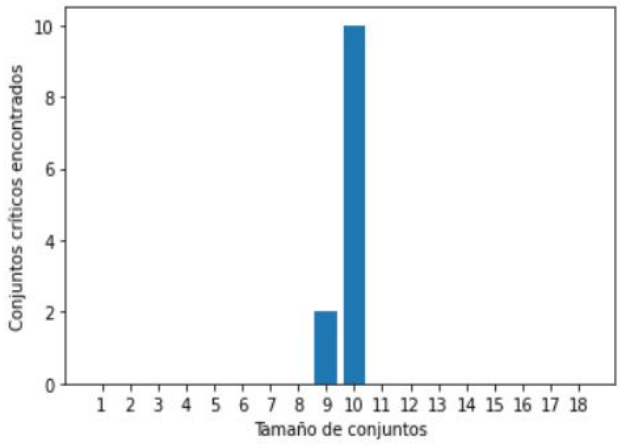


Figura 4.36: Estudio estadístico $L_{6,5}$ y Θ_1 (Fuente: Elaboración propia)

2. Sea $\Theta_2 \equiv ((12)(45), (23)(46), (12)(45))$:

```
graficaEstudioEstadístico(representante_L65,autotopismos_L65[2])
```

```
Con el tamaño:  8  , hay:  12  aciertos.
Con el tamaño:  9  , hay:  2  aciertos.
```

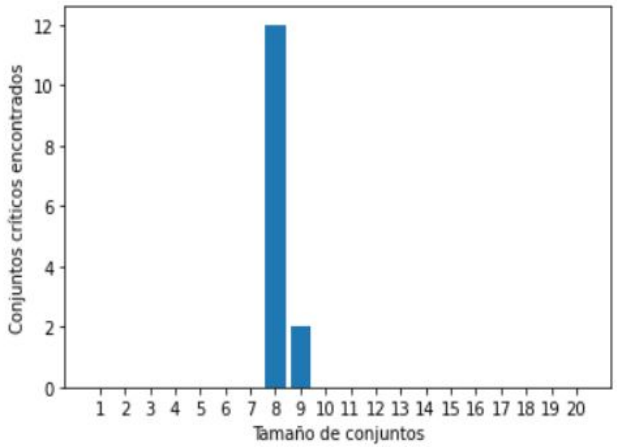


Figura 4.37: Estudio estadístico $L_{6,5}$ y Θ_2 (Fuente: Elaboración propia)

3. Sea $\Theta_3 \equiv ((345), (123)(465), (123)(465))$:

```
graficaEstudioEstadístico(representante_L65,autotopismos_L65[3])
```

```
Con el tamaño:  4  , hay:  3  aciertos.
Con el tamaño:  5  , hay:  126  aciertos.
Con el tamaño:  6  , hay:  20  aciertos.
```

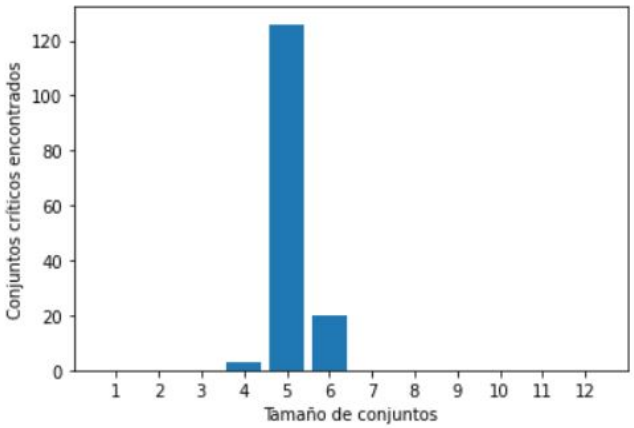


Figura 4.38: Estudio estadístico $L_{6,5}$ y Θ_3 (Fuente: Elaboración propia)

4. Sea $\Theta_4 \equiv ((345), (143526), (143526))$:

```
graficaEstudioEstadístico(representante_L65,autotopismos_L65[4])
```

```
Con el tamaño:  3  , hay:  138  aciertos.
```

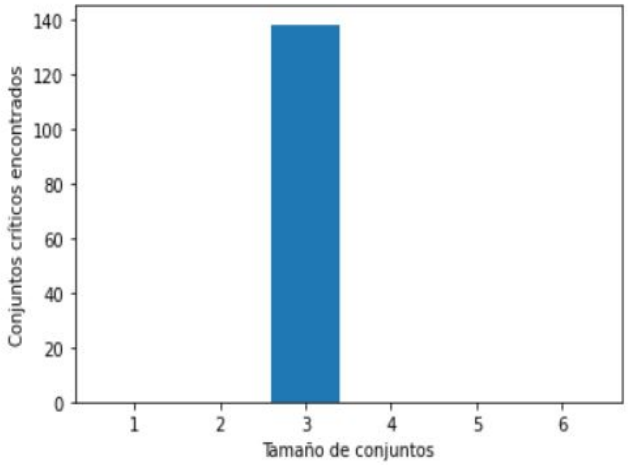


Figura 4.39: Estudio estadístico $L_{6,5}$ y Θ_4 (Fuente: Elaboración propia)

5. Sea $\Theta_5 \equiv ((12)(45), (15)(26)(34), (14)(25)(36))$:

```
graficaEstudioEstadístico(representante_L65,autotopismos_L65[5])
```

```
Con el tamaño:  6  , hay:  6  aciertos.
Con el tamaño:  7  , hay:  46  aciertos.
Con el tamaño:  8  , hay:  1  aciertos.
```

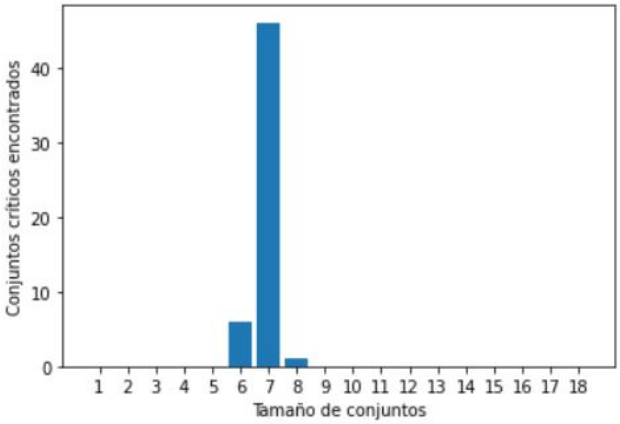


Figura 4.40: Estudio estadístico $L_{6,5}$ y Θ_5 (Fuente: Elaboración propia)

Caso 6: Suponemos el cuadrado latino $L_{6,6}$:

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

Se realiza el estudio estadístico con cada uno de sus autotopismos:

1. Sea $\Theta_1 \equiv ((23), (12)(34)(56), (12)(34)(56))$:

```
graficaEstudioEstadístico(representante_L66,autotopismos_L66[1])
```

```
Con el tamaño:  7  , hay:  3  aciertos.
Con el tamaño:  8  , hay:  16  aciertos.
Con el tamaño:  9  , hay:  5  aciertos.
```

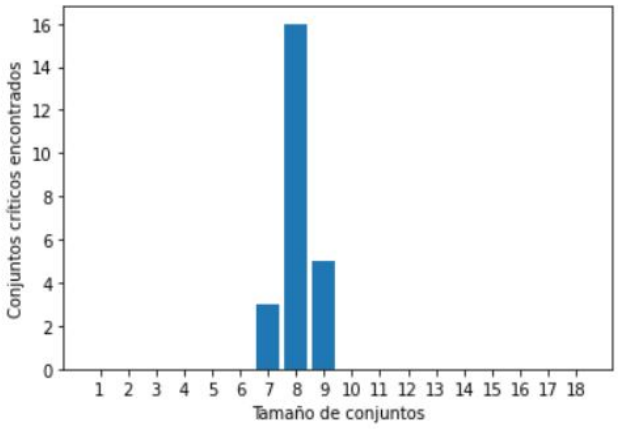


Figura 4.41: Estudio estadístico $L_{6,6}$ y Θ_1 (Fuente: Elaboración propia)

2. Sea $\Theta_2 \equiv ((25)(34), (25)(34)(25)(34))$:

```
graficaEstudioEstadístico(representante_L66,autotopismos_L66[2])
```

```
Con el tamaño:  7  , hay:  4  aciertos.
Con el tamaño:  8  , hay:  5  aciertos.
Con el tamaño:  9  , hay:  1  aciertos.
```

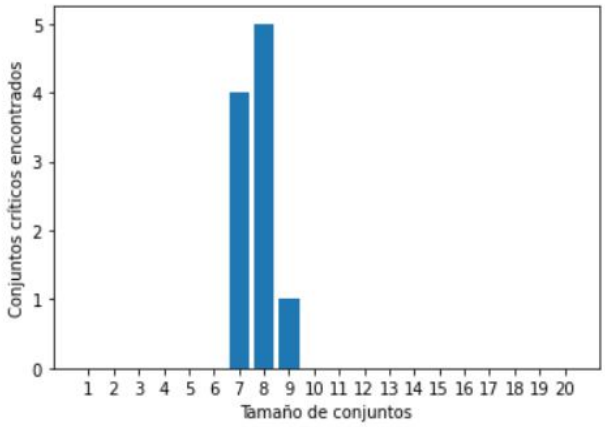


Figura 4.42: Estudio estadístico $L_{6,6}$ y Θ_2 (Fuente: Elaboración propia)

3. Sea $\Theta_3 \equiv ((354), (124)(365), (124)(365))$:

```
graficaEstudioEstadístico(representante_L66,autotopismos_L66[3])
```

```
Con el tamaño:  4  , hay:  6  aciertos.
Con el tamaño:  5  , hay:  149  aciertos.
Con el tamaño:  6  , hay:  3  aciertos.
```

