Universidad de Cantabria

Facultad de Ciencias

Una mirada matemática al cubo de Rubik
(A mathematical view of the Rubik cube)

Trabajo de Fin de Grado
para acceder al

GRADO EN MATEMÁTICAS

Autor: Joseba Martínez Arrizabalaga

Director: Mónica Blanco Gómez

Septiembre - 2024

UNIVERSIDAD DE CANTABRIA

Resumen

Una mirada matemática al cubo de Rubik

En este trabajo se estudia el cubo de Rubik con una perspectiva matemática. Para ello se introduce la notación de Singmaster que permite describir cualquier cubo independiente a los colores del mismo, describir el movimiento de los cubiletes al rotar las caras del cubo y con ello establecer la estructura de grupo del conjunto de todas los operaciones sobre el cubo de Rubik. Así hemos llegado al primer teorema fundamental del cubo de Rubik, que da condiciones necesarias y suficientes para que una colocación aleatoria de los cubiletes de una configuración se pueda resolver sin necesidad de desmontar el cubo. Este resultado nos permitirá, entre otras, determinar el cardinal del grupo del cubo de Rubik, el número de configuraciones y llegar al segundo teorema fundamental, que da condiciones necesarias y suficientes para que exista una secuencia de giros de las caras del cubo que transforme una configuración inicial dada en otra final. Terminaremos con la primera cota para el Número de Dios, que es el máximo número de giros necesarios para resolver cualquier cubo.

Palabras clave: Cubo de Rubik, Teoría de Grupos, Teoría de Grafos, Combinatoria.

A mathematical view of the Rubik cube

In this work we analyse the Rubik cube from a mathematical point of view. For this we have introduced Singmaster's notation, which allows to describe any Rubik cube regardless of the choice of colors. This also allows to describe the movement of the cubicles when we rotate any of the faces of the cube, and stablish a group structure of the set of all moves on the Rubik cube. Thereafter, we introduce the first fundamental theorem of the Rubik cube, which gives necesary and suficient conditions to claim whether a cube, whose cubicles have been randomly assambled, can be solved rotating its faces. Then, we are able to introduce further results, as the cardinality of the Rubik's cube group and the second fundamental theorem, which gives necessary and suficient conditions for a given move to exist. Finally, we go over the God's Number, that gives the minimum number of moves that allows to solve any cube.

Keywords: Rubik Cube, Group Theory, Graph theory, Combinatorics.

Agradecimientos

Dado que ya he aprovechado otros trabajos para gradecer el apoyo de la gente que he tenido alrededor desde que empecé la universidad, quiero centrar estos agradecimientos a Mónica por todo el tiempo dedicado en revisar, repensar y hacerme reescribir partes de este trabajo, con el cual cierro mi etapa como estudiante del doble grado de física y matemáticas en la UC.

Índice general

1. Introducción **1**
1.1. Motivación 1
1.2. Conceptos preliminares 2

2. Cubo de Rubik como objeto matemático **7**
2.1. Cubículos y cubiletes 8
2.2. Movimientos y coloraciones del cubo de Rubik 9
2.3. Operaciones sobre el cubo de Rubik 11
2.4. Longitudes de palabras y operaciones en el cubo 12

3. Configuraciones del cubo de Rubik **15**
3.1. Notación de Singmaster 15
3.2. Operaciones vistas como permutaciones 18
3.3. Configuraciones - Notación Christoph Bandelow 19
3.4. Operaciones – notación de Bandelow 23

4. Grupo del Cubo de Rubik **27**
4.1. El conjunto Rc_3 de operaciones sobre el cubo de Rubik es un grupo . . 27
4.2. Grupo Two-Squares 28
4.3. Acción del grupo de Cubo de Rubik sobre $\mathcal{S}$ 30

5. Teorema Fundamental del Cubo de Rubik **33**
5.1. Primer teorema en teoría del Cubo 33
5.2. Algunos resultados útiles 34
5.3. Resolviendo el cubo en 4 etapas 35

6. El Algoritmo de Dios y el Cubo de Rubik **41**
6.1. Grafo de Cayley del Cubo de Rubik 41
6.2. El Número de Dios en la métrica de media vuelta 42
6.2.1. Primeras cotas al Número de Dios 42
6.2.2. El valor definitivo 43
6.2.3. El algoritmo de búsqueda de soluciones 45
6.3. Secuencias canónicas 46

Bibliografía **49**

A. Operaciones empleadas en el trabajo **51**

Capítulo 1

Introducción

1.1. Motivación

El cubo de Rubik es probablemente el puzzle más popular jamás vendido. Fue inventado en 1974 por Ernö Rubik, y desde su salida al mercado ganó una gran popularidad, vendiéndose hasta 350 millones de unidades para el año 1980. En 1981, el matemático estadounidense, David Singmaster publicó *Notes on Rubik's Magic Cube'* [11], el primer análisis del cubo de Rubik, en el que daba un algoritmo para resolverlo.

Cuando este puzzle de combinación fue introducido al público, los esfuerzos se centraron principalmente en resolverlo. En la actualidad, el cubo de Rubik sigue siendo un objeto de gran popularidad, aunque el enfoque sobre el mismo ha cambiado: por un lado existen las llamadas competiciones de Speed-cubing, que consisten en resolver cubo de Rubik mezclados de forma aleatoria en el menor tiempo posible siendo el record establecido el 14 de junio de 2023 de 3.134 segundos [8]; por otro lado, también existe interés en encontrar el menor número de movimientos posibles para resolver cualquier configuración del cubo de Rubik. A este número se le conoce en el entorno del cubo de Rubik como el "Número de Dios". La respuesta a esta última pregunta se resolvió en 2010, y se determinó que el Número de Dios es 20, lo cual quiere decir que se puede resolver el cubo de Rubik, cualquiera que sea la configuración inicial, en 20 pasos o menos. El Número de Dios tan solo acota el número mínimo de movimientos para resolver cualquier cubo, sin embargo, todavía no se conoce el algoritmo que genere ese camino mínimo. Por lo tanto, los esfuerzos actuales se centran en encontrar esa secuencia de 20 movimientos o menos.

El cubo de Rubik se ha estudiado desde diferentes áreas del conocimiento, como la informática, la ingeniería y las matemáticas. De hecho, en matemáticas se puede describir el cubo de Rubik mediante la teoría de grupos, de forma que las diferentes transformaciones y configuraciones del cubo forman un subgrupo del grupo de permutaciones generado por las diferentes rotaciones de las caras del cubo. Además, la teoría de grupos permite comprender el funcionamiento del cubo.

En este trabajo, introduciremos la notación necesaria para describir las diferentes configuraciones del cubo de Rubik y cómo las rotaciones de las caras afectan a dichas configuraciones. Además, se mostrarán algunos resultados sobre el cubo de Rubik que permitirán dar la demostración del teorema fundamental del cubo de Rubik, un teorema de vital importancia en este campo, no por su complejidad, sino por su impacto en la teoría del cubo de Rubik, ya que permite conocer qué colocación de las pegatinas del cubo de Rubik se puede alcanzar mediante alguna secuencia de giros de las caras del cubo.

Las figuras o esquemas del cubo de Rubik incluidas en este trabajo son de creación propia. Éstas han sido generadas empleando el paquete `tikz` que permite generar dibujos, el paquete `rubikcube` que dentro de `tikz` permite dibujar el esquema de un cubo de Rubik y `rubikrotation` que permite generar nuevas configuraciones del cubo de Rubik, introduciendo una secuencia de rotaciones de las caras del cubo de Rubik.

1.2. Conceptos preliminares

En esta sección introduciremos los conceptos matemáticos necesarios para desarrollar la teoría del cubo de Rubik. Dirigimos al lector a [7] para un mayor detalle de los conceptos de álgebra de esta sección y [10], Capítulo 11 para conceptos de grafos y algoritmos de búsqueda.

Empezaremos por dar una definición precisa del concepto intuitivo *cara de un cubo*, que nos servirá para referirnos a diferentes partes que conforman al cubo. En efecto, en el contexto de politopos, se definen las caras de un politopo [2] de la forma siguiente.

Definición 1.1 (Politopo)**.**
Un politopo es la envoltura convexa de un conjunto finito de puntos.

Definición 1.2 (Cara)**.**
Una cara de un politopo P es la intersección de P con un hiperplano de soporte H. Un hiperplano de soporte es aquel que divide el espacio en dos semiespacios, y es tal que P está completamente contenido en alguno de esos dos semiespacios cerrados y tal que $H \cap P \neq \emptyset$.

De acuerdo a la Definición 1.2, los conjuntos $\emptyset$ y C son ambas caras de C, llamadas *caras impropias*. El resto de las caras de C son caras propias. Con la definición dada, las aristas que unen los vértices de un cubo también son caras del mismo. Por otro lado, también existe el concepto de faceta de un politopo.

Definición 1.3 (Faceta)**.**
Se llama faceta de un politopo de dimensión n a una cara de dimensión $n-1$ del mismo.

Sin embargo, la teoría de politopos no es necesaria para desarrollar la teoría del cubo de Rubik y dado que el concepto de faceta no es necesariamente conocido por los lectores de este texto, haremos un abuso de notación y llamaremos *cara del cubo* a las facetas que lo conforman.

Definición 1.4 (Cara de un cubo)**.**
Llamamos cara de un cubo a cada una de las 6 facetas del politopo que define dicho cubo.

Otro concepto que se manejará durante el trabajo es el de grupo.

Definición 1.5 (Grupo)**.**
Un grupo es un par $(G, *)$, donde G es un conjunto no vacío y $*$ es una aplicación

$$\begin{aligned} * : \ & G \times G \to G \\ & (a, b) \mapsto a * b, \end{aligned}$$

donde $G \times G = \{(x, y) : x, y \in G\}$ es el producto cartesiano de G consigo mismo y además verifica las siguientes propiedades:

- Propiedad asociativa: $(x * y) * z = x * (y * z)$, $\forall x, y, z \in G$.
- Existencia de Elemento Neutro: $\exists\, e \in G$ tal que $e * x = x * e = x$, $\forall x \in G$.
- Existencia de inverso: para todo $x \in G$, $\exists x' \in G$ tal que $x * x' = x' * x = e_G$, donde e_G es el elemento neutro de G.

Definición 1.6 (Grupo abeliano)**.**
G se dice grupo abeliano si es grupo y además $a \cdot b = b \cdot a$ para todo $a, b \in G$. En caso contrario se dice no abeliano.

A partir de este, surge la necesidad de introducir la definición de subgrupo.

Definición 1.7 (Subgrupo)**.**
Dado $(G, \cdot)$ un grupo, un subgrupo de G es un subconjunto no vacío $H \subseteq G$ que a su vez es grupo.

Definición 1.8 (Clase lateral)**.**
Dado G un grupo y S un subgrupo de G, dado un elemento $g \in G$, llamamos

- $gH = \{gh : h \in H\}$ es una clase lateral a izquierda de H en G.
- $Hg = \{hg : h \in H\}$ es una clase lateral a derecha de H en G.

Definición 1.9 (Grupo generado por X)**.**
Sea $(G, \cdot)$ un grupo y X un subconjunto no vacío de G. Llamamos subgrupo generado por X a la intersección de todos los subgrupos de G que contienen a X, lo denotamos por $\langle X \rangle$, i.e.,

$$\langle X \rangle := \bigcap_{X \subseteq H, H \text{subgrupo de } G} H.$$

La siguiente proposición caracteriza los elementos de un subgrupo generado.

Proposición 1.2.1.
Sea $(G, \cdot)$ un grupo y X un subconjunto no vacío de G, entonces $\langle X \rangle$ está formado por los productos de los elementos de X y sus inversos, es decir,

$$\langle X \rangle = \{x_1^{e_1} x_2^{e_2} \cdots x_r^{e_r} : r \in \mathbb{N},\, x_i \in X,\, e_i \in \{1, -1\}\}$$

Existe un conjunto especial de grupos que se llama grupo cíclico

Definición 1.10 (Grupo cíclico)**.**
Un grupo $(G, \cdot)$ es cíclico si está generado por un solo elemento, es decir, G es cíclico si y solo si existe $a \in G$ tal que $G = \langle a \rangle$

Otro concepto que surgirá de forma natural al estudiar el cubo de Rubik es el de permutación.

Definición 1.11 (Permutación)**.**
Sea X un conjunto no vacío, llamamos permutación a toda aplicación biyectiva $\sigma : X \to X$.

Definición 1.12 (Grupo de permutaciones)**.**
Sea X un conjunto no vacío. El conjunto de permutaciones de X con la composición

de aplicaciones como operación es un grupo y se denomina grupo de permutaciones de X, $(S(X), \circ)$ donde

$$S(X) := \{\sigma : X \to X : \sigma \text{ es biyectiva}\}$$

Definición 1.13 (Grupo simétrico)**.**
Sea X_n un conjunto finito con $n \in \mathbb{N}$ elementos. Podemos denotar sus elementos por $1, 2, ..., n$, es decir, $X_n = \{1, 2, ..., n\}$. En este caso el grupo de permutaciones de X_n, se denomina grupo simétrico y el conjunto de permutaciones se denota por S_n.

Definición 1.14 (Permutaciones, Ciclos y Trasposiciones)**.**
Sean $i_1, i_2, ..., i_l$ elementos de X_n distintos dos a dos. Se representa por $(i_1, i_2, ..., i_l)$ a la permutación que aplica

$$i_1 \to i_2, \qquad i_2 \to i_3, \qquad ....., \qquad i_l \to i_1,$$

y que deja fijos los elementos de $X_n \setminus \{i_1, ..., i_l\}$. Diremos que este tipo de permutación son ciclos de longitud l. Los ciclos de longitud 2 se denominan transposiciones.

Otro resultado relevante es el de la descomposición de una permutación en transposiciones.

Teorema 1.2.2.
Toda permutación de S_n con $n \geq 2$ se puede expresar como composición de transposiciones (no necesariamente disjuntas ni de manera única).

Teorema 1.2.3.
Sea $\sigma \in S_n$ una permutación y $\tau_1, ..., \tau_r, \tilde{\tau}_1, ..., \tilde{\tau}_s \in S_n$ transposiciones. Si se cumple que

$$\sigma = \tau_1 \cdots \tau_r = \tilde{\tau}_1 \cdots \tilde{\tau}_s$$

Entonces r y s tienen la misma paridad, es decir, ambos números son pares o ambos son impares.

Definición 1.15 (Permutaciones pares e impares)**.**
Sea $\sigma \in S_n$ una permutación. Si σ descompone en un número par de transposiciones, decimos que σ es una permutación par y si σ descompone en un número impar de transposiciones, decimos que σ es una permutación impar. Definimos el índice de una permutación como:

$$i(\sigma) = \begin{cases} 1 & \text{si } \sigma \quad \text{es par} \\ -1 & \text{si } \sigma \quad \text{es impar} \end{cases}$$

Definición 1.16 (Grupo Alternado A_n)**.**
Se llama grupo alternado de n elementos al subgrupo de las permutaciones pares de S_n.

Un concepto ligado al de grupo es el de acción de un grupo sobre un conjunto. Este será útil porque los giros de las caras del cubo de Rubik y sus combinaciones tendrán un efecto sobre el conjunto de las configuraciones del cubo, que será en efecto una acción de grupo.

Definición 1.17 (Acción de un grupo sobre un conjunto)**.**
Una acción de un grupo G sobre un conjunto X es una función $\cdot : G \times X \to X$ (denotada como $g \cdot x$ para $g \in G$ y $x \in X$) que satisface las siguientes dos propiedades:

1. **Propiedad de identidad:** Para todo $x \in X$, $e \cdot x = x$, donde e es el elemento neutro de G.
2. **Propiedad de asociativa:** Para todos $g, h \in G$ y $x \in X$, $(gh) \cdot x = g \cdot (h \cdot x)$.

En este trabajo veremos también que podemos observar el cubo de Rubik como un grafo. Dicho grafo será un grafo de Cayley que definimos a continuación.

Definición 1.18 (Grafo de Cayley de un grupo)**.**
Dado G un grupo, y $S \subseteq G$ un subconjunto cerrado por inversos (si $s \in S$ entonces $s^{-1} \in S$), el grafo de Cayley de este grupo es aquel cuyos vértices son los elementos de G y dos vértices $x, y \in G$ están conectados por una arista si $x^{-1}y \in S$.

Otro concepto importante en el contexto de grafos que se usará en el trabajo es el de distancia entre dos vértices y diámetro.

Definición 1.19 (Distancia entre vértices)**.**
La distancia entre dos vértices de un grafo es el número de aristas del camino más corto entre ellos. Si los vértices nos son accesibles a través de un camino, entonces la distancia es infinita.

Definición 1.20 (Diámetro de un grafo)**.**
El diámetro de un grafo es la distancia máxima entre cualesquiera dos vértices.

Dado un árbol, podemos explorar todos sus vértices a través del algoritmo de búsqueda en profundidad. Dicho árbol será un grafo G conexo, cuyo conjunto de vértices denotamos por V y las aristas por E.

Entrada: Grafo $G = (V, E)$, nodo inicial s
Resultado: Nodos visitados en el grafo
para *cada vértice* $u \in V$ **hacer**
  visitado$[u] \leftarrow$ falso;
fin
`DFS-Visitar(`s`);`
procedimiento `DFS-Visitar(`u`)`**:**
  visitado$[u] \leftarrow$ verdadero;
  para *cada v adyacente a u* **hacer**
    si *visitado*$[v] =$ *falso* **entonces**
      `DFS-Visitar(`v`);`
    fin
  fin
fin

Algoritmo 1: Búsqueda en Profundidad (DFS)

Relacionado con esto definiremos el método de búsqueda en una profundidad dada.

Definición 1.21 (Búsqueda en profundidad d)**.**
El método de búsqueda en profundidad d, es el método de explorar en profundidad restringido al árbol con vértices a distancia menor o igual que d de la raíz.

Capítulo 2

Cubo de Rubik como objeto matemático

El cubo de Rubik original es un cubo con 6 caras, cada una de las cuales se divide en una malla 3×3 con 9 pegatinas de colores. El cubo de Rubik consiste de 26 pequeños subcubos (el centro o núcleo del cubo no se considera). Cada una de estas 26 piezas tiene una parte oculta que apunta hacia el interior del cubo y que se ensambla con las piezas de su entorno. Por otro lado, la pieza central de cada cara está fija al núcleo del cubo, de forma que sólo puede rotar sobre sí misma, lo que permite al resto de las piezas encajadas a su alrededor rotar, trasladando los subcubos a nuevas posiciones.

En la Figura 2.1 se muestra a la izquierda una ilustración del cubo de Rubik donde las pegatinas de cada cara tienen todas el mismo color y a su derecha el cubo obtenido mediante una cierta secuencia de rotaciones de las caras del mismo.

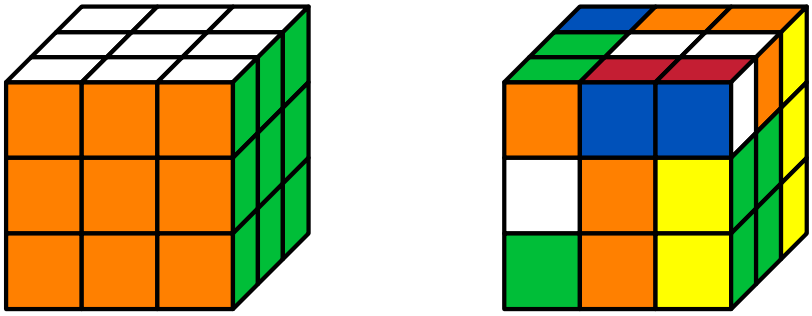

FIGURA 2.1: Dos ilustraciones del cubo de Rubik. A la izquierda el cubo de Rubik resuelto, a la derecha el cubo obtenido mediante una cierta secuencia de rotaciones de las caras del cubo.

El objetivo del cubo de Rubik es el siguiente: partiendo del cubo de Rubik resuelto, donde cada cara tiene un sólo color, se desordenan sus piezas mediante una secuencia aleatoria de giros de sus caras y que será desconocida para el jugador. Una vez ahí, el jugador debe encontrar una secuencia de giros que resuelva el cubo, es decir, que cada cara tenga un único color.

Existen además múltiples variaciones del cubo de Rubik original, así como cubos de Rubik 2×2, 7×7, Megaminx [14], Pyraminx [13].

2.1. Cubículos y cubiletes

Para poder describir el cubo de Rubik y hablar de sus distintos elementos, es útil introducir los conceptos de cubilete y cubículo traducidos de los términos *cubie* y *cubicle* empleados por David Singmaster [11], quién publicó en 1979 el primer análisis matemático del cubo de Rubik y cuya notación es empleada de forma general por el resto de autores.

Definición 2.1 (Cubilete y Cubículo)**.**

- Llamaremos *cubilete* a cada uno de los 26 subcubos que conforman la parte visible del cubo de Rubik
- Llamaremos *cubículo* a las posiciones en el espacio ocupadas por los 26 cubiletes.

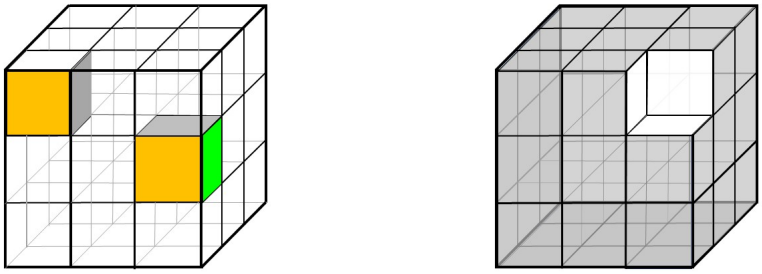

FIGURA 2.2: En la figura de la izquierda se resaltan dos ejemplos de cubiletes: el cubilete en la parte superior izquierda del cubo y el cubilete en la parte del frente, derecha. En la figura de la derecha se muestra un hueco que es un cubículo del cubo de Rubik.

Los cubículos son posiciones espaciales que se mantienen fijas al rotar las caras del cubo, por lo que establecen un marco de referencia. De esta forma, al aplicar un giro sobre una de las caras del cubo, los cubículos no cambian de posición mientras que los cubiletes pasarán a ocupar nuevos cubículos.

No todos los cubiletes y cubículos del cubo de Rubik son iguales, de hecho, distinguimos tres tipos que definiremos como *cubilete (ó cubículo)* esquina, borde y centro traducidos de los términos *corner*, *edge* y *center* empleados por Singmaster.

Definición 2.2 (Cubiletes y Cubículos Esquina, Borde y Centro)**.**

- Se llama cubilete esquina al cubilete con tres caras visibles. Un cubo de Rubik tiene 8 cubiletes esquina. Los cubículos esquina serán los cubículos ocupados por los cubiletes esquina.
- Se llama cubilete borde a los que tienen 2 caras visibles. El cubo de Rubik tiene 12 cubiletes borde. Los cubículos borde serán los ocupados por los cubiletes borde.
- Se llama cubilete centro a los que sólo tienen una cara visible. Hay 6 de estos, uno por cada cara del cubo. Los cubículos centro son los ocupados por los cubiletes centro.

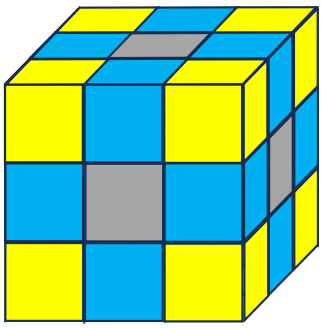

FIGURA 2.3: Cubículos borde en azul, esquina en amarillo y cubículos centro en gris.

2.2. Movimientos y coloraciones del cubo de Rubik

Las únicas operaciones posibles sobre el cubo de Rubik para variar la posición de los cubiletes son las rotaciones de las 6 caras del cubo. Existen operaciones aparentemente diferentes, como la rotación de una sección central, ó la sección central junto a una cara paralela, sin embargo, estas siempre se pueden descomponer como rotaciones de algunas de las 6 caras seguidas de rotaciones del cubo completo. Por ende, se trabajará solamente con rotaciones de las 6 caras sin considerar rotaciones del cubo completo si no se especifica lo contrario. En la Figura 2.4 se muestra un giro de la cara superior.

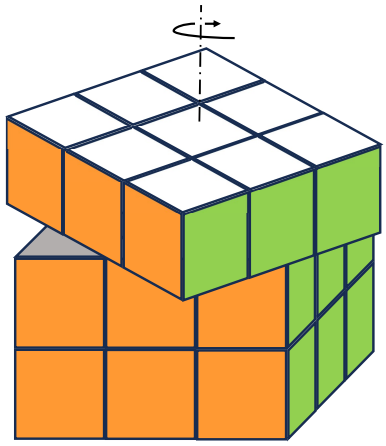

FIGURA 2.4: Giro de la cara superior del cubo. Los cubiletes centrales quedan fijos.

El hecho de trabajar sin rotar el cubo completo, permite con facilidad llegar a las siguiente observación.

Observación 1. Dado que al aplicar una rotación de cualquier cara del cubo de Rubik el cubilete centro no se mueve a un nuevo cubículo, el color de la cara visible del cubilete centro determina el color de la cara que ocupa al resolver el cubo.

Ahora sabemos que el color final tras resolver el cubo de Rubik será el determinado por los cubiletes centro. En cambio, no resulta útil trabajar con colores en el cubo de

Rubik. Esto se debe a que la elección de colores de un cubo no es universal y depende también de cómo se coloquen dichos colores, es decir, se pueden asignar los mismos 6 colores a las caras de dos cubos de forma que estos no se puedan trasformar el uno en el otro mediante rotaciones. Un ejemplo que lo prueba es el siguiente: dados dos cubos resueltos, el primero de los cuales tiene la cara superior blanca, la del frente naranja y la de la derecha verde; el otro cubo, su cara superior es blanca, la del frente verde y la de la derecha naranja. Solo podemos intentar transformar un cubo en el otro mediante rotaciones del cubo completo, sin embargo, no es posible llevar a cabo dicha transformación. Diremos que son cubos con coloraciones distintas.

Introducimos ahora el concepto de coloración.

Definición 2.3 (Coloración del Cubo)**.**
Llamaremos coloración de un cubo a la asignación de colores a las caras del mismo. Dos coloraciones de un cubo se consideran equivalentes si una es una rotación del cubo completo de la otra.

A partir de esta definición podemos introducir la siguiente proposición obtenida a partir de un ejercicio propuesto en las notas de Signmaster, aunque la demostración de la misma es de elaboración propia. Este resultado será importante para la elección de la notación del cubo.

Proposición 2.2.1.
Existen 30 coloraciones posibles no equivalentes del cubo 3 dimensional.

Demostración. Considerar un cubo y 6 colores $\{a, b, c, d, e, f\}$ distintos dos a dos. Sin pérdida de generalidad, asumimos que el color f está en la cara inferior. Se dan dos casos:

- La cara del cubo con color e es colindante a la cara inferior de color f. En este caso podemos situar el color e al fondo. Fijar estas dos posiciones evita rotaciones del cubo que den configuraciones equivalentes. El número de coloraciones posibles de las 4 caras restantes son 4!.
- Si el color e no es colindante, es decir, está en la cara opuesta (arriba). Aún existen rotaciones que dejan estos dos colores en la misma posición. Fijamos el color d al fondo. Existen 3! coloraciones posibles.

Por lo tanto, en total existen $3! + 4! = 30$ coloraciones. □

Para evitar la confusión que pueda acarrear el uso de colores, se emplea una notación más general usada por David Singmaster [11] que detallaremos más en la Sección 3.1, la cual no depende de la coloración del cubo.

Notación 2.2.1 (Notación de Singmaster)**.**
Tomando las iniciales de las seis palabras en inglés para derecha, izquierda, frente, atrás, arriba y abajo, es decir, Right, Left, Front, Back, Up, Down respectivamente, etiquetamos cada cara del cubo de acuerdo a su posición.

De esta forma, asignamos cara U a la cara situada en la zona superior. Como el cubilete central es fijo, el color de su cara visible determina el color de la cara U. Tras esto, se fija la cara que se encuentra de frente como cara F y el color de la cara visible del cubilete central de esta cara determina el color de la misma. Una vez asignadas estas dos etiquetas, el resto de las caras quedan determinadas respecto a estas. En la Figura 2.5 se muestra el etiquetado de las caras de un cubo cualquiera.

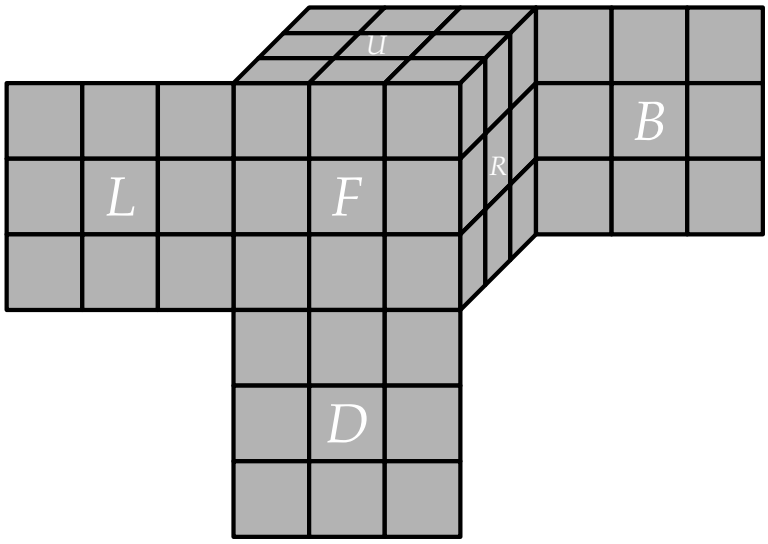

FIGURA 2.5: Etiquetado de las caras de un cubo de Rubik.

2.3. Operaciones sobre el cubo de Rubik

Dado que los giros siempre son de alguna de las 6 caras y solamente de estas, podemos emplear la misma notación para los giros.

Notación 2.3.1.
Usaremos la misma notación de R, L, F, B, U y D para referirnos a los giros de un cuarto de vuelta en sentido horario de las caras R, L, F, B, U y D respectivamente. Emplear la misma notación no será un problema, ya que especificará si se trata de un giro o de la cara.

Para los giros en sentido antihorario usamos la notación de potencias R^{-1}, L^{-1}, F^{-1} B^{-1}, U^{-1} y D^{-1}. Esta notación tomará sentido cuando consideremos los movimientos como elementos de un grupo, donde el elemento inverso de un giro será el giro en sentido opuesto.

Para describir una secuencia de giros aplicada sobre el cubo de Rubik, empleamos la notación multiplicativa, de forma que si tenemos M_1 e M_2 dos giros cualesquiera, siguiendo el convenio introducido por David Singmaster [11], $M_1^2 M_2$ es la operación que primero aplica el giro de un cuarto de vuelta M_1 dos veces y después aplica M_2.

Observación 2. Las secuencias de giros pueden verse como palabras formadas por el alfabeto $\{U, L, F, B, U, D, U^{-1}, L^{-1}, F^{-1}, B^{-1}, U^{-1}, D^{-1}\}$.

Notar que dos secuencias de giros diferentes, es decir, dos palabras diferentes, pueden tener el mismo efecto sobre el cubo de Rubik como UD y DU por lo que diremos que son equivalentes y por tanto la misma operación.

Definición 2.4 (Palabras equivalentes)**.**
Dos palabras X e Y se dicen equivalentes si tienen el mismo efecto sobre el cubo de Rubik. En ese caso escribiremos $X = Y$ y diremos que definen la misma operación.

Cuando hablemos de una operación sobre el cubo de Rubik, nos referiremos a una secuencia de giros concreta, sin importar el representante de dicha operación. Así, introducimos el conjunto de todas las operaciones en el cubo de Rubik.

Definición 2.5 (Conjunto de operaciones en el cubo de Rubik Rc_3)**.**
Se define el conjunto de operaciones en el cubo de Rubik como el conjunto de las palabras en el alfabeto $\{U, D, F, B, R, L\}$, bajo la relación de equivalencia descrita en la Definición 2.4. Se denota por Rc_3.

Definición 2.6 (Giro vacío)**.**
Llamaremos giro vacío a la operación sobre el cubo de Rubik que deja a este invariante y lo denotaremos por I.

2.4. Longitudes de palabras y operaciones en el cubo

Con la Definición 2.4, podemos escribir $U^4 = I$. Sin embargo, cuando aplicamos U^4 giramos 4 veces un cuarto de vuelta la cara U y al aplicar I no hacemos nada con el cubo. Esta noción motiva la introducción de la siguiente definición, que cuenta todos los giros de un cuarto de vuelta que tenemos que realizar para seguir la secuencia de giros definida por una palabra dada.

Definición 2.7 (Longitud de una palabra en la métrica de un cuarto de vuelta)**.**
Dada una palabra en el alfabeto $\{U, L, F, B, U, D, U^{-1}, L^{-1}, F^{-1}, B^{-1}, U^{-1}, D^{-1}\}$, llamamos longitud de la palabra en la métrica de un cuatro de vuelta al número de letras del alfabeto concatenado.

Sin embargo, también podríamos definir la longitud de una secuencia de giros sin importar cuanto se rote cada cara, sino cuantas veces. Por ejemplo, en la secuencia U^2D se gira la cara U una vez y la cara D una vez, por lo que tendría longitud dos a pesar de que haya 3 giros de un cuarto de vuelta.

Definición 2.8 (Longitud de una palabra en la métrica de media vuelta)**.**
Dada una palabra en el alfabeto $\{U, L, F, B, U, D, U^2, L^2, F^2, B^2, U^2, D^2, U^{-1}, L^{-1}, F^{-1}, B^{-1}, U^{-1}, D^{-1}, U^{-2}, L^{-2}, F^{-2}, B^{-2}, U^{-2}, D^2\}$ de forma que si aparecen dos giros de un cuarto de vuelta cómo M_1M_1 se contrae como M_1^2, llamamos longitud de la palabra en la métrica de media vuelta al número de elementos del alfabeto concatenado de dicho diccionario.

Para clarificar estas definiciones, mostramos un ejemplo de longitud de una palabra en ambas métricas.

Ejemplo 2.4.1.
Con las definiciones anteriores, la palabra $UFRRUD^{-1}$ tiene longitud 6 en la métrica de un cuarto de vuelta, ya que concatena 6 giros de un cuarto de vuelta. Si contraemos los giros de la cara R con UFR^2UD^{-1}, en la métrica de media vuelta su longitud es 5.