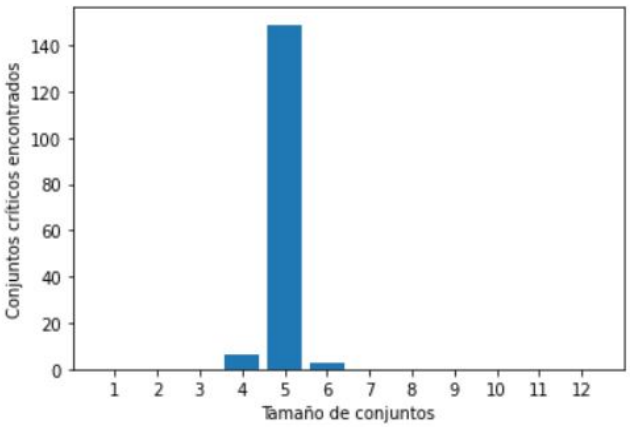


Figura 4.43: Estudio estadístico $L_{6,6}$ y Θ_3 (Fuente: Elaboración propia)

4. Sea $\Theta_4 \equiv ((2453), (2453), (2453))$:

```
graficaEstudioEstadístico(representante_L66,autotopismos_L66[4])
```

```
Con el tamaño:  5  , hay:  11  aciertos.
Con el tamaño:  6  , hay:  96  aciertos.
```

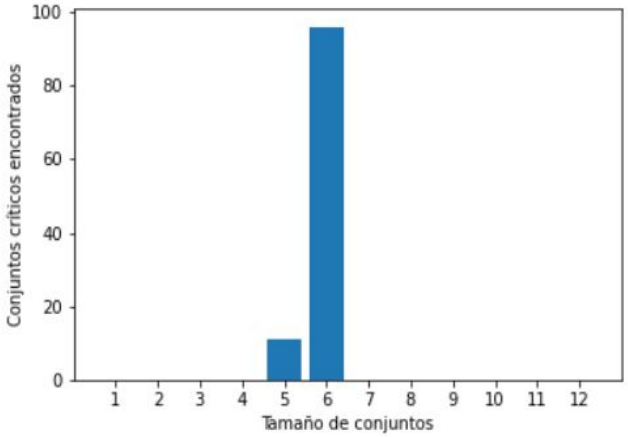


Figura 4.44: Estudio estadístico $L_{6,6}$ y Θ_4 (Fuente: Elaboración propia)

5. Sea $\Theta_5 \equiv ((354)(12), (164325), (134526))$:

```
graficaEstudioEstadístico(representante_L66,autotopismos_L66[5])
```

```
Con el tamaño:  2  , hay:  128  aciertos.
Con el tamaño:  3  , hay:  185  aciertos.
```

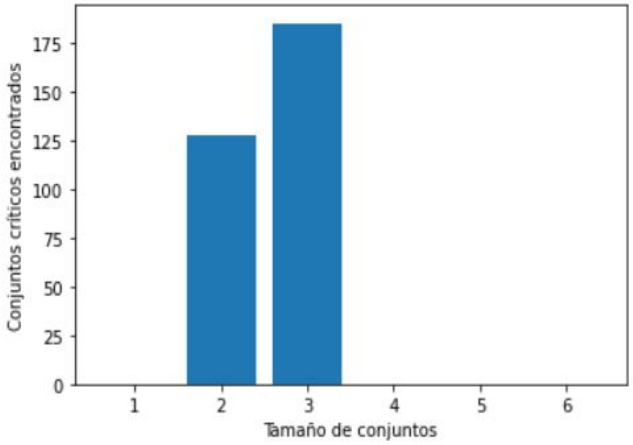


Figura 4.45: Estudio estadístico $L_{6,6}$ y Θ_5 (Fuente: Elaboración propia)

6. Sea $\Theta_6 \equiv ((12345), (26543), (12345))$:

```
graficaEstudioEstadístico(representante_L66,autotopismos_L66[6])
```

```
Con el tamaño:  3  , hay:  535  aciertos.
Con el tamaño:  4  , hay:  19  aciertos.
```

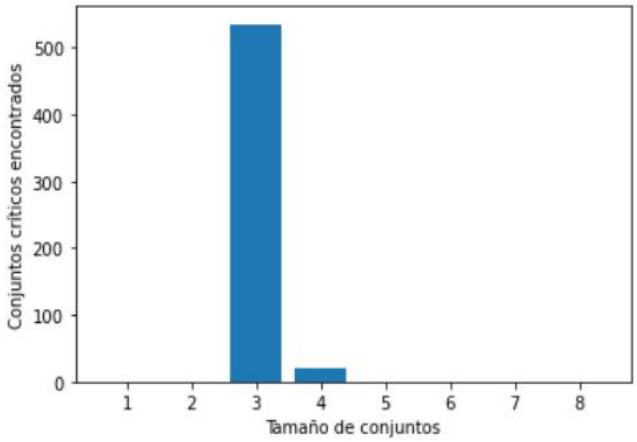


Figura 4.46: Estudio estadístico $L_{6,6}$ y Θ_6 (Fuente: Elaboración propia)

Caso 7: Suponemos el cuadrado latino $L_{6,7}$:

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

Se realiza el estudio estadístico con cada uno de sus autotopismos:

1. Sea $\Theta_1 \equiv ((12)(56), (14)(35), (24)(36))$:

```
graficaEstudioEstadístico(representante_L67,autotopismos_L67[1])
```

```
Con el tamaño:  7  , hay:  2  aciertos.
Con el tamaño:  8  , hay:  3  aciertos.
Con el tamaño:  9  , hay:  2  aciertos.
```

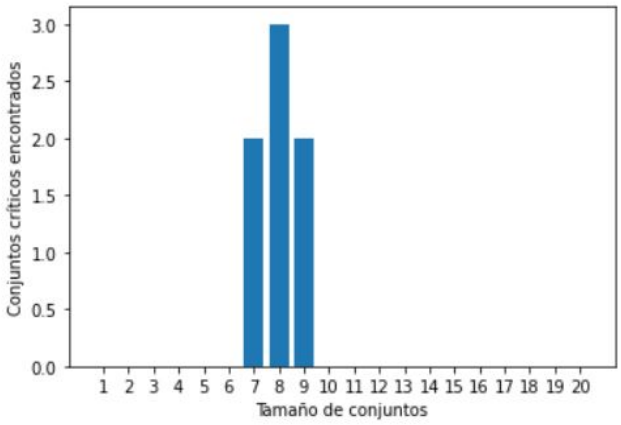


Figura 4.47: Estudio estadístico $L_{6,7}$ y Θ_1 (Fuente: Elaboración propia)

2. Sea $\Theta_2 \equiv ((15)(26)(34), (15)(26)(34), \mathrm{Id}_6)$:

```
graficaEstudioEstadístico(representante_L67,autotopismos_L67[2])
```

```
Con el tamaño:  9  , hay:  8  aciertos.
Con el tamaño:  10  , hay:  2  aciertos.
```

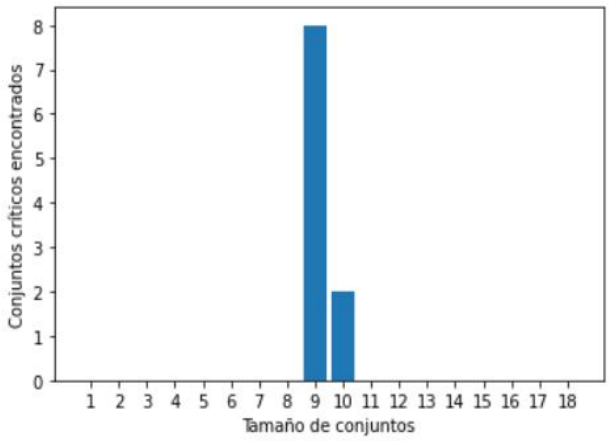


Figura 4.48: Estudio estadístico $L_{6,7}$ y Θ_2 (Fuente: Elaboración propia)

3. Sea $\Theta_3 \equiv ((14)(26)(35), (15)(24)(36), (13)(45))$:

```
graficaEstudioEstadístico(representante_L67,autotopismos_L67[3])
```

```
Con el tamaño:  6  , hay:  12  aciertos.
Con el tamaño:  7  , hay:  43  aciertos.
Con el tamaño:  8  , hay:  5  aciertos.
```

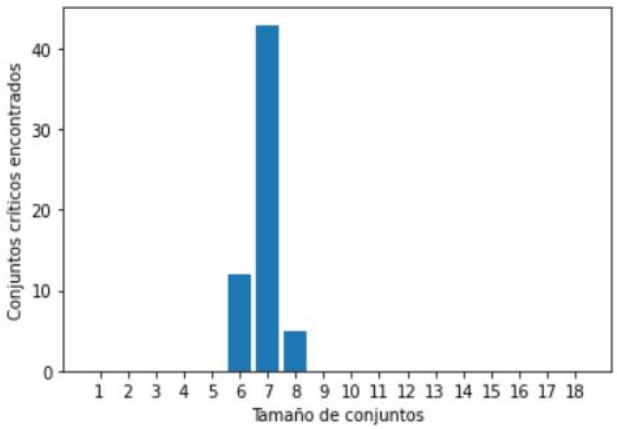


Figura 4.49: Estudio estadístico $L_{6,7}$ y Θ_3 (Fuente: Elaboración propia)

4. Sea $\Theta_4 \equiv ((123)(456), (164)(235), (136)(254))$:

```
graficaEstudioEstadístico(representante_L67,autotopismos_L67[4])
```

```
Con el tamaño:  4  , hay:  387  aciertos.
Con el tamaño:  5  , hay:  8  aciertos.
```

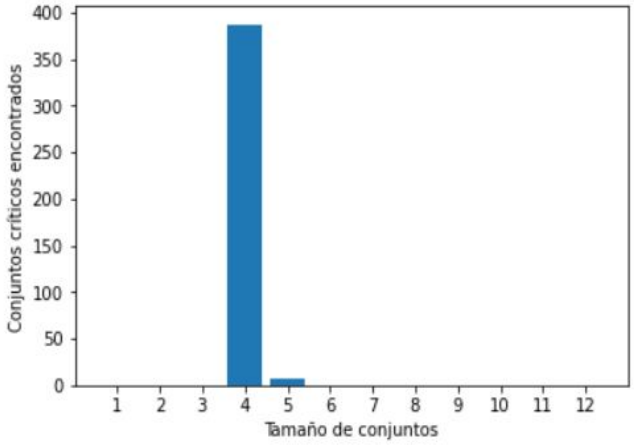


Figura 4.50: Estudio estadístico $L_{6,7}$ y Θ_4 (Fuente: Elaboración propia)

5. Sea $\Theta_5 \equiv ((142536), (136542), (163)(245))$:

```
graficaEstudioEstadístico(representante_L67,autotopismos_L67[5])
```

```
Con el tamaño:  3  , hay:  283  aciertos.
```

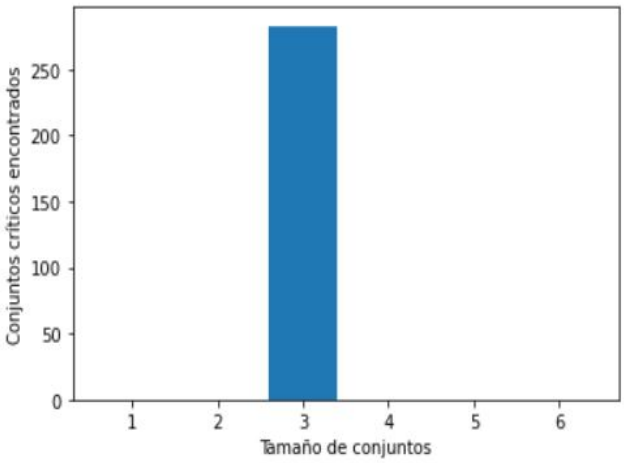


Figura 4.51: Estudio estadístico $L_{6,7}$ y Θ_5 (Fuente: Elaboración propia)

Caso 8: Suponemos el cuadrado latino $L_{6,8}$:

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

Se realiza el estudio estadístico con cada uno de sus autotopismos:

1. Sea $\Theta_1 \equiv ((142536), (136542), (163)(245))$:

```
graficaEstudioEstadístico(representante_L68,autotopismos_L68[1])
```

```
Con el tamaño:  8  , hay:  5  aciertos.
Con el tamaño:  9  , hay:  1  aciertos.
```

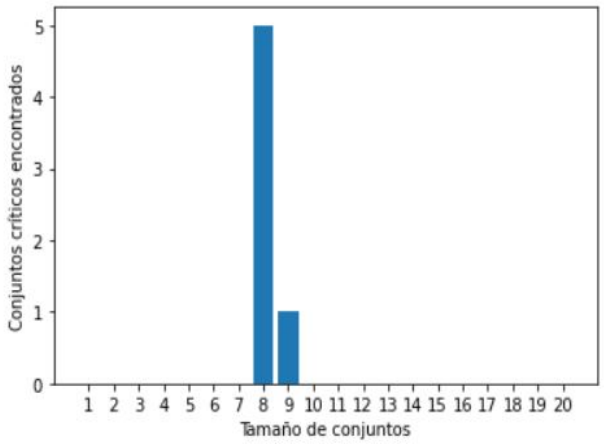


Figura 4.52: Estudio estadístico $L_{6,8}$ y Θ_1 (Fuente: Elaboración propia)

2. Sea $\Theta_2 \equiv ((12)(34), (14)(36), (24)(56))$:

```
graficaEstudioEstadístico(representante_L68,autotopismos_L68[2])
```

```
Con el tamaño:  5  , hay:  13  aciertos.
Con el tamaño:  6  , hay:  115  aciertos.
```

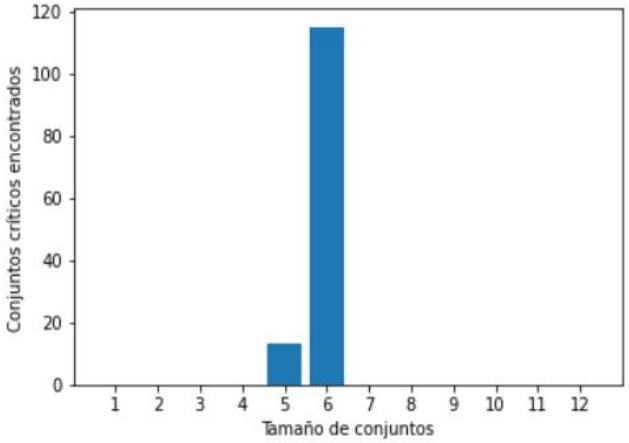


Figura 4.53: Estudio estadístico $L_{6,8}$ y Θ_2 (Fuente: Elaboración propia)

3. Sea $\Theta_3 \equiv ((24), (14)(23)(56), (14)(23)(56))$:

```
graficaEstudioEstadístico(representante_L68,autotopismos_L68[3])
```

```
Con el tamaño:  7  , hay:  5  aciertos.
Con el tamaño:  8  , hay:  8  aciertos.
Con el tamaño:  9  , hay:  4  aciertos.
```

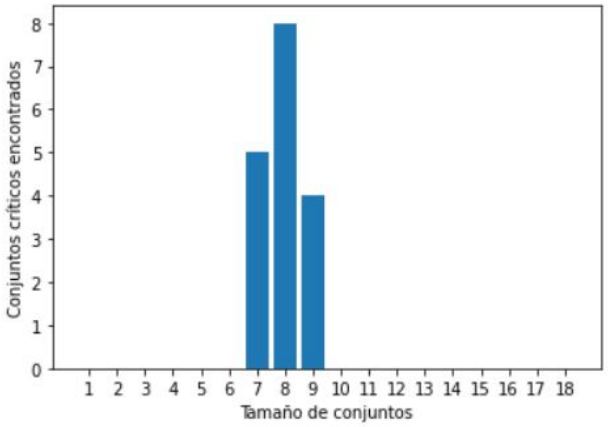


Figura 4.54: Estudio estadístico $L_{6,8}$ y Θ_3 (Fuente: Elaboración propia)

Caso 9: Suponemos el cuadrado latino $L_{6,9}$:

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

Se realiza el estudio estadístico con cada uno de sus autotopismos:

1. Sea $\Theta_1 \equiv ((13)(24)(56), (12)(34)(56), (16)(23))$:

```
graficaEstudioEstadístico(representante_L69,autotopismos_L69[1])
```

```
Con el tamaño:  6  , hay:  35  aciertos.
Con el tamaño:  7  , hay:  50  aciertos.
Con el tamaño:  8  , hay:  3  aciertos.
```

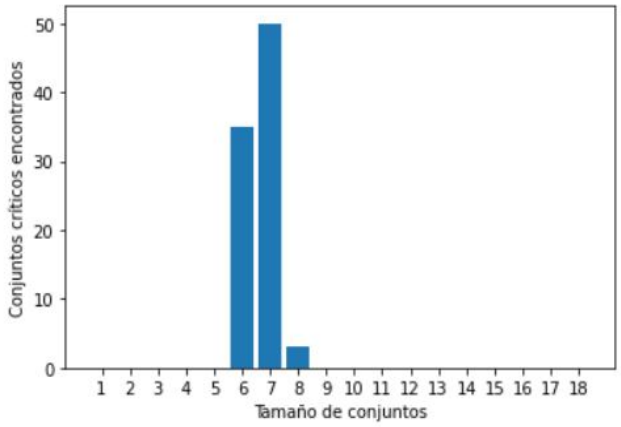


Figura 4.55: Estudio estadístico $L_{6,9}$ y Θ_1 (Fuente: Elaboración propia)

Caso 10: Suponemos el cuadrado latino $L_{6,10}$:

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

Se realiza el estudio estadístico con cada uno de sus autotopismos:

1. Sea $\Theta_1 \equiv ((34), (14)(23)(56), (14)(23)(56))$:

```
graficaEstudioEstadístico(representante_L610,autotopismos_L610[1])
```

```
Con el tamaño:  7  , hay:  12  aciertos.
Con el tamaño:  8  , hay:  19  aciertos.
Con el tamaño:  9  , hay:  2  aciertos.
```

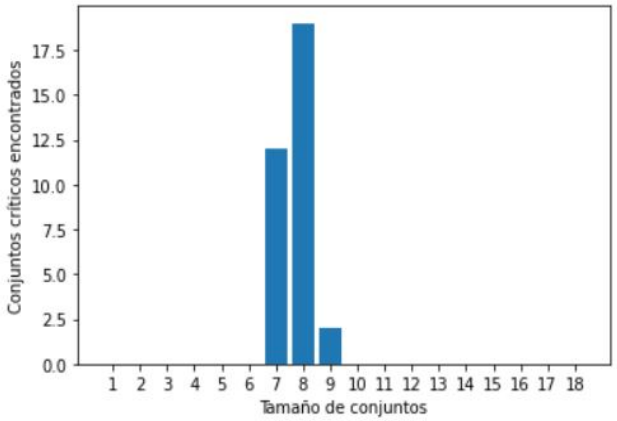


Figura 4.56: Estudio estadístico $L_{6,10}$ y Θ_1 (Fuente: Elaboración propia)

2. Sea $\Theta_2 \equiv ((12)(34), (25)(36), (12)(34))$:

```
graficaEstudioEstadístico(representante_L610,autotopismos_L610[2])
```

```
Con el tamaño:  7  , hay:  1  aciertos.
Con el tamaño:  8  , hay:  3  aciertos.
Con el tamaño:  9  , hay:  8  aciertos.
```

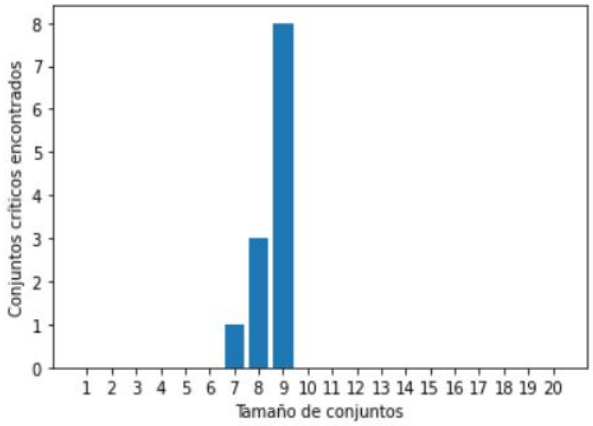


Figura 4.57: Estudio estadístico $L_{6,10}$ y Θ_2 (Fuente: Elaboración propia)

Caso 11: Suponemos el cuadrado latino $L_{6,11}$:

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

Se realiza el estudio estadístico con cada uno de sus autotopismos:

1. Sea $\Theta_1 \equiv ((12)(35), (12)(56), (16)(34))$:

```
graficaEstudioEstadístico(representante_L611,autotopismos_L611[1])
```

```
Con el tamaño:  8  , hay:  4  aciertos.
Con el tamaño:  9  , hay:  1  aciertos.
```

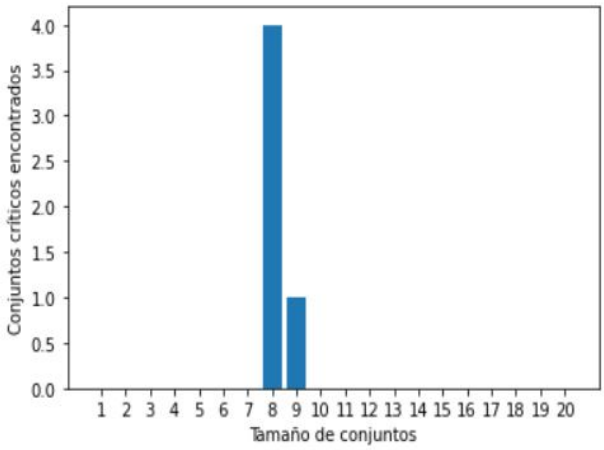


Figura 4.58: Estudio estadístico $L_{6,11}$ y Θ_1 (Fuente: Elaboración propia)

Caso 12: Suponemos el cuadrado latino $L_{6,12}$:

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

Se realiza el estudio estadístico con cada uno de sus autotopismos:

1. Sea $\Theta_1 \equiv (\mathrm{Id}_6, (126)(345), (126)(345))$:

```
graficaEstudioEstadístico(representante_L612,autotopismos_L612[1])
```

```
Con el tamaño:  8  , hay:  144  aciertos.
```

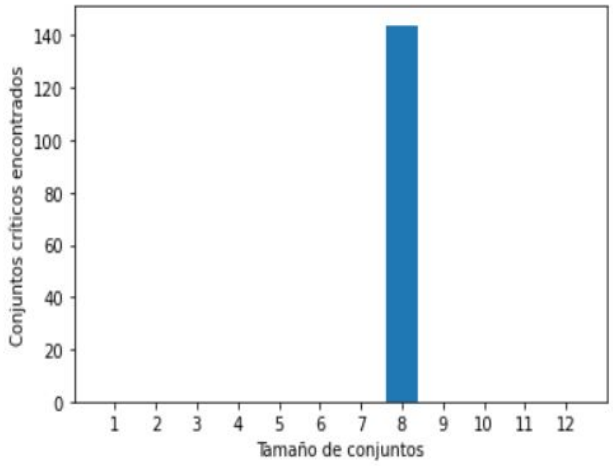


Figura 4.59: Estudio estadístico $L_{6,12}$ y Θ_1 (Fuente: Elaboración propia)

2. Sea $\Theta_2 \equiv ((34), (13)(24)(56), (13)(24)(56))$:

```
graficaEstudioEstadístico(representante_L612,autotopismos_L612[2])
```

```
Con el tamaño:  7  , hay:  4  aciertos.
Con el tamaño:  8  , hay:  10  aciertos.
Con el tamaño:  9  , hay:  3  aciertos.
```

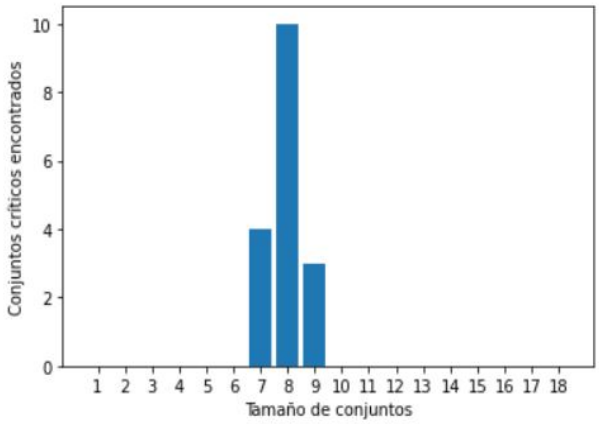


Figura 4.60: Estudio estadístico $L_{6,12}$ y Θ_2 (Fuente: Elaboración propia)

3. Sea $\Theta_3 \equiv ((45), (132465), (132465))$:

```
graficaEstudioEstadístico(representante_L612,autotopismos_L612[3])
```

```
Con el tamaño:  4  , hay:  398  aciertos.
Con el tamaño:  5  , hay:  176  aciertos.
```

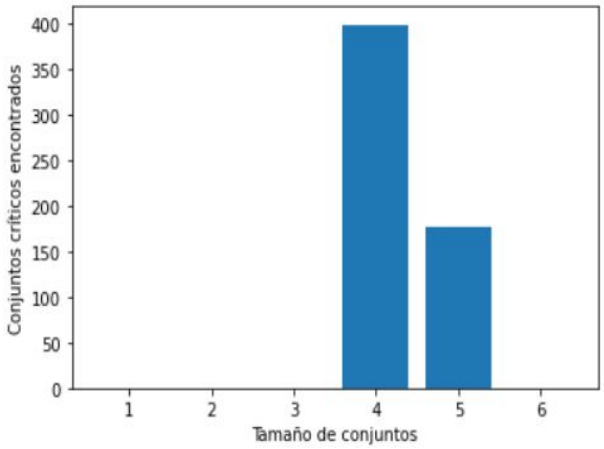


Figura 4.61: Estudio estadístico $L_{6,12}$ y Θ_3 (Fuente: Elaboración propia)

4. Sea $\Theta_4 \equiv ((345), (345), (345))$:

```
graficaEstudioEstadístico(representante_L612,autotopismos_L612[4])
```

```
Con el tamaño:  8  , hay:  8  aciertos.
Con el tamaño:  9  , hay:  11  aciertos.
```

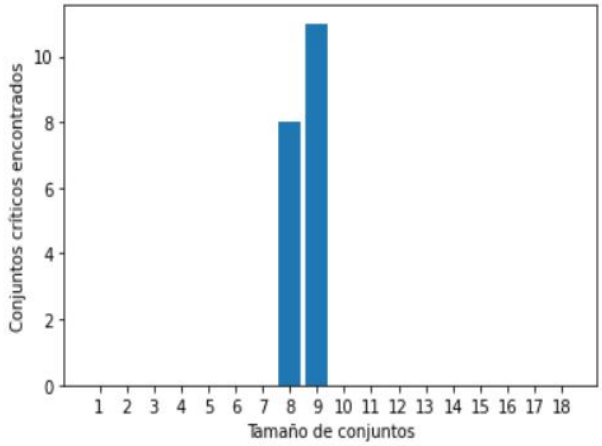


Figura 4.62: Estudio estadístico $L_{6,12}$ y Θ_4 (Fuente: Elaboración propia)

5. Sea $\Theta_5 \equiv ((345), (126)(354), (126)(354))$:

```
graficaEstudioEstadístico(representante_L612,autotopismos_L612[5])
```

```
Con el tamaño:  6  , hay:  85  aciertos.
Con el tamaño:  7  , hay:  11  aciertos.
```

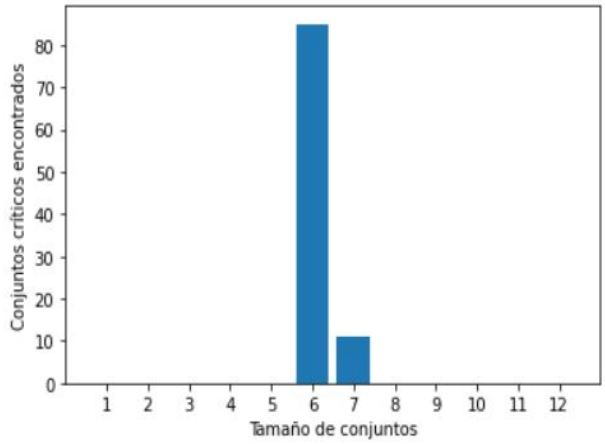


Figura 4.63: Estudio estadístico $L_{6,12}$ y Θ_5 (Fuente: Elaboración propia)

6. Sea $\Theta_6 \equiv ((12)(35), (26)(34), (12)(35))$:

```
graficaEstudioEstadístico(representante_L612,autotopismos_L612[6])
```

```
Con el tamaño:  8  , hay:  2  aciertos.
Con el tamaño:  9  , hay:  1  aciertos.
```

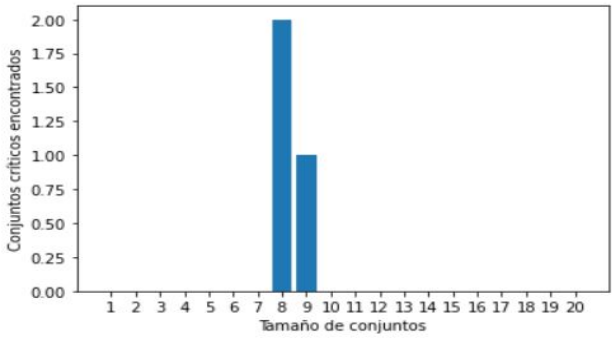


Figura 4.64: Estudio estadístico $L_{6,12}$ y Θ_6 (Fuente: Elaboración propia)

7. Sea $\Theta_7 \equiv ((354)(12), (132564), (142365))$:

```
graficaEstudioEstadístico(representante_L612,autotopismos_L612[7])
```

```
Con el tamaño:  3  , hay:  354  aciertos.
```

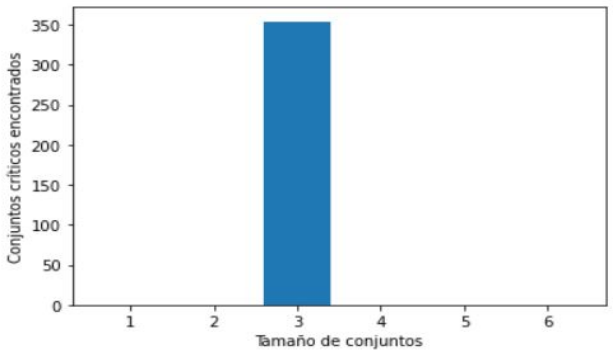


Figura 4.65: Estudio estadístico $L_{6,12}$ y Θ_7 (Fuente: Elaboración propia)

Como se ha podido comprobar a lo largo de las ejecuciones realizadas, el número de aciertos se reduce considerablemente en comparación con los ejemplos estudiados anteriormente. Esto se debe a que, como se mencionaba en apartados anteriores, la selección de combinaciones de órbitas y, por tanto, de conjuntos, es completamente aleatoria, por lo que a mayor número de combinaciones, más complicado resultará encontrar conjuntos que sean críticos. Esto nos lleva a pensar que será necesario hacer un estudio teórico similar al llevado a cabo en órdenes inferiores si se quieren obtener conjuntos críticos en dichos órdenes. Aún así, a través de este estudio estadístico, hemos hecho una primera aproximación que permite conjeturar el tamaño posible de los conjuntos críticos en orden 6 en los casos analizados.