También podemos definir la longitud de una operación de la forma siguiente:

Definición 2.9 (Longitud de una operación en la métrica de un cuarto de vuelta)**.**
Dado el conjunto de palabras o secuencias de giros que definen una cierta operación, llamamos longitud de la operación en la métrica de un cuarto de vuelta al mínimo de las longitudes de esas palabras en la métrica de un cuarto de vuelta.

El giro vacío tiene longitud nula.

De forma análoga para la métrica de media vuelta.

Definición 2.10 (Longitud de una operación en la métrica de media vuelta)**.**
La longitud de una operación en la métrica de media vuelta es el mínimo de las longitudes de las palabras en la métrica de media vuelta que definen dicha operación.

El giro vacío tiene longitud nula.

Capítulo 3

Configuraciones del cubo de Rubik

Hasta ahora hemos hablado de posición de las pegatinas del cubo y colocación de los cubiletes para describir de forma intuitiva el estado de un cubo. A partir de ahora emplearemos el término configuración del cubo para describir cómo se colocan los cubiletes en el cubo.

Definición 3.1 (Conjunto de configuraciones del cubo de Rubik $\mathcal{S}$ y el conjunto ampliado $\mathcal{S}^*$)**.**
Llamaremos conjunto ampliado de configuraciones del cubo de Rubik al conjunto de todas las configuraciones que se pueden alcanzar ensamblando todos los cubiletes del cubo. Por otro lado, llamaremos conjunto de configuraciones del cubo de Rubik a aquellas configuraciones que se pueden alcanzar a partir del cubo resuelto solamente rotando las caras del mismo.

Además, emplearemos la notación de Singmaster, que permite describir configuraciones y definir las operaciones como permutaciones. También utilizaremos la notación introducida por Christoph Bandelow [1] que mediante una 4-tupla nos permitirá describir cualquier configuración del cubo, además de las operaciones sobre el mismo.

Estas dos notaciones serán útiles para demostrar en el Capítulo 4 que Rc_3 es un grupo y que este define una acción de grupo sobre el conjunto de las configuraciones.

3.1. Notación de Singmaster

En la Proposición 2.2.1 de la Sección 2 se da una idea de por qué no es conveniente trabajar con los colores del cubo para describirlo. En su lugar usamos la notación de Singmaster que introducimos al principio de la Sección 2.2, la cual no depende de la coloración del cubo.

La notación de Singmaster nombra los cubículos y cubiletes empleando las seis etiquetas posicionales.

Notación 3.1.1 (Para cubiletes y cubículos)**.**
Partiendo del cubo resuelto, se etiquetan los cubiletes indicando las caras del cubo que ocupan. Por ejemplo, el cubilete borde, que en la configuración resuelta sus caras ocupan la cara X y la cara Y del cubo, lo denotaremos como XY y nombraremos el cubículo que ocupa en la configuración resuelta como xy.

Por otro lado, el cubilete esquina cuyas caras ocupan las caras X, Y y Z del cubo en la configuración resuelta se denotará por XYZ y ocupa el cubículo xyz.

Diremos que un cubículo o un cubilete está en la cara X si este toca dicha cara.

Notación 3.1.2 (Orden de las siglas de cubiletes y cubículo)**.**
Respecto al orden de las siglas, los cubículos y cubiletes borde no tienen un orden canónico de las mismas. En el caso de los cubiletes esquina, existe cierto convenio: se etiquetan respetando el sentido horario de las caras cuando se mira a esta esquina desde el exterior del cubo. Un ejemplo para comprenderlo es el siguiente: en la Figura 3.1 en la que se muestra el cubilete URF. En este, el sentido horario sería el del ciclo de las caras $U \to R \to F \to U$, con lo que, dependiendo cual sea la primera letra, podemos escribir URF, FUR ó RFU.

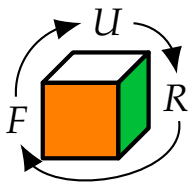

FIGURA 3.1: Cubilete URF, FUR ó RFU.

Para conocer la etiqueta de cada cubilete cuando el cubo no está resuelto, dado que conocemos el color de cada cara cuando el cubo está resuelto, el cubilete XY será el cubilete borde que tenga el color de la cara X y el color de la cara Y y de forma análoga para los cubiletes esquina.

Para hacer referencia a una cara de un cubilete o un cubículo, usaremos la misma nomenclatura de los cubiletes o cubículos de forma que la primera letra de la etiqueta indicará a cuál de las caras del mismo hacemos referencia. Por ejemplo, la cara XY es la cara del cubilete borde XY con el color de la cara X, y la cara YX será la que tenga el color de la cara Y del cubo. Para los cubículos, la cara xy será la cara del correspondiente cubículo situada en la cara X del cubo.

La idea de considerar las caras y el orden de las letras toma importancia al describir cómo se mueven los cubiletes al aplicar una operación sobre el cubo, tal y como se describirá en la Sección 3.2. La Figura 3.2 recoge el etiquetado de las 54 caras de todos los cubículos del cubo.

En la Tabla 3.1 se recogen todas las etiquetas de cubículos y cubiletes borde.

Cubículos	Cubiletes
uf ó fu	UF ó FU
ul ó lu	UL ó LU
ub ó bu	UB ó BU
ur ó ru	UR ó RU
rf ó fr	RF ó FR
fl ó lf	FL ó LF
lb ó bl	LB ó BL
br ó rb	BR ó RB
df ó fd	DF ó FD
dl ó ld	DL ó LD
db ó bd	DB ó BD
dr ó rd	DR ó RD

TABLA 3.1: Etiquetas de cubículos y cubiletes borde.

En la Tabla 3.2 se recogen todas las etiquetas de cubículos y cubiletes esquina posibles.

Cubículos	Cubiletes
urf, rfu ó fur	URF, RFU ó FUR
ufl, flu ó luf	UFL, FLU ó LUF
ulb, lbu ó bul	ULB, LBU ó BUL
ubr, bru ó rub	UBR, BRU ó RUB
dfr, frd ó rdf	DFR, FRD ó RDF
dlf, lfd ó fdl	DLF, LFD ó FDL
dbl, bld ó ldb	DBL, BLD ó LDB
drb, rbd ó bdr	DRB, RBD ó BDR

TABLA 3.2: Etiquetas de cubículos y cubiles esquina.

Observación 3. Dado que un cubilete no puede contener colores de caras opuestas, ninguna etiqueta tendrá letras correspondientes a caras opuestas, por ejemplo, u y d (arriba y abajo) no pueden estar en la misma etiqueta.

Definición 3.2 (Conjunto de cubículos borde y esquina)**.**
Llamaremos $\mathcal{X}$ al conjunto de etiquetas de caras de todos los cubículos borde y esquina del cubo de Rubik.

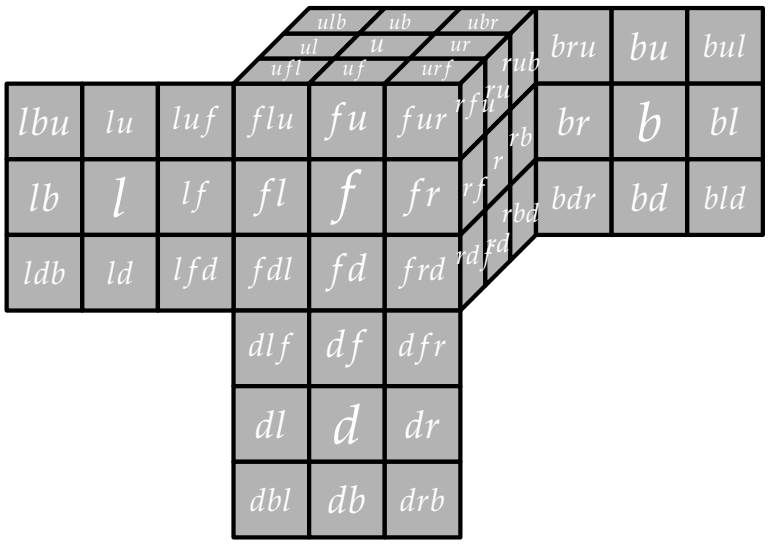

FIGURA 3.2: Cubículos con todas sus caras visibles etiquetadas. Observar que las 3 caras ocultas del cubo estás desplegadas para poder observarse.

3.2. Operaciones vistas como permutaciones

Cualquier operación sobre el cubo de Rubik da lugar a una reorganización de los 20 cubiletes no fijos del mismo. Dicha reorganización se puede observar como una permutación de los cubiletes.

Por ejemplo, si el cubilete del cubículo ufl se mueve al cubículo drb, escribimos

$$ufl \mapsto drb\,,$$

sin embargo, existen 3 maneras distintas de colocar un cubilete esquina en un cubículo esquina. La ventaja de la notación de caras elegida, es que la correspondencia anterior indica, no sólo a qué cubículo se mueve cierto cubilete, sino también su orientación: la cara del cubilete que ocupaba la cara ufl ocupará la cara drb y la cara del cubilete en flu ocupará la cara rbd y la cara del cubilete inicialmente en luf tomará la cara bdr, resaltando la importancia del orden de las siglas.

Mediante esta notación, podemos describir las permutaciones inducidas por las rotaciones U, D, F, B, R y L. Se comprueba que la rotación U se puede ver como una

permutación del conjunto $\mathcal{X}$ de caras de cubículos

$$\begin{aligned} U : \mathcal{X} &\to \mathcal{X} \\ uf &\mapsto ul \\ ufl &\mapsto ulb \\ ul &\mapsto ub \\ ulb &\mapsto ubr \\ ub &\mapsto ur \\ ubr &\mapsto urf \\ ur &\mapsto uf \\ urf &\mapsto ufl \end{aligned}$$

Por convención, los cubículos que no se mueven se dejan fuera de la lista, pero si una pieza es torcida o girada, se debe incluir. Además, si se da la imagen de una cara de un cubículo $\alpha_1\alpha_2\alpha_3 \mapsto \beta_1\beta_2\beta_3$, donde $\alpha_i, \beta_i \in \{u, f, l, b, r, d\}$ para $i = 1, 2, 3$, la imagen de las otras caras del cubículo cumplen $\alpha_2\alpha_3\alpha_1 \mapsto \beta_2\beta_3\beta_1$ y $\alpha_3\alpha_1\alpha_2 \mapsto \beta_3\beta_1\beta_2$. De igual forma, si la imagen de una cara borde $\gamma_1\gamma_2 \mapsto \delta_1\delta_2$, donde $\gamma_i, \delta_i \in \{u, f, l, b, r, d\}$ para $i = 1, 2$, entonces, $\gamma_2\gamma_1 \mapsto \delta_2\delta_1$.

Nos resulta útil emplear la notación de ciclo (α, β, γ) donde $\alpha, \beta, \gamma \in \mathcal{X}$ que indica que α va a β, β va a γ y γ a α. La operación anterior se puede reescribir como un producto de ciclos

$$U = (uf,\ ul,\ ub,\ ur)(ufl,\ ulb,\ ubr,\ urf).$$

Recogemos así la descripción en ciclos disjuntos de los 6 giros del cubo de Rubik [6]

$$\begin{aligned} U &= (uf,\ ul,\ ub,\ ur)(ufl,\ ulb,\ ubr,\ urf) \\ R &= (ur,\ br,\ dr,\ fr)(ubr,\ bdr,\ rdf,\ rfu) \\ F &= (fu,\ fr,\ fd,\ fl)(fur,\ frd,\ fdl,\ flu) \\ L &= (lu,\ lf,\ ld,\ lb)(luf,\ lfd,\ ldb,\ lbu) \\ B &= (bu,\ bl,\ bd,\ br)(bul,\ bld,\ bdr,\ bru) \\ D &= (df,\ dr,\ db,\ dl)(dlf,\ dfr,\ drb,\ dbl) \end{aligned}$$

3.3. Configuraciones - Notación Christoph Bandelow

La notación de Singmaster que describe los giros como permutaciones es útil para conocer cómo se mueven los cubiletes entre los cubículos al aplicar una cierta operación, sin embargo, no es una notación intuitiva para describir las configuraciones del cubo. Por eso, empleamos la notación introducida por Christoph Bandelow [1], que permite expresar cualquier configuración del cubo de Rubik mediante una 4-tupla.

La primera coordenada de la tupla indica el cubículo ocupado por cada cubilete esquina, ignorando su orientación. La segunda indica lo mismo para los cubiletes borde. La tercera coordenada indica cómo se orienta cada cubilete esquina y la última cómo se orientan los cubiletes borde.

Para indicar la posición de los cubiletes se enumeran los cubículos esquina del (1) al (8) y los cubículos borde del [1] al [12] como se muestra en la Figura 3.3. Los cubiletes se enumeran igual que el cubículo que ocupan en la configuración resuelta.

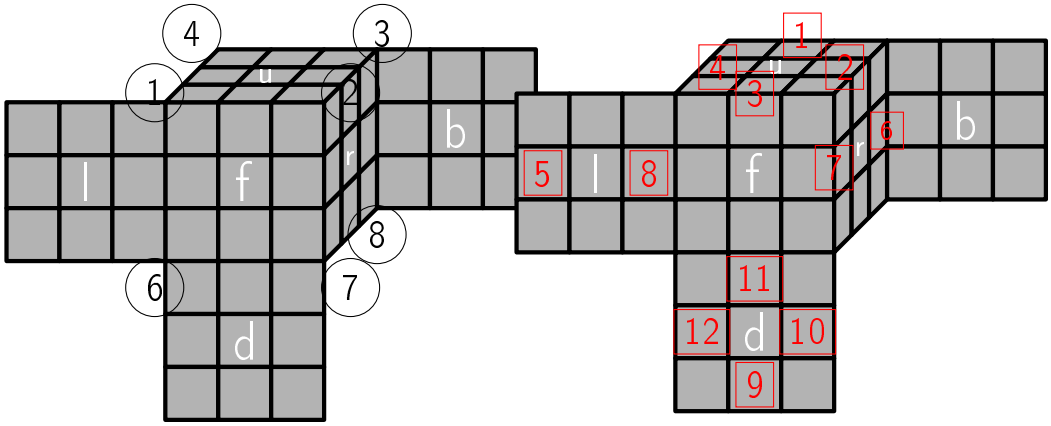

FIGURA 3.3: En la izquida una enumeración de cubículos esquina. En la derecha, una enumeración de cubículos borde.

Singmaster	Bandelow
ufl	(1)
urf	(2)
ubr	(3)
ulb	(4)
dbl	(5)
dlf	(6)
dfr	(7)
drb	(8)

Singmaster	Bandelow
ub	[1]
ur	[2]
uf	[3]
ul	[4]
lb	[5]
br	[6]
rf	[7]
fl	[8]
db	[9]
dr	[10]
df	[11]
dl	[12]

TABLA 3.3: Correspondencia entre la notación de Singmaster y Bandelow para cubículos

La Tabla 3.3 incluye la correspondencia entre los cubículos en la notación de Singmaster y la numeración dada en la notación de Bandelow.

Las posiciones de los cubiletes esquina y borde se pueden dar mediante un elemento del grupo simétrico de 8 elementos y otro del grupo simétrico de 12 elementos respectivamente, que serán las dos primeras coordenadas de la 4-tupla e indicarán a qué cubículo se ha desplazado cada cubilete desde su cubículo en la configuración resuelta. Entonces, si la primera coordenada de la 4-tupla fuese la permutación en notación de ciclo (4, 7, 6), entonces, con la enumeración de la Figura 3.3, el cubilete ULB (que en la configuración resuelta ocupa el cubículo (4)) ocuparía el cubículo frd (etiquetado con el (7)), el cubilete FRD (que en la configuración resuelta ocupa el cubículo etiquetado con el (7)) al fdl (etiquetado con el (6)) y el FDL (que en la

configuración resuelta ocupa el cubículo etiquetado con el (6)) al *ulb* (etiquetado con el (4)). Este ejemplo se ilustra en la Figura 3.4.

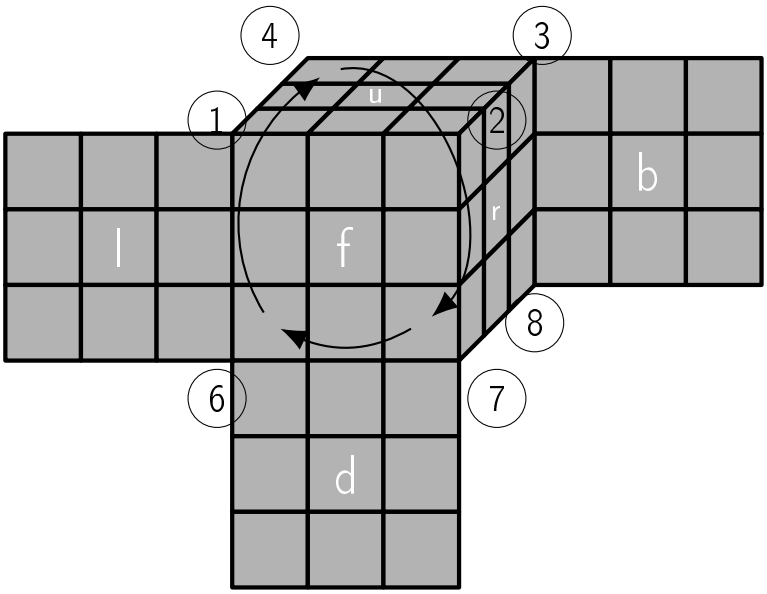

FIGURA 3.4: Ilustración del movimiento de los cubiletes borde definido por el ciclo (4, 7, 6).