A continuación se introduce, a modo de resumen, un cuadro que recoge los resultados obtenidos (en negrita) a lo largo de las ejecuciones anteriores. En este trabajo no se ha estudiado el caso de la identidad, por ser éste un caso particular en el que no hay órbitas distintas de las triviales y, además, este caso ya es conocido hasta orden 6 (Adams, Bean, y Khodkar, 2003).

n	$\Theta \in \mathrm{Atop}(L_{6.n})$	z_Θ	$\mathrm{scs}_\Theta(L_{6.n})$	$\mathrm{lcs}_\Theta(L_{6.n})$	Referencia
1	$(\mathrm{Id}_6, \mathrm{Id}_6, \mathrm{Id}_6)$	$(1^6, 1^6, 1^6)$	11	17	(Adams y cols., 2003)
	$((36)(45), (36)(45), (36)(45))$	$(2^2 1^2, 2^2, 1^2, 2^2 1^2)$	**7**	**9**	
	$((12)(35)(46), (12)(34)(56), \mathrm{Id}_6)$	$(2^3, 2^3, 1^6)$	**9**	**10**	
	$((12)(34)(56), (12)(35)(46), (36)(45))$	$(2^3, 2^3, 2^2 1^2)$	**7**	**8**	
2	$(\mathrm{Id}_6, \mathrm{Id}_6, \mathrm{Id}_6)$	$(1^6, 1^6, 1^6)$	12	18	(Adams y cols., 2003)
	$((23)(45), (23)(45), (23)(45))$	$(2^2 1^2, 2^2 1^2, 2^2 1^2)$	**7**	**9**	
	$((14)(25)(36), (14)(26)(35), \mathrm{Id}_6)$	$(2^3, 2^3, 1^6)$	**9**	**10**	
	$((14)(26)(35), (14)(25)(36), (23)(56))$	$(2^3, 2^3, 2^2 1^2)$	**7**	**8**	
	$((456), (456), (456)))$	$(31^3, 31^3, 31^3)$	**8**	**9**	
	$((123)(456), (15)(26)(34), (163524))$	$(3^2, 2^3, 6)$	**4**	**4**	
	$((132)(465), (123)(456), \mathrm{Id}_6)$	$(3^2, 3^2, 1^6)$	**8**	**8**	
	$((123)(456), (132)(456), (465))$	$(3^2, 3^2, 31^3)$	**6**	**7**	
	$((142635), (153426), (13)(46))$	$(6, 6, 2^2 1^2)$	**4**	**4**	
	$((142536), (143526), (456))$	$(6, 6, 31^3)$	**3**	**3**	
3	$(\mathrm{Id}_6, \mathrm{Id}_6, \mathrm{Id}_6)$	$(1^6, 1^6, 1^6)$	11	16	(Adams y cols., 2003)
	$((456), (123), (123))$	$(31^3, 31^3, 31^3)$	**8**	**9**	
	$((14)(26)(35), (15)(26)(34), (12)(45))$	$(2^3, 2^3, 2^2 1^2)$	**6**	**8**	
	$((123)(465), (132)(465), \mathrm{Id}_6)$	$(3^2, 3^2, 1^6)$	**8**	**8**	
	$((123)(456), (123)(465), (132))$	$(3^2, 3^2, 31^3)$	**6**	**6**	
	$((153624), (152634), (13)(45))$	$(6, 6, 2^2 1^2)$	**4**	**4**	
4	$(\mathrm{Id}_6, \mathrm{Id}_6, \mathrm{Id}_6)$	$(1^6, 1^6, 1^6)$	9	17	(Adams y cols., 2003)
	$((23)(45), (23)(45), (23)(45))$	$(2^2 1^2, 2^2 1^2, 2^2 1^2)$	**7**	**9**	
	$((16)(25)(34), (16)(25)(34), \mathrm{Id}_6)$	$(2^3, 2^3, 1^6)$	**9**	**10**	
	$((14)(25)(36), (15)(26)(34), (23)(45))$	$(2^3, 2^3, 2^2 1^2)$	**6**	**8**	
	$((123)(465), (16)(25)(34), (153624))$	$(3^2, 2^3, 6)$	**4**	**4**	
	$((123)(465), (132)(456), \mathrm{Id}_6)$	$(3^2, 3^2, 1^6)$	**8**	**8**	
	$((123)(465), (123)(465), (132)(456))$	$(3^2, 3^2, 3^2)$	**4**	**5**	
	$((142635), (153624), \mathrm{Id}_6)$	$(6, 6, 1^6)$	5	5	Teorema 3.11
	$((142635), (142635), (123)(465))$	$(6, 6, 3^2)$	**3**	**3**	
5	$(\mathrm{Id}_6, \mathrm{Id}_6, \mathrm{Id}_6)$	$(1^6, 1^6, 1^6)$	10	17	(Adams y cols., 2003)
	$(\mathrm{Id}_6, (15)(24)(36), (15)(24)(63))$	$(1^6, 2^3, 2^3)$	**9**	**10**	
	$((12)(45), (23)(46), (12)(45))$	$(2^2 1^2, 2^2 1^2, 2^2 1^2)$	**8**	**9**	
	$((345), (123)(465), (123)(465))$	$(31^3, 3^2, 3^2)$	**4**	**6**	
	$((345), (143526), (143526))$	$(31^3, 6, 6)$	**3**	**3**	
	$((12)(45), (15)(26)(34), (14)(25)(36))$	$(2^2 1^2, 3^2, 3^2)$	**6**	**8**	
6	$(\mathrm{Id}_6, \mathrm{Id}_6, \mathrm{Id}_6)$	$(1^6, 1^6, 1^6)$	11	17	(Adams y cols., 2003)
	$((23), (12)(34)(56), (12)(34)(56))$	$(21^4, 2^3, 2^3)$	**7**	**9**	
	$((25)(34), (25)(34)(25)(34))$	$(2^2 1^2, 2^2 1^2, 2^2 1^2)$	**7**	**9**	
	$((354), (124)(365), (124)(365))$	$(31^3, 3^2, 3^2)$	**4**	**6**	
	$((2453), (2453), (2453))$	$(41^2, 41^2, 41^2)$	**5**	**6**	
	$((354)(12), (164325), (134526))$	$(321, 6, 6)$	**2**	**3**	
	$((12345), (26543), (12345))$	$(51, 51, 51)$	**3**	**4**	
7	$(\mathrm{Id}_6, \mathrm{Id}_6, \mathrm{Id}_6)$	$(1^6, 1^6, 1^6)$	11	17	(Adams y cols., 2003)
	$((12)(56), (14)(35), (24)(36))$	$(2^2 1^2, 2^2 1^2, 2^2 1^2)$	**7**	**9**	
	$((15)(26)(34), (15)(26)(34), \mathrm{Id}_6)$	$(2^3, 2^3, 1^6)$	**9**	**10**	
	$((14)(26)(35), (15)(24)(36), (13)(45))$	$(2^3, 2^3, 2^2 1^2)$	**6**	**8**	
	$((123)(456), (164)(235), (136)(254))$	$(3^2, 3^2, 3^2)$	**4**	**5**	
	$((142536), (136542), (163)(245))$	$(6, 6, 3^2)$	**3**	**3**	
8	$(\mathrm{Id}_6, \mathrm{Id}_6, \mathrm{Id}_6)$	$(1^6, 1^6, 1^6)$	10	17	(Adams y cols., 2003)
	$((12)(34), (14)(36), (24)(56))$	$(2^2 1^2, 2^2 1^2, 2^2 1^2)$	**8**	**9**	
	$((1234), (2653), (1234))$	$(41^2, 41^2, 41^2)$	**5**	**6**	
	$((24), (14)(23)(56), (14)(23)(56))$	$(21^4, 2^3, 2^3)$	**7**	**9**	
9	$(\mathrm{Id}_6, \mathrm{Id}_6, \mathrm{Id}_6)$	$(1^6, 1^6, 1^6)$	10	17	(Adams y cols., 2003)
	$((13)(24)(56), (12)(34)(56), (16)(23))$	$(2^3, 2^3, 2^2 1^2)$	**6**	**8**	
10	$(\mathrm{Id}_6, \mathrm{Id}_6, \mathrm{Id}_6)$	$(1^6, 1^6, 1^6)$	10	17	(Adams y cols., 2003)
	$((34), (14)(23)(56), (14)(23)(56))$	$(21^4, 2^3, 2^3)$	**7**	**9**	
	$((12)(34), (25)(36), (12)(34))$	$(2^2 1^2, 2^2 1^2, 2^2 1^2)$	**7**	**9**	
11	$(\mathrm{Id}_6, \mathrm{Id}_6, \mathrm{Id}_6)$	$(1^6, 1^6, 1^6)$	10	17	(Adams y cols., 2003)
	$((12)(35), (12)(56), (16)(34))$	$(2^2 1^2, 2^2 1^2, 2^2 1^2)$	**8**	**9**	
12	$(\mathrm{Id}_6, \mathrm{Id}_6, \mathrm{Id}_6)$	$(1^6, 1^6, 1^6)$	11	17	(Adams y cols., 2003)
	$(\mathrm{Id}_6, (126)(345), (126)(345))$	$(1^6, 3^2, 3^2)$	**8**	**8**	
	$((34), (13)(24)(56), (13)(24)(56))$	$(21^4, 2^3, 2^3)$	**7**	**9**	
	$((45), (132465), (132465))$	$(21^4, 6, 6)$	**4**	**5**	
	$((345), (345), (345))$	$(31^3, 31^3, 31^3)$	**8**	**9**	
	$((345), (126)(354), (126)(354))$	$(31^3, 3^2, 3^2)$	**6**	**7**	
	$((12)(35), (26)(34), (12)(35))$	$(2^2 1^2, 2^2 1^2, 2^2 1^2)$	**8**	**9**	
	$((354)(12), (132564), (142365))$	$(321, 6, 6)$	**3**	**3**	

Cuadro 4.1: Autotopismos de $L_{6,1}$–$L_{6,12}$.