Respecto a la orientación de los cubiletes en los cubículos, cada cubilete esquina se puede colocar de 3 formas diferentes en su cubículo y los borde de dos. Para describir la orientación de los cubiletes, fijamos un signo + en una cara de cada cubículo y se usará como sistema de referencia. Un ejemplo se muestra en la parte izquierda de la Figura 3.5. Enumeramos las caras de cada cubilete, de forma que en la configuración resuelta, la cara del cubilete que ocupa la cara del cubículo con un signo + tenga valor 0 y el resto se enumeran en sentido horario como se muestra en la parte derecha Figura 3.5. Notar que el signo + toma una posición en el cubículo, por lo que al rotar las caras del cubo, la posición del signo + permanece fija pero los números en las caras de los cubiletes sí tomarán nuevas posiciones.

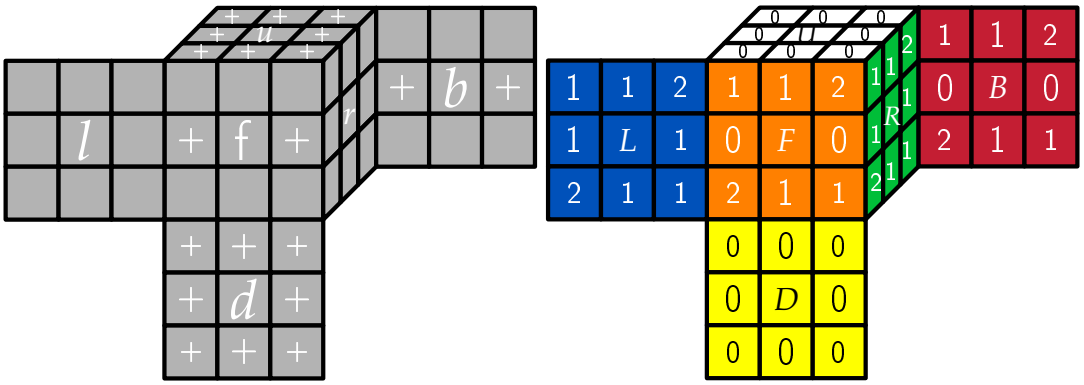

FIGURA 3.5: A la izquierda se marcan las caras de referencia de cada cubículo con una cruz. A la derecha se indica la enumeración de las caras de los cubiletes esquina y borde a partir de las caras de referencia.

Más formalmente, la notación empleada por Bandelow da lugar a la siguiente definición, que permite describir cualquier configuración del cubo de Rubik.

Definición 3.3 (Vector de posición)**.**
Llamamos vector de posición del cubo de Rubik a la tupla (ρ, σ, v, w) donde $\rho \in S_8, \sigma \in S_{12}$ recogen la posición de los cubiletes en los cubículos y $v \in \mathbb{Z}_3^8$ y $w \in \mathbb{Z}_2^{12}$ la orientación de los cubiletes.

$\rho \in S_8 : \rho(i) = j$ si el cubilete esquina (i) está en el cubículo esquina (j)

$\sigma \in S_{12} : \sigma(i) = j$ si el cubilete borde [i] está en el cubículo borde [j]

$v = (v_1, v_2, ..., v_8) \in \mathbb{Z}_3^8 = \{0, 1, 2\}^8 : v_i$ es el número de la cara del cubilete esquina que ocupa la cara del cubículo esquina (i)-ésimo con el signo +.

$w = (w_1, w_2, ..., w_{12}) \in \mathbb{Z}_2^{12} : w_i$ es el número de la cara del cubilete borde que ocupa la cara del cubículo borde [i]-ésimo con el signo +.

Ejemplo 3.3.1.
Con la definición anterior, la configuración del cubo resuelta sería

$$(id_8, id_{12}, 0_8, 0_{12})$$

donde id_n es el elemento neutro del grupo simétrico de orden n y 0_n es la n-tupla de ceros. Esto quiere decir que, en la configuración resuelta, el cubilete (tanto esquina como borde) i-ésimo está en el cubículo $id(i) = i$ y que todas las caras de los cubículos marcadas con un + están ocupadas por el 0 del respectivo cubilete.

Otro ejemplo menos trivial es el de la configuración con vector de posición $((1, 4, 3, 7, 6), (1, 2, 7, 11, 8, 3), (1, 2, 0, 0, 0, 2, 1, 0), (0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0))$ que se muestra a la derecha de la Figura 3.7.

Proposición 3.3.1 (Conjunto de configuraciones y conjunto ampliado)**.**
El conjunto ampliado de configuraciones del cubo de Rubik coincide con el conjunto $\mathcal{S}^* := S_8 \times S_{12} \times \mathbb{Z}_3^8 \times \mathbb{Z}_{12}^2$. Por lo tanto, se llama conjunto de configuraciones del cubo de Rubik al subconjunto de configuraciones $\mathcal{S} \subset \mathcal{S}^*$ que se pueden alcanzar mediante operaciones aplicadas sobre la configuración resuelta y se introduce en el siguiente capítulo.

Demostración. Directo a partir de la Definición 3.3 y la Definición 3.1 ya que dicha notación permite describir cualquier colocación de los cubiletes esquina (en los cubículos esquina) y los cubiletes borde (en los cubículos borde), lo que es lo mismo, describe cualquier configuración que se puede alcanzar desensamblando y volviendo a ensamblar todas las piezas del cubo de Rubik. □

Hasta el momento no hemos introducido herramientas que nos permitan saber qué configuraciones de $\mathcal{S}^*$ pertenecen a $\mathcal{S}$. La notación de Bandelow nos permitirá dar respuesta a esta pregunta en la Sección 5.1 mediante el primer teorema del cubo de Rubik.

3.4. Operaciones – notación de Bandelow

En la Sección 3.3 hemos visto que podemos escribir las configuraciones del cubo de Rubik como una 4-tupla. De esta forma, si aplicamos una operación sobre un cubo, el cubo resultante se describirá mediante una nueva 4-tupla, es decir, las operaciones mandan las 4-tuplas en otras 4-tuplas o lo que es lo mismo, podemos ver las operaciones sobre el cubo de Rubik como endomorfismos en el conjunto $\mathcal{S}$ de configuraciones del cubo de Rubik.

Proposición 3.4.1 ([Lema 11.4, 4]).
Dada una configuración del cubo de Rubik definida por el vector de posición $a := (\rho, \sigma, \boldsymbol{v}, \boldsymbol{w}) \in \mathcal{S}$, el vector de posición de la configuración tras aplicarle un giro $M := (\pi, \tau, \phi, \psi) \in \{R, L, U, D, F, B\}$ será $M \cdot a := (\pi, \tau, \phi, \psi) \cdot (\rho, \sigma, \boldsymbol{v}, \boldsymbol{w}) = (\pi \circ \rho, \tau \circ \sigma, \phi(\boldsymbol{v}), \psi(\boldsymbol{w}))$ donde $\pi \in S_8$, $\tau \in S_{12}$, $\phi : \mathbb{Z}_8^3 \to \mathbb{Z}_8^3$ y $\psi : \mathbb{Z}_{12}^2 \to \mathbb{Z}_{12}^2$ de forma que la tupla (π, τ, ϕ, ψ) viene dada en cada caso por:

$$\begin{aligned}
R = ((2,3,8,7),(2,6,10,7),&(v_1, v_7+1, v_2+2, v_4, v_5, v_6, v_8+2, v_3+1),\\
&(w_1, w_7, w_3, w_4, w_5, w_{10}, w_2, w_8, w_9, w_6, w_{11}, w_{12}))\\
L = ((1,6,5,4),(5,12,8,4),&(v_4+2, v_2, v_3, v_5+1, v_6+2, v_1+1, v_7, v_8),\\
&(w_1, w_2, w_3, w_5, w_{12}, w_6, w_7, w_4, w_9, w_{10}, w_{11}, w_8))\\
U = ((1,4,3,2),(1,2,3,4),&(v_2, v_3, v_4, v_1, v_5, v_6, v_7, v_8),\\
&(w_4, w_1, w_2, w_3, w_5, w_6, w_7, w_8, w_9, w_{10}, w_{11}, w_{12}))\\
D = ((5,8,7,6),(9,12,11,10),&(v_1, v_2, v_3, v_4, v_8, v_5, v_6, v_7),\\
&(w_1, w_2, w_3, w_4, w_5, w_6, w_7, w_8, w_{10}, w_{11}, w_{12}, w_9))\\
F = ((1,2,7,6),(3,,7\,11,8),&(v_6+1, v_1+2, v_3, v_4, v_5, v_7+2, v_2+1, v_8),\\
&(w_1, w_2, w_8+1, w_4, w_5, w_6, w_3+1, w_{11}+1, w_9, w_{10}, w_7+1, w_{12}))\\
B = ((8,3,4,5),(1,5,9,6),&(v_1, v_2, v_8+1, v_3+2, v_4+1, v_6, v_7, v_5+2),\\
&(w_6+1, w_2, w_3, w_4, w_1+1, w_9+1, w_7, w_8, w_5+1, w_{10}, w_{11}, w_{12}))
\end{aligned}$$

Demostración. Se deja la comprobación al lector. □

Veamos un ejemplo de cómo los giros sobre las caras del cubo de Rubik afectan a las configuraciones como se indica en la Proposición 3.4.1.

Ejemplo 3.4.1.
Supongamos que partimos del cubo de Rubik en la configuración resuelta, al que le corresponde el vector de posición $a = (id_8, id_{12}, 0_8, 0_{12})$. Si aplicamos el giro U tendremos:

$$U \cdot a = ((1,4,3,2),\ (1,2,3,4),\ 0_8,\ 0_{12}).$$

Si miramos a los cubiletes esquina en la Figura 3.6, vemos que el cubilete ULB ahora ocupa el cubículo ubr (enumerado con un (3)), el UBR ocupa el urf (enumerado con un (2)), el cubilete URF ocupa el cubículo ufl (enumerado con un (1)) y el UFL al ulb (enumerado con el (4)). Y el resto de los cubiletes esquina siguen en la posición de partida. Respecto a los cubiletes borde, el UB pasa a ur (enumerado con un 2), el UR al uf (enumerado con el 3) el UF al ul (enumerado con un 4) y el UL al ub (enumerado con el 1).

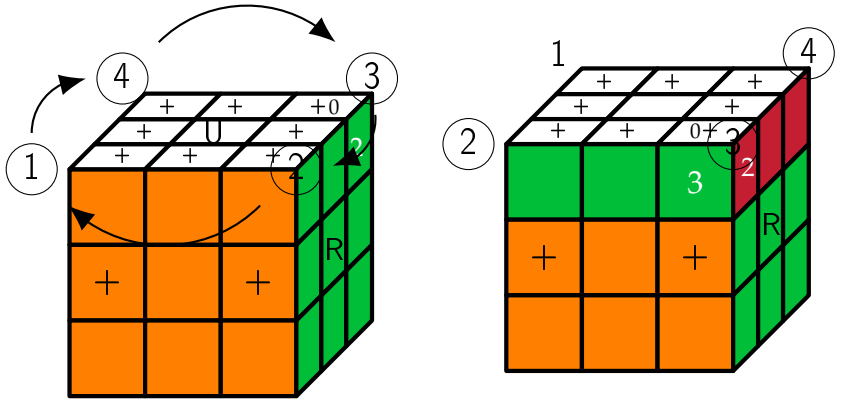

FIGURA 3.6: Giro U. Sólo se indica el efecto sobre los cubiletes esquina por conveniencia.

Observando las orientaciones, si miramos a la Figura 3.6 nuevamente, las caras de referencia de los cubículos siguen ocupadas por las caras de los cubiletes enumerados con un 0, por lo que la tercera y cuarta coordenada de la tupla seguirá siendo 0.

Ahora aplicamos el giro F.

$$
\begin{aligned}
&F \cdot ((1,4,3,2),(1,2,3,4),0_8,0_{12}) \\
&= ((1,2,7,6)(1,4,3,2),(3,7,11,8)(1,2,3,4), \\
&\quad (1,2,0,0,0,2,1,0),(0,0,1,0,0,0,1,1,0,0,1,0)) = \\
&= ((1,4,3,7,6),(1,2,7,11,8,3,4), \\
&\quad (1,2,0,0,0,2,1,0),(0,0,1,0,0,0,1,1,0,0,1,0))
\end{aligned}
$$

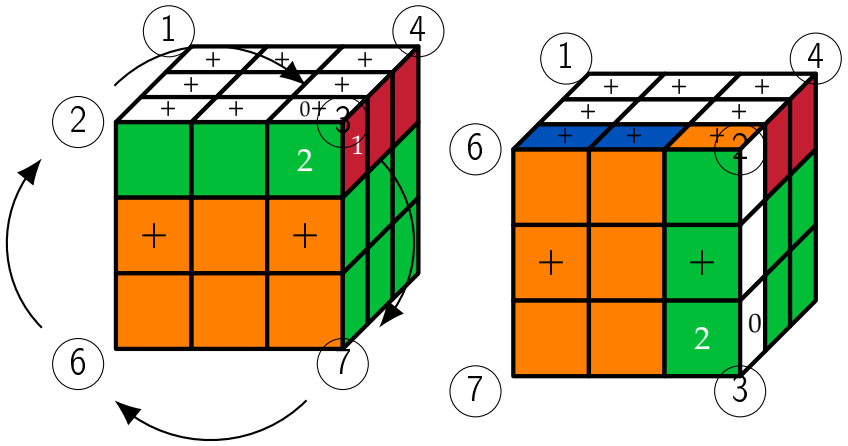

FIGURA 3.7: Giro UF. Sólo se indica el efecto sobre los cubiletes esquina por conveniencia.

Observemos detalladamente el movimiento del cubilete UBR. En la configuración resuelta, este cubilete ocupa el cubículo etiquetado con el (3). Al aplicar el giro U, vemos en la Figura 3.6 que pasa al cubículo etiquetado con un (2). La primera coordenada de la tupla $U \cdot a = ((1,4,3,2),(1,2,3,4),\ 0_8,\ 0_{12})$ indica que el cubilete del

cubículo (3) pasa a ocupar cubículo (2). Al concatenar con un giro F como se ve en la Figura 3.7, el cubilete que estaba en el cubículo (2), en este caso el UBR (ó el cubilete (3)), ocupará el cubículo (7). Esto se indica en la primera coordenada de $R \cdot (U \cdot a) = ((1, 4, 3, 7, 6), (1, 2, 7, 11, 8, 3, 4), (1, 2, 0, 0, 0, 2, 1, 0), (0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0))$ que expresa cómo el cubilete que en la configuración resuelta ocupaba el cubículo esquina (3), ocupará el cubículo (7).

Veamos ahora el efecto del giro F sobre las orientaciones de los cubiletes y nos centramos en el vector de la tercera coordenada de la 4-tupla. La séptima coordenada de este vector corresponde al cubículo (7). Tras aplicar el giro F que se ilustra en la Figura 3.7, el cubilete que estaba en el cubículo (2) ocupará el cubículo (7). La cara de referencia del cubículo (2) está en la cara U, por lo que al aplicar el giro F, la cara del cubilete que ocupaba la cara de referencia del cubículo ocupará la cara R del cubículo (7). Podemos entender la nueva orientación de dicho cubilete como que ahora tiene un uno sobre la cara con una cruz.

Capítulo 4

Grupo del Cubo de Rubik

Al aplicar una secuencia de giros que da una cierta operación, es intuitivo pensar que para deshacer el efecto de esa operación basta repetir dicha secuencia en sentido inverso , lo que lleva a pensar que el conjunto de todos las operaciones sobre el cubo de Rubik tiene estructura de grupo.

4.1. El conjunto Rc_3 de operaciones sobre el cubo de Rubik es un grupo

Proposición 4.1.1.
El conjunto Rc_3 introducido en la Definición 2.5 es el grupo generado por los elementos U, R, F, L, B, D, es decir,

$$Rc_3 = \langle U, R, F, L, B, D \rangle \tag{4.1}$$

Demostración.

- Claramente es un conjunto no vacío.
- La composición de operaciones es operación interna por la definición de grupo generado.
- El giro vacío I es el elemento neutro y pertenece al conjunto ya que $U^3U = I \in Rc_3$ y que la composición es operación interna.
- Existencia del elemento inverso: basta considerar que todo elemento $M \in Rc_3$ se puede descomponer en una secuencia de giros $M = M_1 \cdots M_n$ con $M_i \in \{U, F, R, B, D, L\}$ para $i = 1, \ldots, n$. Así, el elemento inverso de M es $M^{-1} = M_n^{-1} \cdots M_1^{-1}$ ya que $MM^{-1} = M_1 \cdots M_n M_n^{-1} \cdots M_1 = I$ y $M^{-1}M = M_n^{-1} \cdots M_1^{-1} M_1 \cdots M_n = I$ donde aplicamos la propiedad asociativa asumida como cierta y que para cada par de giros $M_i M_i^{-1} = I$ y $M_i^{-1} M_i = I$. Nótese que el inverso de U, F, R, B, D, L son U^3, F^3, R^3, B^3, D^3, L^3 respectivamente.
- La composición de operaciones cumple la propiedad asociativa. Este concepto no es trivial ya que no es evidente la idea de agrupar operaciones, aunque la prueba de este punto es directa a partir de los conceptos introducidos en la Sección 3.2: la notación de Singmaster permite ver los giros U, R, F, L, B, D como permutaciones, lo que ayuda a entender la composición de dos giros. Podemos pensar en la operación dada por la composición de dos o más giros, como aquella que arranca los cubiletes del cubo de Rubik y los recoloca igual que si se hubieran concatenado los giros. Dado que la composición de permutaciones es asociativa, Rc_3 también.