CAPÍTULO 5

Análisis temporal y costes de desarrollo

En este capítulo identificaremos las actividades, tareas e hitos que conforman el proyecto. Posteriormente las situaremos en el tiempo siguiendo un cronograma y formalizaremos una estimación de los costes del proyecto.

5.1– Actividades, tareas e hitos

En esta sección llevaremos a cabo la agrupación de tareas en función de actividades, destacando los diferentes hitos. Por conveniencia, incluimos también el responsable de cada actividad aunque, a excepción del *tester* cuyo papel será jugado también por ambos tutores del TfG, todos los roles serán recogidos en la misma persona: el autor del TfG. Entonces:

1. Iniciación del proyecto. *Jefe de proyecto.*
   - *a*) Identificación de objetivos del proyecto.
   - *b*) Acta de constitución (adjudicación del proyecto).
2. Elaboración de planes:
   - *a*) Plan de riesgos. *Analista.*
   - *b*) Plan de calidad. *Analista.*
   - *c*) Plan de comunicaciones. *Analista.*
   - *d*) **Seguimiento y control.** Entregable: versión alfa de los planes. *Jefe de proyecto.*
3. Estudio Teórico Cuadrados Latinos. *Jefe de proyecto.*
4. Desarrollo del algoritmo.
   - *a*) Diseño. *Diseñador.*
   - *b*) Codificación Funciones genéricas y auxiliares. *Desarrollador.*
   - *c*) Codificación Comparticion de Secretos. *Desarrollador.*
   - *d*) Codificación Estudio Estadístico. *Desarrollador.*
   - *e*) Obtención de resultados (estudio estadístico). *Desarrollador.*
   - *f*) **Seguimiento y control.** Entregable: versión alfa. *Jefe de proyecto.*
   - *g*) Fase de pruebas. Versión beta. *Tester.*
5. Elaboración de la memoria. *Jefe de proyecto.*

a) Revisión de la memoria con el cliente (Tutor TfG).

6. Cierre del proyecto (Defensa del TfG). *Jefe de proyecto.*

5.1.1. Distribución de roles y responsabilidades

Rol	Nº	Concepto	Hora Inicio	Hora Final
Analista	1	Plan de riesgos	1,00	2,00
Analista	2	Plan de calidad	3,00	4,00
Analista	3	Plan de comunicación	5,00	6,00
Jefe de Proyecto	4	Entregable planes	7,00	7,00
Jefe de Proyecto	5	Estudio Teórico	8,00	127,00
Diseñador	10	Diseño Codificacion	128,00	147,00
Desarrollador	11	Codificación Funciones genéricas y auxiliares	148,00	199,00
Desarrollador	12	Codificación Comparticion de Secretos	200,00	204,00
Desarrollador	13	Codificación Estudio Estadístico	205,00	209,00
Desarrollador	14	Obtención de resultados (estudio estadístico)	210,00	214,00
Jefe de Proyecto	14	Entregable Codificación	215,00	215,00
Tester	15	Pruebas Codificación	216,00	230,00
Jefe de Proyecto	16	Elaboración de Memoria	231,00	290,00
Jefe de Proyecto	17	Revision Memoria con cliente	291,00	300,00
		TOTAL		300,00

Nota: Si una tarea comienza en una hora A y termina en una hora B, el comienzo será en la hora A:00:00 y el final en la hora B:59:59. Si suponemos que A es 1 y B es 2, entonces la tarea comenzaría en la hora 1:00:00 y terminaría en la hora 2:59:59, teniendo una duración de 2h.

5.1.2. Cronograma

	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
1	**Elaboración de planes**	**0,75 días**	**mar 08/02/22**	**mié 09/02/22**	
2	Plan de riesgos	2 horas	mar 08/02/22	mar 08/02/22	
3	Plan de calidad	2 horas	mar 08/02/22	mar 08/02/22	2
4	Plan de comunicaciones	2 horas	mié 09/02/22	mié 09/02/22	3
5	Entregable planes	0 horas	mié 09/02/22	mié 09/02/22	4
6	Estudio teórico	120 horas	mié 09/02/22	mié 23/03/22	5
7	**Codificación**	**12,75 días**	**mié 23/03/22**	**mié 27/04/22**	**6**
8	Diseño codificación	20 horas	mié 23/03/22	mié 30/03/22	6
9	Codificación Funciones genéricas y auxiliares	52 horas	mié 30/03/22	sáb 16/04/22	8
10	Codificación Comparticion de Secretos	5 horas	sáb 16/04/22	mar 19/04/22	9
11	Codificación Estudio Estadístico	5 horas	mar 19/04/22	mié 20/04/22	10
12	Obtención de resultados	5 horas	jue 21/04/22	vie 22/04/22	11
13	Entregable codificació	0 horas	vie 22/04/22	vie 22/04/22	12
14	Pruebas codificación	15 horas	vie 22/04/22	mié 27/04/22	13
15	Elaboración de la memo	60 horas	jue 28/04/22	mié 18/05/22	14
16	Revisión de la memoria	10 horas	jue 19/05/22	sáb 21/05/22	15
17	**Reunión Tutor TfG**	**37,63 días**	**vie 11/02/22**	**vie 27/05/22**	
34	Cierre. Defensa TfG	0 horas	vie 24/06/22	vie 24/06/22	

Figura 5.1: Tareas cronograma

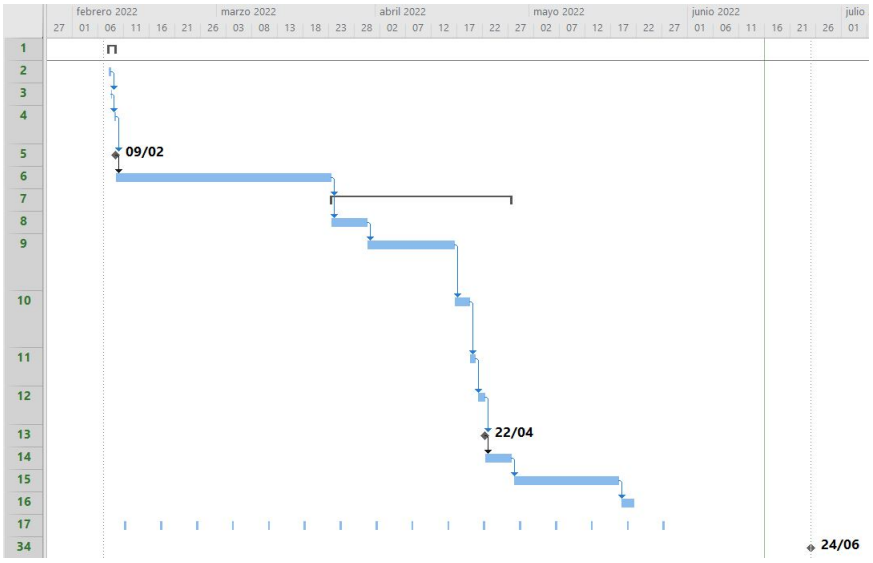


Figura 5.2: Diagrama de Gantt

Cabe destacar que se ha usado un calendario adaptado a los requisitos temporales del alumno con el objetivo de compaginar el proyecto con la continuación de sus estudios (se establece una jornada laboral de 4 horas diarias de martes a sábado, y se incluyen reuniones semanales (cada viernes) con los tutores del TfG).

5.2– Costes de desarrollo

5.2.1. Coste relativo al salario

Para llevar a cabo el cálculo de salario por horas se tienen en cuenta los salarios medios anuales entre el número de horas que se trabajan al año. Suponiendo entonces una jornada anual laboral de 1800 horas:

Rol	€/h	h	€
Jefe de Proyecto	35,43	192	6.802,56
Analista	12	6	72
Diseñador	14,72	20	294,40
Desarrollador	29,08	67	1.948,36
Tester (*)	14,79	25	1.109,25

*Como podemos comprobar, el coste relativo al Tester se triplica. Esto se debe a que las funciones de tester son llevadas a cabo por tres personas de manera simultánea (Ambos tutores del TfG y el alumno que lo realiza).

5.3– Desarrollo real del proyecto

A continuación se indica el tiempo real dedicado a cada tarea:

PROJECT - TIME ENTRY	DURATION	PERCENTAGE
TFG	302:07:00	100.0%
Estudio teórico	86:16:00	28.55%
Memoria	90:29:00	29.95%
Obtención de resultados	7:28:00	2.47%
Probar Funcionamiento	11:11:00	3.7%
Programación	97:38:00	32.32%
Revision Memoria	9:05:00	3.01%

Figura 5.3: Tiempo dedicado a cada tarea (Fuente: Toggl Track)

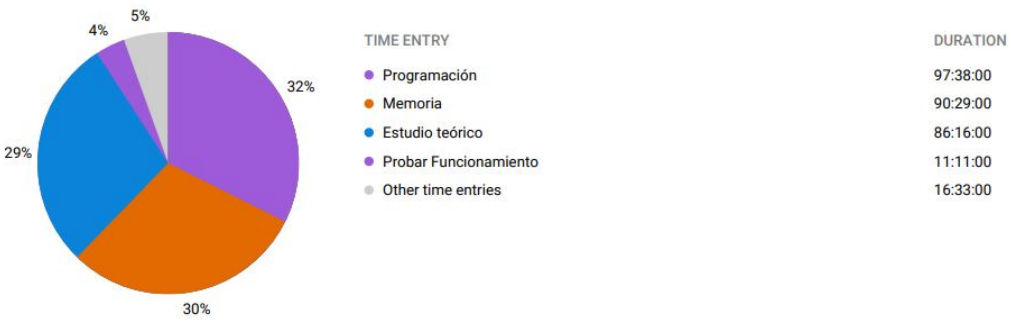


Figura 5.4: Gráfico tiempo dedicado a cada tarea (Fuente: Toggl Track)

CAPÍTULO 6

Análisis de requisitos

Una vez se ha llevado a cabo una introducción breve a los conceptos fundamentales sobre los que se sostiene el presente documento, se han mostrado las aportaciones realizadas al ambito sobre el que versa el trabajo y se ha detallado el horizonte temporal del proyecto, sería conveniente que se realizara un análisis de los requisitos. Cabe destacar que el presente proyecto no lleva a cabo el desarrollo de una aplicación como tal, sino que se desarrolla un algoritmo haciendo uso del software JUPYTER NOTEBOOKS y el lenguaje de programación PYTHON, por tanto, no existirán requisitos de interfaz o implementación.