□

Una pregunta que nos podemos hacer sobre este grupo es si es conmutativo, y la respuesta es directa.

Proposición 4.1.2.
El grupo del cubo de Rubik no es conmutativo.

Demostración. Basta considerar las operaciones U^2R^2 y R^2U^2 que son distintas como se muestra en la Figura 4.1. □

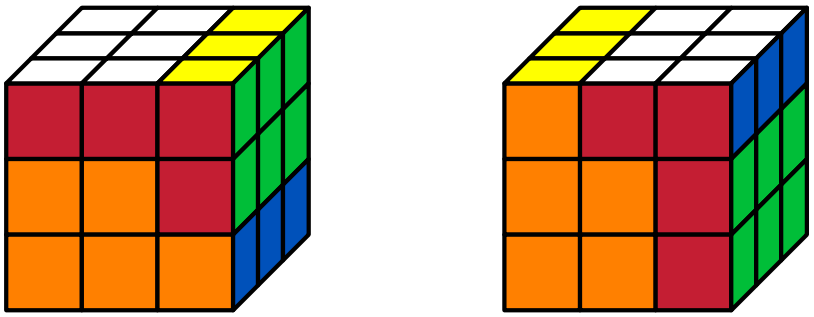

FIGURA 4.1: A la izquierda el cubo de Rubik tras aplicar la operación U^2R^2 y a la derecha R^2U^2.

Una segunda pregunta que se puede plantear es sobre la cardinalidad del grupo. Para ello hacemos primero la siguiente observación.

Observación 4. Hay una biyección directa entre el conjunto de operaciones Rc_3 y el conjunto de configuraciones del cubo $\mathcal{S}$, asignando a cada operación $M \in Rc_3$ la configuración obtenida de aplicar $M \cdot (id_8, id_{12}, 0_8, 0_{12})$ (ver Prop. 4.3.2).

Proposición 4.1.3.
El grupo del cubo de Rubik es finito.

Demostración. El grupo del cubo de Rubik es biyectable con el conjunto $\mathcal{S}$, que es subconjunto de $\mathcal{S}^*$, el cual es finito, por lo tanto el grupo del cubo de Rubik es finito. □

De momento sólo tenemos las herramientas para saber que el grupo del cubo de Rubik es finito, pero no para determinar su cardinal. El Primer Teorema Fundamental del Cubo de Rubik permitirá calcular de forma directa el cardinal de Rc_3.

Sin embargo, podemos adelantar que el grupo del cubo Rubik, a pesar de sencillo, es muy grande, por lo que es interesante estudiar subgrupos más pequeños generados por movimientos más simples o limitados. Se muestra como ejemplo uno de los primeros subgrupos que se pueden estudiar que es el llamado Two-Squares, que es el generado por el giro de media vuelta de dos caras.

4.2. Grupo Two-Squares

El grupo Two-Squares es el grupo generado por los giros de media vuelta de caras contiguas. En este caso, estudiaremos el grupo generado por U^2 y R^2.

Observación 5. El grupo de dos cuadrados no es abeliano. Ya hemos visto que $U^2R^2 \neq R^2U^2$ en la Figura 4.1 de la página 28.

Una pregunta que puede surgir sobre el subgrupo generado, es sobre su cardinalidad, que se da en la siguiente proposición.

Proposición 4.2.1.
En el grupo $\langle U^2, R^2 \rangle$ hay 12 operaciones distintas.

Para demostrar este resultado, comencemos primero dando el siguiente lema:

Lema 4.2.2.
La operación $(U^2R^2)^6$ es igual al giro vacío. Además, $(U^2R^2)^6$ es la palabra formada por la concatenación de U^2 y R^2 de forma alternada de longitud en la métrica de media vuelta más corta que define la misma operación que el giro vacío.

Demostración. Sea $M := (U^2R^2)^6$, una palabra de longitud 12 en la métrica de media vuelta y veamos que coincide con la identidad. Para comprobar esta afirmación basta aplicar dicha secuencia de giros sobre un cubo de Rubik y observar que queda invariante, lo cual se ilustra dividido en 12 pasos en la Figura A.1 del Apéndice A, por lo tanto $M = Id$. En la misma ilustración es directo ver que $(U^2R^2)^n \neq I$ para $0 < n < 6$ y $(U^2R^2)^nU^2 \neq I$ para $0 \leq n < 6$, luego (U^2R^2) es la concatenación de U^2 R^2 más corta que es igual al giro vacío. □

Lema 4.2.3.
Considerar los conjuntos $\mathcal{U} := \{U^2, U^2R^2, ...\}$ y $\mathcal{R} := \{R^2, R^2U^2, ...\}$ cuyos elementos son las operaciones definidas por palabras que concatenan U^2 y R^2 alternadamente, de forma que las operaciones del primer conjunto están dadas por palabras que comienzan con U^2 y los del segundo con R^2. Entonces $\mathcal{U} = \mathcal{R}$ bajo la equivalencia dada en la Definición 2.4.

Demostración. Considerar la operación dada por la palabra $M := (U^2R^2)^6$. Por el Lema 4.2.2, $M = I$.

Si multiplicamos por R^2 a la derecha de ambos lados de la igualdad $M = Id$, tenemos $MR^2 = R^2$, luego $R^2 \in \mathcal{U} = \{U^2, U^2R^2, ...\}$ dado que M comienza por U^2. Asimismo, es directo que $\{R^2, R^2U^2, ...\} \subseteq \{U^2, U^2R^2, ...\}$. De forma análoga se tiene la inclusión contraria. □

Notar que estamos haciendo un abuso de notación, ya que a pesar de que las palabras de los dos conjuntos son distintas, nos estamos refiriendo al conjunto de operaciones que definen las mismas.

Para conocer el cardinal del conjunto hay que saber cuántos elementos distintos tiene, para lo cual introducimos el siguiente lema.

Lema 4.2.4.
Todas las palabras del conjunto $\{U^2, U^2R^2, ...\}$ de longitud menor que 12 (en la métrica de media vuelta) definen operaciones distintas.

Demostración. La afirmación de este Lema es directa a partir de la Figura A.1, en la que se comprueba que todas las operaciones son distintas. □

Demostración de la Proposición 4.2.1. Observar que $U^2U^2 = U^4 = I$ y $R^2R^2 = R^4 = I$, por tanto, los elementos del grupo Two-Squares estará formado por secuencias de giros R^2 y U^2, es decir

$$\langle U^2, R^2\rangle = \{U^2, U^2R^2, U^2R^2U^2, ...\} \cup \{R^2, R^2U^2, R^2U^2R^2, ...\}$$

Por el Lema 4.2.3, los dos conjuntos de la unión definen las mismas operaciones. Además, por el Lema 4.2.2, la secuencia $U^2R^2U^2R^2U^2R^2U^2R^2U^2R^2U^2R^2$, de longitud 12 en la métrica de media vuelta, es la primera que es igual al giro vacío y, por el Lema 4.2.4, todas las concatenaciones de a lo sumo 12 giros U^2 y R^2 que comienzan por U^2 son distintas, luego el conjunto de operaciones en las palabras $\{U^2, U^2R^2, ...\}$ tiene cardinal 12, en consecuencia, el grupo $\langle U^2, R^2\rangle$ tiene cardinal 12. □

Otra pregunta que puede surgir al ver el patrón de las operaciones es si el grupo es cíclico, es decir, si está generado por un sólo elemento. En la siguiente proposición se prueba que no lo es.

Proposición 4.2.5.
El grupo $\langle U^2, R^2\rangle$ no es un grupo cíclico.

Demostración. Por las observaciones anteriores el grupo $\langle U^2, R^2\rangle = \{U^2, U^2R^2, ..., (U^2R^2)^6\}$. Supongamos por reducción al absurdo que es cíclico, es decir, existe un elemento en el grupo que lo genera. Si dicho elemento fuera de la forma $U^2 \cdots U^2$ está claro que no generaría el grupo, pues $(U^2 \cdots U^2)^2 = U^2 \cdots U^2U^2 \cdots U^2 = U^2 \cdots R^2R^2 \cdots U^2 = ... = I$ y el grupo tendría cardinal dos. Luego, debe ser de la forma $U^2 \cdots R^2$. Consideremos ahora la potencia $(U^2 \cdots R^2)^r$. Tras contraer las secuencias de la forma $(U^2R^2)^6 = I$, podemos escribir $(U^2 \cdots R^2)^r = (U^2R^2)^k$ con $k \equiv r \bmod 6$, por lo que $(U^2 \cdots R^2)$ no genera las permutaciones terminadas con U^2. Luego, $\langle U^2, R^2\rangle$ no es un grupo cíclico. □

4.3. Acción del grupo de Cubo de Rubik sobre $\mathcal{S}$

A lo largo de este trabajo se ha introducido la idea de que al aplicar una operación sobre un cubo en una configuración dada, se genera una nueva configuración. Ahora veremos que en efecto, se trata de una acción del grupo del cubo de Rubik Rc_3 sobre el conjunto $\mathcal{S}$ dado en la Proposición 3.3.1.

La afirmación de que el grupo del cubo de Rubik Rc_3 define una acción sobre el conjunto $\mathcal{S}^*$ es intuitiva, sin embargo, los detalles de su demostración serán útiles en la demostración del teorema fundamental del cubo de Rubik.

Proposición 4.3.1.
El grupo del cubo de Rubik Rc_3 define una acción sobre el conjunto $\mathcal{S}$ de configuraciones del cubo de Rubik .

Demostración. Una operación $M \in Rc_3$ la escribimos como una secuencia de n giros $M = M_1 \cdots M_n$ con $M_i \in \{R, L, U, D, F, B\}$. Escribimos cada giro $M_i := (\pi_i, \tau_i, \phi_i, \psi_i)$ como en la Proposición 3.4.1, de forma que la concatenación de dos giros $M_iM_j = (\pi_j \circ \pi_i, \tau_j \circ \tau_i, \phi_j \circ \phi_i, \psi_j \circ \psi_i)$, por lo que podemos escribir $M = (\pi, \tau, \phi, \psi) = (\pi_n \circ \cdots \circ \pi_1, \tau_n \circ \cdots \circ \tau_1, \phi_n \circ \cdots \circ \phi_1, \psi_n \circ \cdots \circ \psi_1)$

Ahora definimos la acción de las operaciones del grupo del cubo de Rubik Rc_3 sobre el conjunto de configuraciones del cubo.

$$\begin{aligned} \cdot : Rc_3 \times \mathcal{S}^* &\longrightarrow \mathcal{S}^* \\ (M, a) &\mapsto M \cdot a = (\pi, \tau, \phi, \psi) \cdot (\rho, \sigma, \boldsymbol{v}, \boldsymbol{w}) = (\pi \circ \rho, \tau \circ \sigma, \phi(\boldsymbol{v}), \psi(\boldsymbol{w})) \end{aligned}$$

En efecto, la aplicación '$\cdot$' define la acción de Rc_3 sobre $\mathcal{S}^*$:

- Rc_3 es un grupo y $\mathcal{S}^*$ es un conjunto.
- Dado $s \in \mathcal{S}^*$, la acción del giro vacío $I(s) = s$ por lo que es el elemento neutro.
- Se cumple la propiedad asociativa, $M_1\dot{(}M_2 \cdot a) = (M_1 M_2) \cdot a$, por la asociatividad de la composición de aplicaciones en cada coordenada.

□

A partir de este resultado podemos caracterizar de la forma siguiente todos los elementos del conjunto $\mathcal{S}$ de configuraciones del cubo de Rubik .

Proposición 4.3.2.
El conjunto $\mathcal{S}$ de configuraciones del cubo de Rubik es la órbita de $(id_8,\ id_{12},\ 0_8,\ 0_{12})$ por la acción de Rc_3.

Demostración. Directo a partir de la definición de conjunto de configuraciones del cubo de Rubik. □

Capítulo 5

Teorema Fundamental del Cubo de Rubik

Este capítulo se centra en la demostración del teorema fundamental del cubo de Rubik y sus consecuencias. Comienza con algunos resultados, que serán útiles para la siguiente sección. Otros resultados ayudarán a demostrar que las condiciones dadas por el teorema son necesarias. Después, se dará una estrategia de resolución del cubo dividida en 4 pasos. Esta servirá para demostrar que las condiciones del teorema son suficientes para que una configuración satisfaciendo dichas condiciones se pueda resolver. Finalmente, se empleará el teorema fundamental para conocer el cardinal del grupo del cubo de Rubik.

5.1. Primer teorema en teoría del Cubo

Teorema 5.1.1 (Teorema Fundamental de la Teoría del Cubo [Teorema 11.1, 4])**.**
El vector de configuración del conjunto ampliado $(\rho, \sigma, \boldsymbol{v}, \boldsymbol{w}) \in \mathcal{S}^* = S_8 \times S_{12} \times \mathbb{Z}_3^8 \times \mathbb{Z}_2^{12}$ pertenece al conjunto de configuraciones del cubo de Rubik $\mathcal{S}$ si y solamente si se satisfacen las 3 condiciones:

- $\text{sign}(\rho) = \text{sign}(\sigma)$
- $v_1 + v_2 + \cdots + v_8 \equiv 0$ (mód 3)
- $w_1 + w_2 + \cdots w_{12} \equiv 0$ (mód 2)

Para la demostración del teorema será útil introducir las siguientes nociones.

Definición 5.1 (Proyección de cubiletes esquina)**.**
Dado $M = (\pi, \tau, \phi, \psi) \in Rc_3$, definimos la proyección de los cubiletes esquina,

$$\begin{aligned} \phi_{esquina} : Rc_3 &\longrightarrow S_8 \\ M = (\pi, \tau, \phi, \psi) &\mapsto \pi \end{aligned}$$

Definición 5.2 (Proyección de cubiletes borde)**.**

$$\begin{aligned} \phi_{borde} : Rc_3 &\longrightarrow S_8 \\ M = (\pi, \tau, \phi, \psi) &\mapsto \tau \end{aligned}$$

Además, también serán útiles los siguientes lemas.

Lema 5.1.2.
Para cualquier operación $M \in Rc_3$ se tiene $\text{sign}(\phi_{borde}(M)) = \text{sign}(\phi_{esquina}(M))$.

Demostración. Dado que cualquier operación M es una concatenación de giros, es decir, $M = M_1 \cdots M_n$ con $M_i \in \{U, D, L, R, F, B\}$ para $i = 1, ..., n$, $\text{sign}(\phi_{borde}(M_i)) = \text{sign}(\phi_{esquina}(M_i))$ por la Proposición 3.4.1 y el signo es un morfismo, es directo que $\text{sign}(\phi_{borde}(M)) = \text{sign}(\phi_{esquina}(M))$. □

Lema 5.1.3.
Dada una configuración $(\rho, \sigma, \boldsymbol{v}, \boldsymbol{w}) \in \mathcal{S}^*$, al aplicar cualquier giro $M \in \{U, D, L, R, F, B\}$, la configuración resultante $M \cdot (\rho, \sigma, \boldsymbol{v}, \boldsymbol{w}) = (\rho', \sigma', v', \boldsymbol{w}')$ cumple $\sum_i^8 v_i \equiv \sum_i^8 v_i'$ (mód 3) y $\sum_i^{12} w_i \equiv \sum_i^{12} w_i'$ (mód 2).

Demostración. Cada giro suma 1 el mismo número de veces que suma 2 en el vector de orientación de los cubiletes esquina, como se indica en la Proposición 3.4.1 por lo que no cambia el valor de $\sum_i^8 v_i'$ (mód 3).

Además, cada giro suma 1 en un número par de coordenadas del vector de orientación de los cubiletes borde, por lo que no modifica el valor de $\sum_i^{12} w_i'$ (mód 2). □

Con estos resultados podemos probar que las condiciones del teorema fundamental son necesarias.

Demostración del Teorema 5.1.1. Las configuraciones que se pueden alcanzar mediante giros a partir de la configuración resuelta son aquellas en la órbita de $(id_8, id_{12}, 0_8, 0_{12})$. Como $\text{sign}(id_8) = \text{sign}(id_{12})$ el Lema 5.1.2 nos dice que cualquier otra configuración alcanzada a partir de esta tendrá la misma paridad en la primera y segunda coordenada de la 4-tupla y por el Lema 5.1.3 no cambiará la suma de las coordenadas de los vectores de orientación en módulo 3 y 2 respectivamente. □

5.2. Algunos resultados útiles

En esta sección introduciremos tres resultados sobre movimientos de cubiletes esquina y borde que serán útiles para la demostración de algunas proposiciones, que a su vez se usarán para demostrar que las condiciones del teorema fundamental del cubo de Rubik son suficientes. Estos lemas se enuncian como afirmaciones dentro de las demostraciones de las proposiciones 11.6, 11.7, 11.8 y 11.9 en *Group Theory and the Rubik's Cube* de Janet Chen [4] y su demostración se deja como ejercicio para el lector. En este trabajo desarrollo dichas demostraciones.

Lema 5.2.1.
Dados dos cubiletes esquina C_1 y C_2 y dos cubículos esquina c_1', c_2' con $C_1 \neq C_2$ y $c_1' \neq c_2'$, existe una operación $M \in Rc_3$ que manda los cubiletes C_1 y C_2 en los cubículos c_1' y c_2' respectivamente.

Demostración. Para probar la afirmación del lema, basta encontrar una operación $M \in Rc_3$ que satisfaga las condiciones. Llevar el cubilete C_1 al cubículo c_1' es muy sencillo. Mediante los giros L, L^{-1}, R, R^{-1} se puede trasladar cualquier cubilete esquina a la cara U o a la cara D y mediante U^i ó D^i podemos mover el cubilete a cualquiera de los 4 cubículos esquina de dicha cara. Por lo tanto, podemos asumir que existe $M_1 \in Rc_3$ que lleva el cubilete C_1 al cubículo c_1'.

Si tras aplicar M_1 el cubilete C_2 ocupa el cubículo c_2', tomamos $M = M_1$ y hemos terminado. En caso contrario, queremos encontrar $M_2 \in Rc_2$ que lleve C_2 a c_2' sin mover C_1. Sin pérdida de generalidad podemos asumir que $c_1' =$ ufl, si no, podemos reorientar el cubo completo de forma que al cubículo c_1' le corresponda la etiqueta ufl y deshacer la reorientación al final. El siguiente paso es llevar el cubilete C_2 a la cara D (si no lo estaba tras aplicar M_1) mediante R, R^{-1}, B ó B^{-1} para no mover C_1.

Cuando C_2 esté en la cara D, podemos llevarlo por los 4 cubículos esquina de la cara D mediante D^i, con $i \in \{0,1,2,3\}$ y si c_2' está en la cara D, hemos terminado. Si por el contrario c_2' está en la cara U, podemos llevar C_2 al correspondiente cubículo de la cara D mediante D^i con $i \in \{0,1,2,3\}$ y llevarlo a la cara U mediante R, R^{-1}, B ó B^{-1}. Luego, existe M_2 que lleva el cubilete C_2 al cubículo c_2' sin mover el cubilete C_1. Por lo tanto, $M = M_1M_2$ lleva los cubiletes esquina C_1 y C_2 a los cubiletes c_1' y c_2' respectivamente.

□

Lema 5.2.2.
Dados tres cubiletes borde C_1, C_2 y C_3, existe una operación $M \in Rc_3$ que manda C_1 al cubículo uf, C_2 a ub y C_3 a db.

Demostración. Girando las caras R, L, F ó B podemos llevar el cubilete C_1 a la cara U y girando la cara U llevarlo a uf, luego existe una operación $M_1 \in Rc_3$ que lleva a C_1 a uf. Ahora, mirando a los cubiletes restantes, está claro que mediante un giro de la cara R, L ó B se puede llevar el cubículo C_3 a la cara D y girando la cara down llevarlo al cubículo df. Llamaremos a esta operación M_2, que además no cambia la posición del cubilete C_1. Antendiendo a los cubículos restantes, el cubilete C_2 debe estar en la cara B o en las caras L ó R. Mediante un giro L^i ó R^i con $i \in \{0,1,2,3\}$ podemos llevarlo a la cara B, tras lo cual, seguido de otro giro B^j con $j \in \{0,1,2,3\}$ para llevar a C_2 al cubículo ub. Llamamos a esta operación M_3, que no mueve el cubilete C_1 ni C_3. Finalmente, llevamos C_3 que estaba en el cubículo df a db mediante D^2. Por lo tanto, $M = M_1M_2M_3D^2$ lleva C_1 a uf, C_2 a ub y C_3 a db. □

Lema 5.2.3.
Dados dos cubiletes borde C_1 y C_2, existe una operación $M \in Rc_3$ que manda C_1 al cubículo ul, C_2 a ur.

Demostración. Primero, girando las caras R, L, F ó B podemos llevar el cubilete C_1 a la cara U y girando la cara U llevarlo a ul. Después, podemos llevar el cubilete C_2 a la cara D si no lo estaba, mediante giros de las caras F, B ó R que no mueven el cubilete C_1. Mediante D^i para algún $i \in \{0,1,2,3\}$ podemos llevar el cubilete C_2 al cubículo dr y con R^2 llevarlo a ur sin mover el cubilete C_1. □

5.3. Resolviendo el cubo en 4 etapas

En esta sección introduciremos una estrategia dividida en 4 etapas que nos permitirá resolver el cubo de Rubik. Estas 4 etapas se presentan como 4 proposiciones en *Group Theory and the Rubik's Cube* de Janet Chen [4] que adoptaremos en este trabajo.

La primera de las 4 proposiciones afirma que podemos llevar todos los cubiletes esquina a su cubículo correspondiente en la configuración resuelta, no necesariamente en la orientación adecuada. La segunda proposición prueba que una vez tenemos

los cubiletes esquina en sus respectivos cubículos, podemos orientarlos para que cada uno tenga la misma orientación que en la configuración resuelta. Una vez ahí, la idea es mover los cubiletes borde sin mover ningún cubilete esquina. La siguiente proposición prueba que podemos llevar los cubiletes borde a su cubículo en la configuración resuelta sin cambiar la posición de los cubículos esquina. En este punto tenemos todos los cubiletes en los cubículos que ocupan en la configuración resuelta. Sin embargo, los cubículos borde no tienen por qué estar orientados igual que en la configuración resuelta. La última proposición prueba que podemos orientar los cubiletes borde no orientados.

Proposición 5.3.1 ([Proposición 11.6, 4])**.**
Dada una configuración $(\rho, \sigma, \boldsymbol{v}, \boldsymbol{w}) \in \mathcal{S}^*$, en su órbita por Rc_3 existe una configuración de la forma $(id_8, \sigma', v', \boldsymbol{w}')$.

Demostración. La idea de la prueba es encontrar una operación $M \in Rc_3$ con $\phi_{esquina}(M) = \rho^{-1}$, o lo que es lo mismo, que $S_8 \subseteq im\,\phi_{esquina}$. Como toda permutación descompone en transposiciones, si consideramos S el conjunto S_8 de trasposiciones de , entonces $S_8 = \langle S \rangle$, por lo que es suficiente probar que $S \subseteq im\,\phi_{esquina}$.

Dada la transposición $(c_1, c_2) \in S$, donde c_1 y c_2 son dos cubículos esquina distintos y cualesquiera, encontramos $M \in Rc_3$ de forma que $\phi_{esquina}(M) = (c_1, c_2)$. Para construir M, primero consideramos la operación $M_0 = ([D, R], F)^3$ que cumple $\phi_{esquina}(M_0) = (3, 8)$. El corchete denota un conmutador que se define en la Notación 5.3.1. Para comprobar esta afirmación, diríjase a la Figura A.2 del Apéndice A, en la que sólo los cubiletes esquina en los cubículos (3) (*ubr*) y (8) (*drb*) se transponen, mientras que el resto de cubiletes esquina permanecen invariantes.

Por el Lema 5.2.1 existe una operación $M' = (\pi', \tau', \phi', \psi') \in Rc_3$ que manda el cubilete del cubículo c_1 al cubículo (3) y el del c_2 al (8). De esta forma

$$\begin{aligned}\phi_{esquina}(M' M_0 M'^{-1}) &= \phi_{esquina}(M'^{-1})\phi_{esquina}(M_0)\phi_{esquina}(M') \\ &= \pi'^{-1}(3, 8)\pi' \\ &= (\pi'^{-1}(3), \pi'^{-1}(8)) \\ &= (c_1, c_2)\end{aligned}$$

con lo que $S \subseteq \text{im}\phi_{\text{esquina}}$. Por lo tanto, existe $M \in Rc_3$ de forma que $\phi_{esquina}(M) = \rho^{-1}$, así,

$$M \cdot (\rho, \sigma, \boldsymbol{v}, \boldsymbol{w}) = (id_8, \sigma', \boldsymbol{v}', \boldsymbol{w}').$$

□

Notación 5.3.1.
Dados dos giros $X, Y \in \{R, L, U, D, F, B\}$, el conmutador de X e Y es $[X, Y] := XYX^{-1}Y^{-1}$.

Proposición 5.3.2 ([Proposición 11.7, 4])**.**
Dada una configuración $(id_8, \sigma, \boldsymbol{v}, \boldsymbol{w})$ con $\sum_i^8 v_i \equiv 0$ (mód 3), en su órbita por Rc_3 existe una configuración de la forma $(id_8, \sigma', 0_8, \boldsymbol{w}')$.

Demostración. Partiendo de la configuración inicial, dado que $\sum_i^8 v_i \equiv 0$, podemos llegar a otra en la que haya el mismo número de coordenadas que sean 1 y 2 en el

vector de orientación de los cubiletes esquina, sin mover los cubiletes esquina de su correspondiente cubículo, sumando 1 y 2 en las coordenadas deseadas sin cambiar los cubiletes esquina de su cubículo:

Sean c_1 y c_2 dos cubículos esquina cualesquiera. Veremos que existe $M \in Rc_3$ que cambia las orientaciones de los cubiletes esquina que ocupan dichos cubículos pero no afecta a ningún otro cubilete esquina. Además, esa operación M rota el cubilete C_1 que ocupa el cubículo c_1 en sentido horario y el cubilete C_2 que ocupa el cubículo c_2 en sentido antihorario. Al girar un cubilete ubicado en el cubículo esquina i-ésimo en sentido horario, se modifica el vector v (tercera coordenada del vector de configuración) de forma que suma 2 en la coordenada i-ésima de v (en módulo 3) y se suma 1 al girar en sentido antihorario (en módulo 3).

Al igual que en la prueba del Lema 5.3.1, encontraremos primero una operación $M_0 \in Rc_3$ que cambie la orientación de sólo 2 cubiletes esquina cualesquiera sin mover ningún cubilete esquina de su cubículo. Tomamos $M_0 = (DR^{-1})^3(D^{-1}R)^3$ que se puede escribir en descomposición de ciclos disjuntos como $(dfr, rdf, frd)(drb, rbd, bdr)(df, dr, fr, ur, br, db, dl)$. Esto se comprueba en la Figura A.3 del Apéndice A. Luego, si C_1 y C_2 son cubiletes en los cubículos dfr y drb respectivamente, el primero gira en sentido antihorario y el segundo en sentido horario.

Ahora, dados dos cubiletes C_1 y C_2 no necesariamente en los cubículos dfr y drb, por el Lema 5.2.1, sabemos que existe una operación $M' \in Rc_3$ que manda el cubilete C_1 al cubículo dfr y el cubilete C_2 al cubículo drb, luego, la operación $M = M'M_0M'^{-1}$ cambia la orientación del cubículo C_1 y C_2 en sentido antihorario y horario respectivamente y no mueve los demás cubiletes esquina.

De esta forma obtenemos el mismo número de coordenadas con un 1 o con un 2. Aplicando la misma estrategia, tomando pares de cubiletes con un 1 y con un 2, giramos el primero en sentido antihorario y el segundo antihorario, llegando al resultado deseado. □

Proposición 5.3.3 ([Proposición 11.8, 4]).
Dada una configuración $(id_8, \sigma, 0_8, \boldsymbol{w}) \in \mathcal{S}^*$ con $\text{sign}(\sigma) = 1$, en su órbita por Rc_3 existe una configuración de la forma $(id_8, id_{12}, 0_8, \boldsymbol{w}')$.

Demostración. La estrategia de esta demostración es encontrar una operación $M \in Rc_3$ que cumpla $\phi_{esquina}(M) = id_8$ y $\phi_{borde}(M) = \sigma^{-1}$ y que mantenga la orientación de los cubiletes esquina.

Como $\text{sign}(\sigma) = 1$, entonces $\sigma^{-1} \in A_{12}$, donde A_{12} es el grupo alternado de 12 elementos y por tanto. Como A_{12} está generado por 3-ciclos, basta ver que existe M con las condiciones dadas para cualquier 3-ciclo (c_1, c_2, c_3) pues σ^{-1} será una combinación de estas.

La operación $M_0 = LR^{-1}U^2L^{-1}RB^2$ descompone como (ub, uf, db) (ver Figura A.4 del Apéndice A) y cumple las condiciones requeridas para M. Por el Lema 5.2.2, dados C_1, C_2 y C_3 tres cubiletes borde de los cubículos c_1, c_2 y c_3 respectivamente, existe $M' \in Rc_3$ que manda C_1 a ub, C_2 a uf y C_3 db. Luego $M = M'M_0M'^{-1}$ tiene una descomposición (c_1, c_2, c_3). □

Proposición 5.3.4 ([Proposición 11.9, 4]).
Dada una configuración $(id_8, id_{12}, 0, \boldsymbol{w}) \in \mathcal{S}^*$ con $\sum_j^{12} w_j \equiv 0$ (mód 2), en su órbita por Rc_3 existe la configuración $(id_8, id_{12}, 0, 0)$.

Demostración. Como $\sum_j^{12} w_j \equiv 0$ (mód 2), existe un número par de coordenadas no nulas, luego si probamos que, dado cualquier par de cubiletes borde, podemos cambiar su orientación, el lema queda probado, ya que podemos cambiar la orientación de cada par de cubiletes a los que corresponden las coordenadas no nulas.

La operación

$$M_0 = LR^{-1}FLR^{-1}DLR^{-1}BLR^{-1}ULR^{-1}F^{-1}LR^{-1}D^{-1}LR^{-1}B^{-1}LR^{-1}U^{-1}$$

que se ilustra en la Figura A.5 del Apéndice A, es descrita por la permutación $(lu, ul)(ru, ur)$, es decir, cambia la orientación de los cubiletes en los cubículos lu y ru y no afecta a ningún otro. Luego, para cada par de cubiletes C_1 y C_2 que corresponden a coordenadas no nulas del vector w, existe una operación $M' \in Rc_3$ que lleva C_1 a lu y C_2 a ru por el Lema 5.2.3. Luego $M = M'M_0M'^{-1}$ cambia la orientación de C_1 y C_2 y hemos concluido la prueba. □

Demostración del Teorema 5.1.1.
Para probar que las condiciones del teorema son suficientes, basta probar la existencia de una operación $M \in Rc_3$ que resuelva cualquier cubo cuya configuración inicial cumpla las condiciones del teorema. Esto es directo a partir de las Proposiciones 5.3.1-5.3.4 aplicando las condiciones del teorema. Los Lemas 5.1.2 y 5.1.3 aseguran que las condiciones de signo de la primera y segunda coordenada, y la suma de los valores de los vectores de orientación se mantengan en las cuatro etapas.

□

El teorema fundamental del cubo permite calcular el cardinal del conjunto $\mathcal{S}$ de configuraciones del cubo de Rubik y por tanto el del grupo del cubo de Rubik. Para ello, primero introduciremos tres observaciones como lemas que serán útiles para probar la cardinalidad del grupo de Rubik.

Lema 5.3.5.
Existe el mismo número de configuraciones $(\rho, \sigma, \mathbf{v}, \mathbf{w}) \in \mathcal{S}^*$ con $\text{sign}(\rho) = \text{sign}(\sigma)$ que $\text{sign}(\rho) \neq \text{sign}(\sigma)$.

Demostración. Construimos una biyección entre los dos conjuntos, que a cada configuración con $\text{sign}(\rho) = \text{sign}(\sigma)$, le asignamos la configuración con los cubiletes de los cubículos urf y ufl intercambiados que tendrá $\text{sign}(\rho) \neq \text{sign}(\sigma)$. □

Lema 5.3.6.
Existe el mismo número de configuraciones $(\rho, \sigma, \mathbf{v}, \mathbf{w}) \in \mathcal{S}^*$ con $\sum_i^8 v_i \equiv 0$, con $\sum_i^8 v_i \equiv 1$ ó con $\sum_i^8 v_i \equiv 2$.

Demostración. Construimos una biyección entre los tres conjuntos, que a cada configuración con $\sum_i^8 v_i \equiv 0$ le asignamos la configuración que gira el cubilete del cubículo ufl una vez en sentido antihorario, que dará una configuración con $\sum_i^8 v_i \equiv 1$. A cada configuración con $\sum_i^8 v_i \equiv 1$ le asignamos la configuración obtenida rotando el cubilete del cubículo ufl una vez en sentido antihorario obteniendo una configuración con $\sum_i^8 v_i \equiv 2$ □

Lema 5.3.7.
Existe el mismo número de configuraciones $(\rho, \sigma, \mathbf{v}, \mathbf{w}) \in \mathcal{S}^*$ con $\sum_j^{12} w_j \equiv 0$ ó con $\sum_j^{12} w_j \equiv 1$.