6.1– Requisitos sobre el algoritmo

- Generar un cuadrado latino L que será usado como clave del protocolo a partir del número de participantes introducido por el usuario. Este cuadrado latino deberá ser el óptimo (mayor tamaño) entre todas las opciones disponibles para garantizar la mayor seguridad para el protocolo. En caso de existir más de una opción con el mismo nivel de seguridad, se elegirá una al azar.
- Hacer uso de técnicas relativas a operaciones con cuadrados latinos (autotopismos, isotopismos, búsqueda de órbitas) para la obtención de un Θ-conjunto crítico S aleatorio del cuadrado latino inicial, siendo Θ un autotopismo del mismo.
- Generar de manera aleatoria un isotopismo que será empleado sobre el cuadrado latino inicial para incrementar el nivel de seguridad, obteniendo un nuevo cuadrado L' isotópico al primero.
- Obtener la proyección S' de S sobre L' y el autotopismo Θ' de L', conjugado de Θ.
- Recuperar la clave L' a partir del conjunto S'.
- Eventualmente, extender el algoritmo para trabajar con cuadrados latinos de órdenes superiores.

6.2– Requisitos temporales

Se debe destacar la existencia de una limitación temporal. El proyecto debe organizarse acorde a la carga de trabajo prevista de la asignatura, en la actualidad (mientras no se modifique la correspondencia vigente entre crédito ECTS y número de horas de trabajo), 300 horas.

CAPÍTULO 7

Manual

Se incluye un archivo README.txt que resume brevemente el funcionamiento y uso de los algoritmos, y que se transcribe a continuación.

```
------------
 README.txt
------------

El presente documento pretende dar una breve explicación sobre
los algoritmos incluidos dentro del archivo:
CuadradosLatinos.ipynb. Para poder abrir el archivo se recomienda
el uso de SageMath 9.2 Notebook.

**********************
* Objetivo Principal *
**********************

El objetivo principal de este trabajo consiste en implementar un
algoritmo que permita obtener el secreto para un protocolo de
compartición de secretos basado en cuadrados latinos y sus
autotopismos, así como las posibles sombras a repartir entre los
participantes. Dicho secreto será un cuadrado latino y las
sombras se obtendrán a partir de sus Theta-conjuntos críticos,
siendo Theta un autotopismo del mismo.

Como objetivo secundario se plantea realizar un estudio
estadístico del tamaño de los Theta-conjuntos críticos de
cuadrados latinos de orden seis con el fin de aplicarlos al
sistema de compartición de secretos para mejorar su seguridad.

****************************
* Algoritmos desarrollados *
****************************

Los algoritmos principales desarrollados son dos:
```

1) comparticionSecretosMononivel(numeroDeParticipantes): Este algoritmo lleva a cabo la función propuesta en el objetivo principal explicado en la sección anterior. El único parámetro necesario que debemos introducir es el número de participantes del esquema de compartición de secretos. El algoritmo retorna diversos datos, entre los que encontramos la clave o las sombras a repartir del esquema.

2) graficaEstudioEstadístico(cuadrado, autotopismo): Este algoritmo lleva a cabo la función propuesta en el objetivo secundario explicado en la sección anterior. Los únicos parámetros que debemos introducir son el cuadrado latino y el autotopismo relativo cuyos conjuntos críticos se desean estudiar. El algoritmo retorna una gráfica donde se indicará para qué tamaños de conjunto de entradas existen conjuntos críticos de manera estadística.

****
* Recomendaciones *
****

A pesar de que el trabajo desarrollado quede resumido en estos dos algoritmos, estos se sostienen sobre diversas funciones auxiliares que recomendamos encarecidamente que lea y estudie si desea comprender verdaderamente el funcionamiento de dicho programa. Todas estas funciones tienen anotaciones en el código para facilitar su entendimiento. No obstante, si le surge cualquier duda, puede contactar con el desarrollador a través de la siguiente dirección de correo: mangonreg@alum.us.es

CAPÍTULO 8

Comparación con otras alternativas

En el presente proyecto se toman dos vertientes de trabajo: el desarrollo de un esquema de compartición de secretos y el estudio estadístico de conjuntos críticos basados en autotopismos no triviales de cuadrados latinos de orden 6.

8.1– Comparación con el esquema de compartición de secretos desearrollado por Cooper, Donovan y Seberry.

El funcionamiento básico del esquema de compartición de secretos que se propone en (Cooper y cols., 1994) se basa en la distribución de un secreto K entre una serie de participantes, permitiendo, en ciertas ocasiones, el desarrollo de esquemas multiniveles mediante la selección de varios conjuntos críticos relativos a K que compartan entradas entre sí. La ventaja principal de este método es que no se necesita reunir a todos los participantes para recuperar el secreto, sino que la tarea puede ser llevada a cabo por diversos conjuntos de participantes, todos ellos incluidos en la estructura de acceso. Este hecho permite la posibilidad sustituir algunos participantes por otros, pero nunca uno cualquiera por otro cualquiera.

En la propuesta que se ha presentado a lo largo de este trabajo, se lleva a cabo un procedimiento similar, sin embargo, se aprovechan las propiedades de los cuadrados latinos y sus atotopismos para dificultar la obtención de la clave a terceros no implicados en el esquema. Para ello se busca un θ-conjunto crítico basado en un autotopismo relativo a un cuadrado latino previamente definido y se aplica un isotopismo aleatorio para transformar el cuadrado latino y el θ-conjunto crítico. Las entradas de dicho conjunto crítico transformado se repartirán como sombras a los participantes del esquema.

En lo referente a plantear un esquema de compartición de secretos con el algoritmo desarrollado, debemos tener en cuenta dos puntos:

1. Por una parte, si consideramos un esquema de compartición de secretos básico, se reparten tantas sombras como participantes haya, requiriéndolos a todos para poder obtener la clave (Tipo 1). En este caso, aquellos participantes cuya sombra derive en una órbita más larga tienen más información que aquellos que presenten órbitas menores, y por tanto, podrían ser considerados de una jerarquía superior (Tipo 2).

2. Por otra parte, si consideramos un esquema de compartición de secretos con sustitutos (Tipo 3), se puede crear un conjunto de sombras que consistiría en un conjunto crítico, cuyo tamaño coincida con el número de participantes, al que se le añadiría algún elemento más de las órbitas implicadas en dicho conjunto. Eso permitiría tener sustitutos para los participantes del esquema. De esta manera existirían varios conjuntos válidos para la recuperación

del secreto, similar al esquema que proponen en el artículo, pero sin la necesidad de tener que buscar Θ-conjuntos críticos que compartan elementos.

Además, en el caso de que alguna de las órbitas obtenidas sea de un único elemento, el participante que reciba esa sombra sería imprescindible. Esto permite hacer un sistema multinivel primitivo, de tal manera que la persona que reciba esa sombra será insustituible y, por tanto, de un nivel jerárquico superior a los demás. Si se quiere evitar que haya una persona insustituible, entonces se debe evitar tener elementos relativos a órbitas triviales dentro del conjunto de sombras (o bien, dar a dos personas esa misma entrada).

Además, este algoritmo tiene la capacidad de reducir la complejidad en la búsqueda de conjuntos críticos para un cuadrado latino dado. Esto se debe a que, cuando comprobamos si el cuadrado parcial, formado por el conjunto que se está estudiando, es únicamente completable, estamos haciendo uso de un autotopismo, es decir, cada una de las entradas relativas a dicho conjunto formará parte de una órbita distinta. Al incluir estas órbitas en dicho cuadrado parcial, el número de entradas vacías, y por tanto de suposiciones que habrá que hacer, se reducirá.

Por último, cabe destacar que este algoritmo es aplicable a cualquier tamaño de conjunto de participantes, siempre y cuando se conozcan conjuntos críticos de dicho tamaño para algún orden de cuadrados latinos.

A continuación se incluye un resumen de la comparativa:

	Esquema Cooper and cols.	Esquema propuesto
Admite esquema mononivel (Tipo 1)	Sí	Sí
Admite esquema multinivel (Tipo 2)	Sí	Sí
Admite sustituto de participantes (Tipo 3)	Sí	Sí
Requiere un único conjunto crítico para esquemas Tipo 2 y 3	No	Sí

Cuadro 8.1: Comparativa entre protocolos de compartición de secretos

8.2– Comparación con estudios de conjuntos críticos basados en autotopismos no triviales de cuadrados latinos.

Como ya se mencionó en diversos apartados del trabajo, hasta el momento sólo se conocen los tamaños para los críticos basados en autotopismos no triviales de cuadrados latinos de orden igual o inferior a cinco (Falcón y cols., 2020). Por tanto, no es posible realizar una comparativa con el estudio estadístico realizado con cuadrados latinos de orden seis, pues no hay nada al respecto en bibliografía. Actualmente este es un problema abierto.

CAPÍTULO 9

Plan de Riesgos

9.1– Identificación de riesgos

Podemos citar como riesgos potenciales:

1. Retrasos eventuales que puedan producirse debido a la compatibilidad entre el proyecto y el desarrollo de los estudios de grado.
2. Aparición de diversas dificultades a la hora de implementar alguna parte del código.
3. Posible saturación de los recursos del sistema en el que se está ejecutando la aplicación. Recordemos que trabajamos con operaciones sobre matrices que, en determinados casos, pueden derivar en un alto consumo de dichos recursos.