Demostración. Construimos una biyección entre los dos conjuntos, que a cada configuración con $\sum_j^{12} w_j \equiv 0$ le asignamos la configuración que gira el cubilete del cubículo uf una vez de modo que $\sum_j^{12} w_j \equiv 1$. □

Proposición 5.3.8.
El número de posibles posiciones del cubo de Rubik es

$$|\mathcal{S}| = \frac{|\mathcal{S}^*|}{12} = 2^{27} \cdot 3^{14} \cdot 5^3 \cdot 7^2 \cdot 11 = 43\,252\,003\,274\,489\,856\,000 \approx 2.3 \cdot 10^{19}$$

Demostración. Comenzamos primero con un conjunto configuraciones ampliado

$$\mathcal{S}^* = S_8 \times S_{12} \times \mathbb{Z}_3^8 \times \mathbb{Z}_2^{12}$$

que tiene cardinal

$$|\mathcal{S}| = 8! \cdot 12! \cdot 3^8 \cdot 2^{12}$$

El conjunto $\mathcal{S}$ de configuraciones es el subconjunto de $\mathcal{S}^*$ tal que

- Del Lema 5.3.5 deducimos que la mitad de las permutaciones de los cubiletes borde y esquina son posibles por la condición de paridad a) del Teorema 5.1.1.
- Del Lema 5.3.6 deducimos que un tercio de las orientaciones son posibles por la condición b) del Teorema 5.1.1.
- Del Lema 5.3.7 deducimos que la mitad de las orientaciones de las esquinas son posibles por la condición de paridad c) del Teorema 5.1.1.

de esta forma

$$|\mathcal{S}| = \frac{|\mathcal{S}^*|}{12} = 2^{27} \cdot 3^{14} \cdot 5^3 \cdot 7^2 \cdot 11$$

□

A partir del primer teorema fundamental, en *Group theory and the Rubik's cube* de Lindsey Daniel [5] proponen el segundo teorema fundamental del cubo de Rubik, que da un criterio sobre las operaciones que son posibles sobre el cubo.

Teorema 5.3.9 (**Segundo Teorema Fundamental de Cubo de Rubik** (Teorema 4.12 [5])**.**
Dada una 4-tupla $M := (\pi, \tau, \phi, \psi)$, define una operación sobre el cubo de Rubik, es decir, $M \in Rc_3$ si y solamente si se satisfacen:

a Las permutaciones que describen los desplazamientos de los cubiletes esquina y borde tienen la misma paridad .

b El número total módulo 3 de ciclos de cubiletes esquina girado en sentido horario es igual al número de cubiletes esquina girado en sentido antihorario.

c Tiene un número par de cubiletes borde reorientados.

Demostración. Comenzamos probando la implicación $\Rightarrow$). Sea $M := (\pi, \tau, \phi, \psi) \in Rc_3$ una operación sobre el cubo de Rubik.

a Directo a partir del Lema 5.1.2.

b Una operación $M \in Rc_3$ es la concatenación de una secuencia de giros $M = M_1 \cdots M_n$ con $M_i \in \{R, L, U, D, F, B\}$ para $i = 1, ..., n$, si escribimos $M_i = (\pi_i, \tau_i, \phi_i, \psi_i)$ como en la Proposición 3.4.1, cada M_i tiene el mismo número de giros en sentido horario que en sentido antihorario, por lo tanto, la operación final debe tener el mismo número de cubiletes rotados en sentido horario que antihorario (módulo 3).

c Reorientar un cubilete implica aumentar el valor de la coordenada j-ésima (correspondiente al cubículo que ocupa) del vector w en 1 (mód 2). Dado que las operaciones llevan elementos de $\mathcal{S}$ en $\mathcal{S}$, por el primer teorema fundamental $\sum_{j=1}^{12} w_j \equiv 0$ mód 2 y por tanto hay un número par de cubiletes reorientados.

Para la implicación contraria tomamos $M := (\pi, \tau, \phi, \psi)$ que satisface las 3 condiciones del teorema y la aplicamos sobre la configuración resuelta $(id_8, id_{12}, 0_8, 0_{12})$, obtenemos una nueva configuración $p = (\rho, \sigma, \boldsymbol{v}, \boldsymbol{w})$. Por la primera condición $\text{sign}(\rho) = \text{sign}(\sigma)$. Por la segunda condición $\sum_{i=1}^{8} v_i \equiv 0$ (mód 3) y por la tercera condición $\sum_{j=1}^{12} w_j \equiv 0$ (mód 2), luego $p \in \mathcal{S}$ por lo que existe $M' \in Rc_3$ tal que $M' \cdot (id_8, id_{12}, 0_8, 0_{12}) = p$. Como M y M' tienen el mismo efecto sobre el cubo de Rubik $M = M'$ y por tanto $M \in Rc_3$ es una operación posible sobre el cubo de Rubik. □

Ejemplo 5.3.1.
Gracias al primer teorema fundamental del cubo de Rubik sabemos que el cubo en la Figura 5.1 no se puede resolver sin desensamblar los cubiletes.

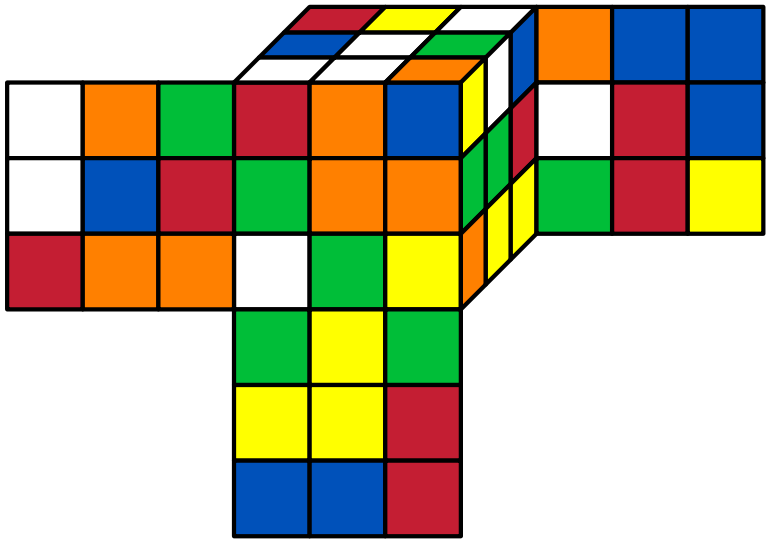

FIGURA 5.1: Cubo de Rubik irresoluble.

Capítulo 6

El Algoritmo de Dios y el Cubo de Rubik

Resolver el cubo de Rubik en el menor tiempo, implica trabajo de memorización de algoritmos de resolución, destreza psicomotriz y tener el mecanismo del cubo en condiciones óptimas que permita rotar las caras con la mayor facilidad posible. Sin embargo, desde el punto de vista matemático, resulta más interesante encontrar el camino más corto al cubo resuelto, es decir, encontrar la palabra más corta que defina la operación que resuelva el cubo. En este capítulo se repasará la resolución del número mínimo de giros para resolver cualquier cubo obtenido por Rikicki et al. [9], aunque sin entrar en grades detalles.

El número de configuraciones posibles del cubo, como se indica en la Proposición 5.3.8 es del orden de 10^{19}, es decir, se podría llenar la superficie de la tierra con cubos distintos de 3 cm de lado sin que ninguno se repitiera. A pesar de ser el número de configuraciones posibles tan grande, se conjeturó que partiendo de cualquier configuración inicial, existe siempre una operación de algo más de 20 giros [11] que resuelva el cubo. Al algoritmo que resuelve cada configuración en el menor número de pasos posible se denomina Algoritmo de Dios, es decir, de acuerdo con las Definiciones 2.7-2.10, encuentra la palabra de menor longitud que define la operación que resuelve el cubo. Además, se llama Número de Dios al máximo de las longitudes de estas operaciones.

El Número de Dios en matemáticas es el diámetro del grafo del cubo de Rubik, en el cual dos configuraciones están unidas por una arista si distan un cuarto de vuelta (o media vuelta dependiendo de la métrica). Dicho grafo es un tipo especial de grafo denominado como grafo de Cayley que se introduce en la Definición 1.18 del Capítulo 1 .

6.1. Grafo de Cayley del Cubo de Rubik

De acuerdo con la Definición 1.18, para crear el grafo del cubo de Rubik, en el que las configuraciones sean los vértices y dos configuraciones estén unidas por una arista si distan en un giro, podemos tomar como grupo el Grupo del Cubo de Rubik Rc_3, y el subconjunto cerrado sería $S = \{U, R, F, L, B, D, U^{-1}, R^{-1}, F^{-1}, L^{-1}, B^{-1}, D^{-1}, U^2, R^2, F^2, L^2, B^2, D^2\}$ para la métrica de media vuelta y $S' = \{U, R, F, L, B, D, U^{-1}, R^{-1}, F^{-1}, L^{-1}, B^{-1}, D^{-1}\}$ en la métrica de un cuarto de vuelta. En la Figura 6.1 se muestra una sección del grafo de Cayley del cubo de Rubik, con la configuración resuelta y las configuraciones adyacentes en la métrica de un cuarto de vuelta [3].

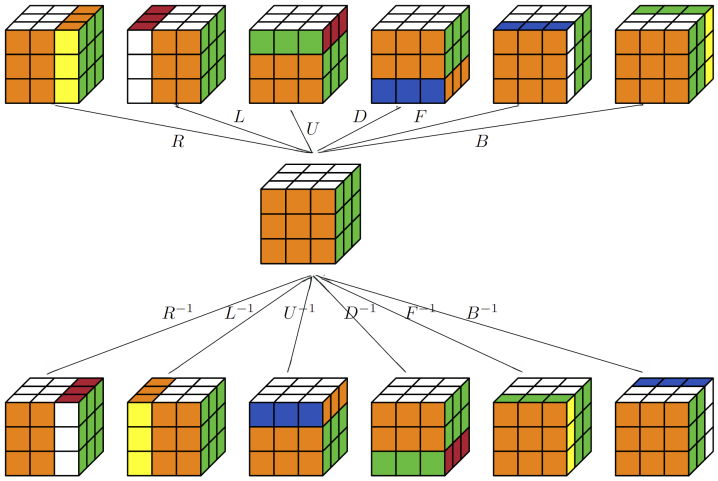

FIGURA 6.1: Grafo de Cayley de los nodos adyacentes a la configuración resuelta del cubo de Rubik.

6.2. El Número de Dios en la métrica de media vuelta

El número de Dios o diámetro del grafo del cubo de Rubik se conjeturó que debía ser 20 ó ligeramente superior. En lo que sigue, si no se especifica lo contrario se hablará siempre en términos de la métrica de media vuelta.

6.2.1. Primeras cotas al Número de Dios

La primera cota inferior se consiguió en 1980 mediante un argumento de conteo que demostraba que hacían falta al menos 18 movimientos para llegar a ciertas configuraciones (desde la configuración resuelta), pero no se probó que hubiera configuraciones que requirieran más movimientos [11]. Las primeras cotas superiores se obtuvieron en 1981. Thistlethwaite [12] probó la existencia de configuraciones que requieren al menos 17 movimientos y daba un algoritmo que resolvía el cubo a lo sumo en 52 movimientos. Este algoritmo es complicado y difícil de memorizar por lo que sólo es práctico para ordenadores. La estrategia que toma no es colocar ciertos cubiletes en los cubículos que les corresponde en la configuración resuelta, sino que trabaja con todas las piezas, restringiéndolas a menos posibilidades hasta que solo queda una posibilidad para cada cubilete que es la de la configuración resuelta:

Primero llega a una configuración que puede ser resuelta sin usar giros de un cuarto de vuelta de las caras U y D. Después, sin usar cuartos de vuelta U y D se llega a una configuración que se puede resolver sin giros de un cuarto de vuelta de las caras F y B. Así se acaba llegando a una configuración en la que no hace falta ningún giro de cuarto de vuelta y el cubo se puede resolver solamente con giros de media vuelta. La idea es ir restringiendo las configuraciones del grupo $RC_3 = G_0 = \langle L, R, F, B, U, D\rangle$ a $G_1 = \langle L, R; F, B, U^2, D^2\rangle$, después a $G_2 = \langle L, R, F^2, B^2, U^2, D^2\rangle$, después a $G_3 = \langle L^2, R^2, F^2, B^2, U^2, D^2\rangle$ y finalmente a $G_4 = I$.

Esta estrategia se puede ver como una secuencia de grupos anidados y en cada etapa se busca la solución del grupo cociente G_i/G_{i+1} [12].

6.2.2. El valor definitivo

Rikicki et at. [9] fueron los primeros en resolver el problema del Número de Dios para la métrica de media vuelta, obteniendo de forma computacional usando fuerza bruta, que el diámetro del grupo del cubo de Rubik en esta métrica es 20.

Almacenar 4.3×10^{19} configuraciones del cubo de Rubik de forma directa es imposible. Aunque cada configuración ocupase 1 Byte de memoria, harían falta más de 10 millones de TeraBytes de memoria, por lo tanto se empleó una estrategia de divide y vencerás. Separaron el grupo del cubo de Rubik en subconjuntos, de forma que cada subconjunto se resuelva rápido y de forma independiente.

La idea detrás de la estrategia empleada es la siguiente: un posible enfoque para resolver el cubo podría ser resolver primero la cara superior. Un argumento combinatorio sencillo, como el que nos daba el número total de configuraciones del cubo de Rubik, nos muestra que existen 2.6×10^{10} configuraciones que pueden tomar los cubiletes de la cara U (los que en la configuración resuelta ocupan los cubículos de la cara U). Para resolver la cara superior, buscamos la distancia desde la posición de partida hasta la resolución de la cara superior y construimos una tabla con dichas distancias. Esta tabla se llama *pattern database* y permite generar secuencias de soluciones incluyendo algunas óptimas.

En algunas ocasiones, la operación que resuelva la cara superior también resolverá el cubo entero. De hecho, todas estas operaciones que resuelven la cara superior, resuelven el cubo completo para alguna configuración inicial dada. Para encontrar dicha configuración basta aplicar la operación inversa sobre el cubo resuelto. Algo que estas dos configuraciones (la que al aplicar dicha operación se resuelve sólo la cara superior y la que resuelve el cubo entero) tienen en común es la posición inicial de los cubiletes de la cara U . Por lo tanto, la posición de los cubiletes de la cara U define una partición del grupo en subconjuntos, lo que permite resolver cada subconjunto por separado. El número de subconjuntos es del orden de 2.6×10^{10} (número de posiciones que pueden tomar los cubiletes de la cara U) y el cardinal de cada subconjunto es 1.7×10^{9} (número de configuraciones fijada la posición de los cubiletes up).

Fijado un subconjunto, todas las configuraciones del mismo tendrán colocaciones diferentes de los cubiletes de la cara U y dada una colocación de los cubiletes de la cara U, existirá una única configuración en cada subconjunto de la partición con dicha colocación. Esto quiere decir que si tenemos una operación que resuelve la cara superior para una configuración de un subconjunto, entonces solamente resolverá la cara superior para esa configuración en ese subconjunto. Además, existirá una única configuración en cada uno de los otros subconjuntos tal que al aplicar esta operación se resuelva la cara superior.

Podemos extender esta noción a un subobjetivo cualquiera y definir particiones. Consideramos un subgrupo H del cubo y podemos tomar H como el objetivo al que queremos llegar, luego una clase a derecha C vendrá dada por $C = H \cdot p$ donde p es un representante arbitrario de C. Si aplicamos una búsqueda en profundidad d, encontraremos todas las operaciones m de longitud d tal que $p \cdot m \in H$. Cada operación m resuelve exactamente una configuración de C, por lo tanto, si m^{-1} es el inverso de m, entonces $m^{-1} \in C$, ya que $p \cdot m = h$ para algún $h \in H$, luego $p = h \cdot m^{-1}$ y por tanto $h' \cdot p = m^{-1}$ con lo que $m^{-1} \in H \cdot p = C$.

Así registramos la posición de cada configuración. Una vez completada la búsqueda en profundidad d, tendremos registradas las posiciones que están a dicha distancia de H. Además, si el subgrupo H se elije cuidadosamente, existirán giros que aplicados sobre cualquier posición de H, la configuración resultante seguirá estando en H. Esto permite extender el *pattern database* de profundidad d, con operaciones que terminen con estos giros. Esta estrategia se llama *prepass* y toma un papel importante en la búsqueda del Número de Dios.

A partir de ahora, el subgrupo H no será un subgrupo genérico, sino el subgrupo del segundo objetivo del algoritmo de 4 objetivos de Thistlethwaite [12] y el primero del algoritmo de dos fases de Kociemba [9].

Una forma de visualizar el subgrupo H es la siguiente: dar el mismo color a las caras opuestas, y eliminar las pegatinas a las caras F, B, L, R de aquellos cubiletes que tocan la cara U ó la cara D. Esto se ilustra en la parte superior derecha en la Figura 6.2.