9.2– Planes de contingencia

Atendiendo a los posibles problemas que pueden surgir, podríamos recurrir a las siguientes medidas:

1. En caso de producirse retrasos eventuales podemos llevar a cabo una reorganización del cronograma si existiese holgura con respecto a la fecha límite de la entrega.
2. Si nos encontramos ante ciertos problemas de implementación debido al desconocimiento de las técnicas que se pueden emplear, podemos llevar a cabo consultas, tanto en internet, como en libros o a profesionales en el ámbito.
3. En caso potencial saturación, podemos llevar a cabo una mezcla de los dos enunciados anteriores, si hay holgura presente con respecto a la fecha de entrega, siempre podemos volver a revisar el código para buscar una solución cuya complejidad sea inferior a la actual y, por tanto, se consuman menos recursos. La búsqueda de esta nueva solución puede realizarse en internet, libros o consultando a profesionales.

CAPÍTULO 10

Plan de Calidad

10.1– Indicadores

Los indicadores de calidad, en general, están asociados a la satisfacción que el producto genera en el público. Como ejemplos de indicadores de calidad podemos destacar los siguientes:

1. Cobertura: En la actualidad, la mayoría de los usuarios que hacían uso de un ordenador de sobremesa, tienen un sistema compatible con Jupyter Notebook

2. Eficacia: La eficacia se define como la relación entre la disponibilidad de un producto y la necesidad para la que ha sido creado. Debemos recordar que nuestra aplicación estaba destinada para llevar a cabo una función muy específica, la cual se basaba en encontrar aquellos conjuntos críticos de un determinado cuadrado latino de tal manera que estos conjuntos críticos pudiesen ser repartidos entre diversos usuarios para ser empleados en un protocolo de compartición de secretos. Podemos intuir, por tanto, que la eficacia será alta, aunque será necesario llevar a cabo encuestas dirigidas a nuestro público objetivo.

3. Competencia: En el mercado no suelen ser abundantes las herramientas de este tipo, por lo que nuestro producto puede llegar a más usuarios.

4. Por último, y no por ello menos importante, podemos citar la validación de los requisitos iniciales propuestos por el cliente. Son una fuente fiable del grado de satisfacción con el producto y por tanto de la calidad del mismo.

10.2– Plan de mejora

Un plan de mejora se trata del conjunto de acciones que se realizan sobre un proyecto con el objetivo de incrementar la calidad y el rendimiento de los resultados.

A la hora de llevar a cabo un plan de mejora debemos tener claros nuestros objetivos, evaluar periódicamente los resultados obtenidos, simplificar los procesos, etc. Pero en nuestro caso, no debemos olvidar que nos encontramos ante un Trabajo fin de Grado, por lo que el punto más importante a tener en cuenta para el proceso de mejora continua es atender a los análisis y feedback proporcionados por los testers, es decir, los tutores del TfG.

CAPÍTULO 11

Plan de Comunicaciones

El plan de comunicaciones se compone de una serie de reuniones entre los tutores del TfG y el alumno. Estas reuniones se realizarán de forma semanal (o cada 10 días) en caso de no producirse ningún incidente que requiera que ambas partes se encuentren antes de lo previsto.

CAPÍTULO 12

Conclusiones y desarrollos futuros

Como se ha mostrado en el desarrollo de esta memoria, el trabajo presentado consta de dos partes diferenciadas, pero a la vez íntimamente relacionadas por cómo se complementan entre sí.

En primer lugar, se ha desarrollado un protocolo criptográfico de compartición de secretos basado en cuadrados latinos. Lo que hace diferente a este esquema respecto a los conocidos hasta el momento es que las sombras a repartir serán los elementos de un conjunto crítico de entradas asociadas a un autotopismo correspondiente al cuadrado latino que servirá de secreto.

Después de todo lo expuesto a lo largo de los distintos capitulos de este trabajo, nos atreveríamos a decir que el algoritmo de compartición de secretos desarrollado parece acertado para el esquema propuesto en (Cooper y cols., 1994).

Por una parte , reduce la complejidad a la hora de buscar conjuntos críticos para un cuadrado latino dado, al incluir un autotopismo que determina las órbitas de las entradas que conforman dicho conjunto y, por tanto, reduce el número de suposiciones que se deben de hacer para el resto de entradas vacías.

Por otra parte, permite el uso de esquemas de compartición de secretos multinivel sin necesidad de emplear más de un conjunto crítico. Esto se debe a que el uso de las órbitas de los elementos relativos al conjunto mencionado, nos permite asignar entradas relativas a órbitas más largas (mayor información) a personas con mayor rango, o bien, reducir el número de entradas que se reparten para asignar entradas redundantes a los sustitutos de los participantes.

Además, hemos podido llevar a cabo un estudio estadístico para desarrollar una aproximación a los tamaños de los conjuntos críticos basados en autotopismos no triviales de cuadrados latinos de orden seis, comprobando su bondad mediante la comparación de la salida del algoritmo con los resultados de algunos ejemplos desarrollados en el artículo (Falcón y cols., 2020). Esto no sólo nos ha permitido verificar el correcto funcionamiento del algoritmo sino que nos ha mostrado un error que existía en uno de los ejemplos del ya mencionado artículo.

De cualquier modo, ha de quedar claro que este trabajo se ha desarrollado en un entorno poco conocido y del que queda mucho por investigar. Algunas de las cuestiones que no hemos trabajado hasta ahora pero que pretendemos abordar en un futuro próximo son:

1. Aplicar el estudio estadístico para conocer aproximaciones a tamaños de conjuntos críticos basados en autotopismos no triviales de cuadrados latinos de órdenes superiores a seis.

2. Llevar a cabo un estudio teórico de casos para conocer exhaustivamente el número de conjuntos críticos basados en autotopismos no triviales de cuadrados latinos de órden seis y superiores, y sus respectivos tamaños.

3. En cuanto al ámbito criptográfico, realizar un estudio sobre cómo los participantes de un esquema de compartición de secretos llevan a cabo la difusión de las sombras que se les otorgan. Para ello se prevé el uso de grafos generalizados de Cayley que, basados en cuasigrupos en lugar de grupos, describan la red de comunicación entre los participantes. También se prevé el uso del coloreado dinámico de dichos grafos, que posibilitara un reparto justo de sombras entre los participantes.

Referencias

Adams, P., Bean, R., y Khodkar, A. (2003, 08). A census of critical sets in the latin squares of order at most six. *Ars Combinatoria*, *68*.

al Buni, A. (1980). *Shams al-ma'arif al-kubra wa-lataíf al-'awarif*. al-Maktabat al-Sha'biyah. Descargado de https://books.google.es/books?id=eSclwAEACAAJ

Ashwini, P., Venkaiah, V. C., y Bhukya, W. N. (2021). Secret sharing scheme based on latin squares. *Journal of Discrete Mathematical Sciences and Cryptography*, *0*(0), 1-15. Descargado de https://doi.org/10.1080/09720529.2021.1925447 doi: 10.1080/09720529.2021.1925447

Blakley, G. R. (1979). Safeguarding cryptographic keys. *1979 International Workshop on Managing Requirements Knowledge (MARK)*, 313-318.

Bose, R., Parker, E., y Shrikhande, S. (1960). Further results on the construction of mutually orthogonal latin squares and the falsity of euler's conjecture. *Canadian Journal of Mathematics*, *12*, 189–203.

Cooper, J., Donovan, D., y Seberry, J. (1994). Secret sharing schemes arising from latin squares. *Bull. Inst. Combin. Appl.*, *12*, 33–43.

Curran, D., y Van Rees, G. H. J. (1979). Critical sets in Latin squares. En *Proceedings of the Eighth Manitoba Conference on Numerical Mathematics and Computing (Univ. Manitoba, Winnipeg, Man., 1978)* (pp. 165–168). Utilitas Math., Winnipeg, Man.

Falcón, R. M. (2006). Latin squares associated to principal autotopisms of long cycles. application in cryptography. *Proceedings of Transgressive Computing 2006: a conference in honor of Jean Della Dora.*, 213–230.

Falcón, R. M. (2011). The set of autotopisms of partial latin squares. *Discrete Math.*, *313*, 1150–1161.

Falcón, R. M., Johnson, L., y Perkins, S. (2020). A census of critical sets based on non-trivial autotopisms of latin squares of order up to five. *AIMS Math.*, *6*, 261–295.

Hulpke, A., Kaski, P., y Östergård, P. (2011). The number of Latin squares of order 11. *J. Math. Comp.*, *80*, 1197–1219.

Ibáñez, P. (2015). *Cuadrados latinos, matemáticas y arte abstracto.* Cuaderno de Cultura Científica. Descargado de https://culturacientifica.com/2015/01/14/cuadrados-latinos-matematicas-y-arte-abstracto/

Kolesova, G., Lam, C. W. H., y Thiel, L. (1990). On the number of 8×8 Latin squares. *J. Combin. Theory Ser. A*, *54*(1), 143–148.

McKay, B. D., Meynert, A., y Myrvold, W. (2007). Small Latin squares, quasigroups, and loops. *J. Combin. Des.*, *15*(2), 98–119.

Nelder, J. (1977). Critical sets in latin squares. *J. Combin. Des.*.

Shamir, A. (1979, nov). How to share a secret. *Commun. ACM*, *22*(11), 612–613. Descargado de https://doi.org/10.1145/359168.359176 doi: 10.1145/359168.359176

Smetaniuk, B. (1979). On the minimal critical set of a Latin square. *Utilitas Math.*, *16*, 97–100.

Stones, R., Su, M., Liu, X., Wang, G., y Lin, S. (2015, 08). A latin square autotopism secret sharing scheme. *Designs, Codes and Cryptography*, *80*. doi: 10.1007/s10623-015-0123-1

Villar, J. L. (2017). *Informe esamcid sobre estructuras de acceso.* Universidad Politécnica de Cataluña. Descargado de `https://web.mat.upc.edu/jorge.villar/esamcid/rep/accs/reportaccessse2.html`