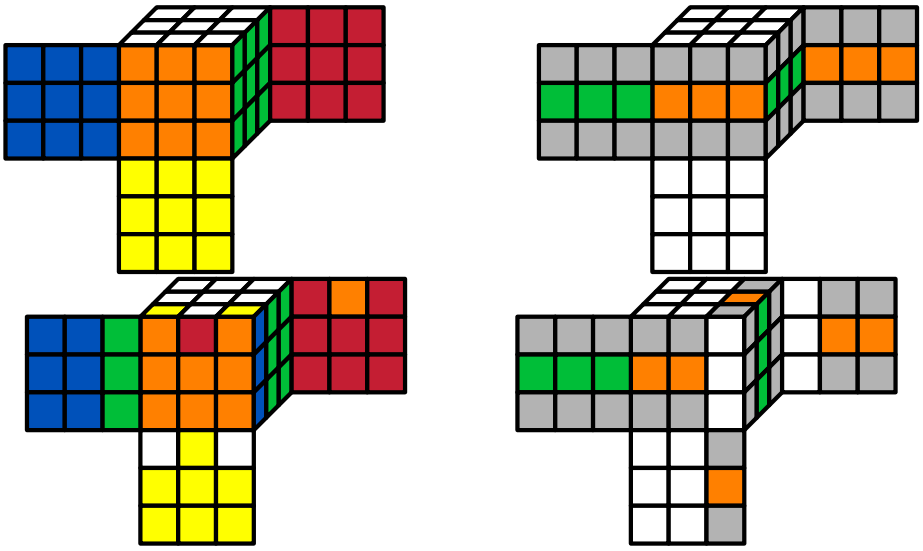

FIGURA 6.2: (a) Coloración normal del cubo, (b) Etiquetado usando la noción del subgrupo H, (c) posición generada usando $R\,L^{-1}\,U^2 L\,R^{-1}$ y (d) la clase lateral $H \cdot R$

Este cubo es invariante por cualquier acción generada por el conjunto $\mathcal{Z} = \{U, U^2, U^3, D, D^2, D^3, F^2, B^2, L^2, R^2\}$. Así tomamos

$$H = \langle \mathcal{Z} \rangle \tag{6.1}$$

Hay 8! permutaciones de los cubiletes esquina sin cambiar de color, hay 4! permutaciones de los bordes verde y rojo y 8! permutaciones de los bordes con una cara blanca. Dado que cada giro es una permutación par sobre los cubiletes, $|H| = 8!8!4!/2 = 19\,508\,428\,800$. Dividimos el grupo del cubo de Rubik en 2 217 093 120 clases laterales, cada una con 19 508 428 800 posiciones, accesible para un ordenador moderno. Elegimos esta división ya que podemos resolver todas las posiciones de cualquier clase a derecha de H en a lo sumo 20 giros de forma rápida mediante un método similar al empleado en el algoritmo de Kociemba.

¿Cómo podemos saber si una configuración está en H? Por ejemplo, ¿cómo se puede ver que la configuración generada por $RL^{-1}U^2LR^{-1}$ está en H? En efecto, dicha configuración también se puede obtener mediante $F^2U^2R^2F^2R^2U^2R^2F^2R^2$, por lo que es un elemento de H. Esto se puede comprobar mediante fuerza bruta o usando algoritmos de estabilizadores de subgrupos.

El subgrupo H también muestra ciertas simetrías. Definiendo relaciones de equivalencia en las clases laterales de H, encontramos 138 639 780 clases de equivalencia que tenemos que resolver. Otra descomposición en subgrupos más pequeños permite reducir este número a 55 882 296.

6.2.3. El algoritmo de búsqueda de soluciones

Para encontrar palabras o secuencias de giros que resuelvan la cara superior (o el subproblema correspondiente) se usa un algoritmo de búsqueda en profundidad, de forma que si tenemos que encontrar una solución en a lo sumo n giros, y hemos empleado más de n para llegar a la configuración actual, no podremos encontrar una solución y habrá que retroceder. Esto daría lugar al algoritmo búsqueda de Thislethwaite:

Entrada: *p*, *secuencia*, *resto*
Resultado: Secuencias registradas
procedure `buscar`(*p*, *secuencia*, *resto*)**:**
  si *dist*[*p*] > *resto* **entonces**
    devolver;
  fin
  si *resto* == 0 **entonces**
    registrar(*secuencia*);
  fin
  en otro caso
    para *movimiento m en movimientos* **hacer**
      `buscar`(*p.mover(m)*, *secuencia.agregar(m)*, *resto* − 1);
    fin
  fin
end

Algoritmo 2: Algoritmo de Thislethwaite

La distancia media dada por este algoritmo es 10, por lo que el algoritmo de búsqueda en profundidad funciona muy rápido, con el orden $\mathcal{O}(d)$ para hallar una solución donde d es el número de giros que requiere este movimiento.

Para resolver un conjunto de la partición hay que registrar las posiciones que ya han sido resueltas y las que no, por lo que hacemos la operación de **registar()**. Asignamos un índice a cada posición en el conjunto y generamos una tupla booleana que llamaremos mapa de bits para registrar las configuraciones ya resueltas.

Aplicando el algoritmo de búsqueda en profundidad, se pueden generar soluciones de distintas longitudes para la misma configuración, de forma que la de menor longitud será la óptima. Este es el principio del algoritmo de búsqueda en profundidad iterado.

Se emplean dos técnicas para resolver las clases laterales. La primera es muy rápida y enumera secuencias canónicas de giros de una longitud fija y marca su posición en el mapa de bits. Las secuencias canónicas se detallan en la siguiente sección. Para

longitudes cortas existen pocas secuencias canónicas pero para longitudes mayores el número de posiciones aumenta exponencialemente por lo que lleva mayor tiempo computacional.

La segunda técnica empleada es el *prepass*, que toma un conjunto de configuraciones y lo extiende rápidamente con todas las operaciones del conjunto $\mathcal{Z}$. Esta es la parte esencial del programa de Rokicki, donde se emplea el mayor esfuerzo computacional, por lo que la elección de un subgrupo adecuado como H es necesaria.

6.3. Secuencias canónicas

Existen diferentes palabras que definen la misma operación cómo UD^2 que genera la misma configuración que D^2U. Además, existen otras que son subóptimas como UU^2 y deben ser evitadas, ya que se llega al mismo resultado con U^{-1}, lo que quiere decir que haríamos dos búsquedas llegando a la misma configuración, sin embargo, con un camino recorreríamos una distancia de 2 pasos y con el otro de 1 solo paso. Para evitar estas redundancias en la búsqueda en profundidad, emplearemos secuencias canónicas de giros. En el ejemplo anterior, U^{-1} sería la secuencia canónica y UU^2 no por lo que emplear dichas secuencias canónicas nos evitaría hacer una búsqueda con la segunda secuencia.

Comenzamos con un método de álgebra lineal para determinar el número de secuencias canónicas de longitud n de un conjunto $\mathcal{Z}$, que denotaremos por $q_n(\mathcal{Z})$. Ordenamos este conjunto $\mathcal{Z}$

$$\mathcal{Z} = \{U, U^2, U^{-1}, F, F^2, F^{-1}, R, R^2, R^{-1}, D, D^2, D^{-1}, B, B^2, B^{-1}, L, L^2, L^{-1}\}, \quad (6.2)$$

Ahora, dados dos giros dos giros $M_i, M_j \in \mathcal{Z}$, donde M_i y M_j son el i-ésimo giro y j-ésimo elemento del conjunto ordenado $\mathcal{Z}$, la secuencia M_iM_j es canónica si y solamente si la entrada (i, j) de la matriz C, es 1, donde C es una matriz 18×18 dada por:

$$C = \begin{pmatrix} Z & W & W & W & W & W \\ W & Z & W & W & W & W \\ W & W & Z & W & W & W \\ Z & W & W & Z & W & W \\ W & Z & W & W & Z & W \\ W & W & Z & W & W & Z \end{pmatrix}, \quad (6.3)$$

donde

$$W = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \qquad \text{y } Z = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad (6.4)$$

Si tomamos el vector $a = (1, 1, ..., 1)$, $a^\top C$ será un vector cuya coordenada i-ésima indica el número de secuencias canónicas de dos giros, cuyo último elemento es el i-ésimo elemento de $\mathcal{Z}$. Como $a^\top C = (12, ..., 12, 18, ..., 18)$ con nueve 12 y nueve 18, la primera coordenada del vector muestra que existen 12 secuencias canónicas de dos giros donde el último giro es U. En efecto, para ser canónica, el primer giro debe

ser alguna potencia de F, R, B, L ya que hay que evitar secuencias de Us y los giros D deben ir después de U. Haciendo $a^\top Ca = 243$ obtenemos $q_2(\mathcal{Z})$. En general

$$q_n(\mathcal{Z}) = a^\top C^{n-1} a \tag{6.5}$$

esto da lugar a la relación de recurrencia

$$q_n(\mathcal{Z}) = 12q_{n-1}(\mathcal{Z}) + 18q_{n-2}(\mathcal{Z}) \qquad (n \geq 3) \tag{6.6}$$

En la Tabla 5.2 de Rokicki [9] se puede observar como utilizando secuencias canónicas hasta profundidad 16, se recorre un número de configuraciones bastante cercano al número real de posiciones del cubo de Rubik, lo que indica que basar la búsqueda en secuencias canónicas ayuda a eliminar muchas secuencias ineficientes.

Bibliografía

[1] Christoph Bandelow. «The Mathematical Model». En: *Inside Rubik's Cube and Beyond*. Boston, MA: Birkhäuser Boston, 1982, págs. 26-55. ISBN: 978-1-4684-7779-5. DOI: 10.1007/978-1-4684-7779-5_2. URL: https://doi.org/10.1007/978-1-4684-7779-5_2.

[2] Arne Brondsted. *An introduction to convex polytopes*. Vol. 90. Springer Science & Business Media, 2012.

[3] Daniel Bump y Daniel Auerbach. *Crystal Bases: Representations and Combinatorics*. http://sporadic.stanford.edu/bump/match/morepolished.pdf. Accessed: 2024-09-03. 2006.

[4] JJ Chen. *Group theory and the Rubik's cube*. 2004. URL: https://people.math.harvard.edu/~jjchen/docs/Group%20Theory%20and%20the%20Rubik's%20Cube.pdf.

[5] Lindsey Daniels. «Group theory and the Rubik's Cube». En: *Lakehead Universityc* (2014).

[6] Alexander H Frey Jr y David Singmaster. *Handbook of cubik math*. ISD LLC, 2020. ISBN: 9780718848248.

[7] J.A. Gallian. *Contemporary Abstract Algebra*. Textbooks in Mathematics. CRC Press, 2021. ISBN: 9781000337334.

[8] *Max Park Récords Personales Actuales*. https://www.worldcubeassociation.org/persons/2012PARK03.

[9] Tomas Rokicki et al. «The Diameter of the Rubik's Cube Group Is Twenty». En: *SIAM J. Discret. Math.* 27 (2013), págs. 1082-1105. DOI: 10.1137/120867366.

[10] K.H. Rosen. *Discrete Mathematics and Its Applications*. McGraw-Hill, 2019. ISBN: 9781260091991. URL: https://books.google.es/books?id=T_K9tgEACAAJ.

[11] David Singmaster. *Notes on Rubik's magic cube*. Enslow Pub Incorporated, 1981.

[12] M. Thistlethwaite. *52-move algorithm for Rubik's Cube*. https://www.jaapsch.net/puzzles/thistle.htm. Último acceso: 2023-09-12.

[13] Keshet Weinstein. «The slice group of the pyraminx». Tesis doct. California State Polytechnic University, Pomona, 2022.

[14] Gerald Jiarong Xu y David Xianfeng Gu. «Solving Megaminx puzzle With Group Theory». En: (2018).

Apéndice A

Operaciones empleadas en el trabajo

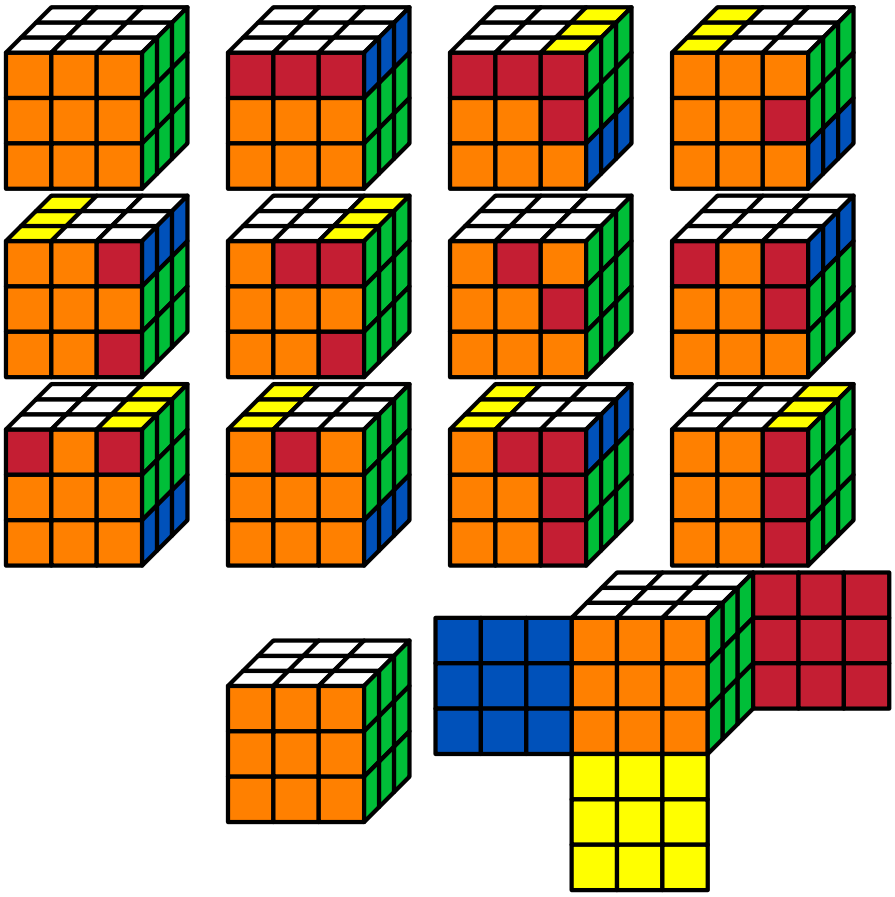

FIGURA A.1: Secuencia de movimientos de $(U^2R^2)^6$. La última figura es la configuración final con el cubo extendido.

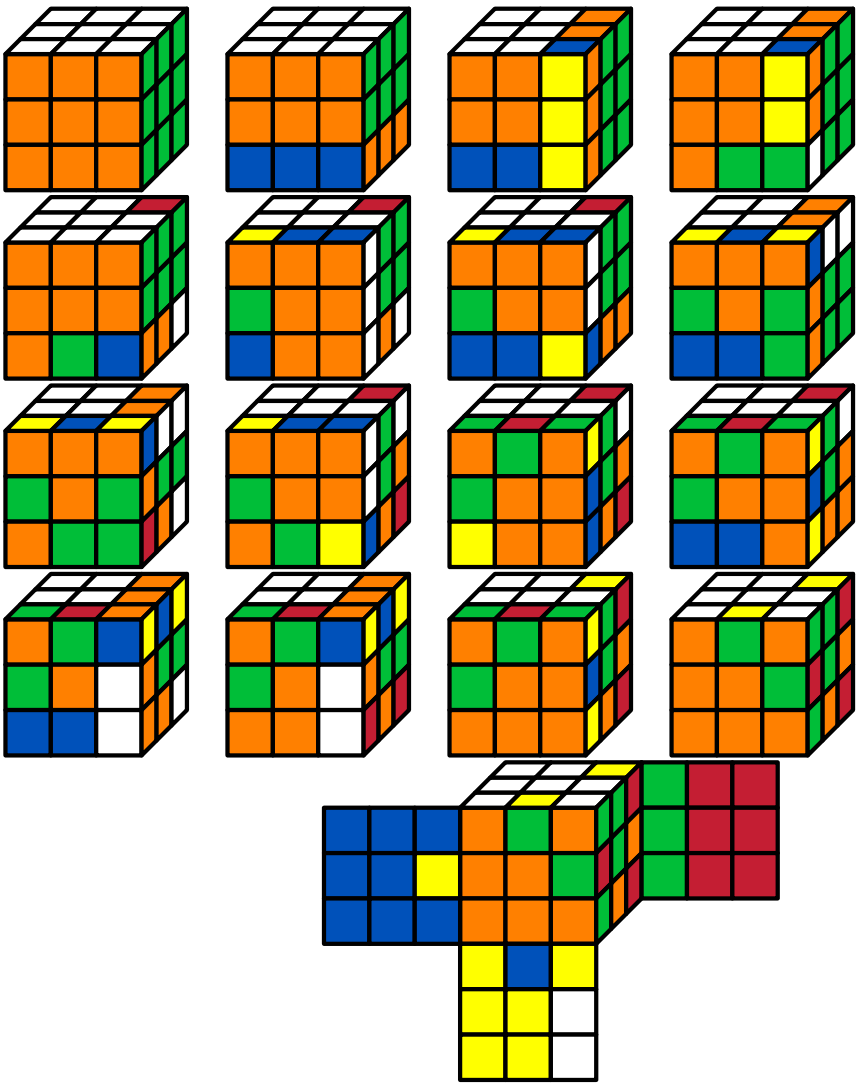

FIGURA A.2: Secuencia de movimientos de $([D, R]F)^3$ que opera sobre los cubiletes esquina de la siguiente forma: intercambia los cubiletes de los cubiculos 3 y 8, pero mantiene inalterados los otros cubiletes esquina.

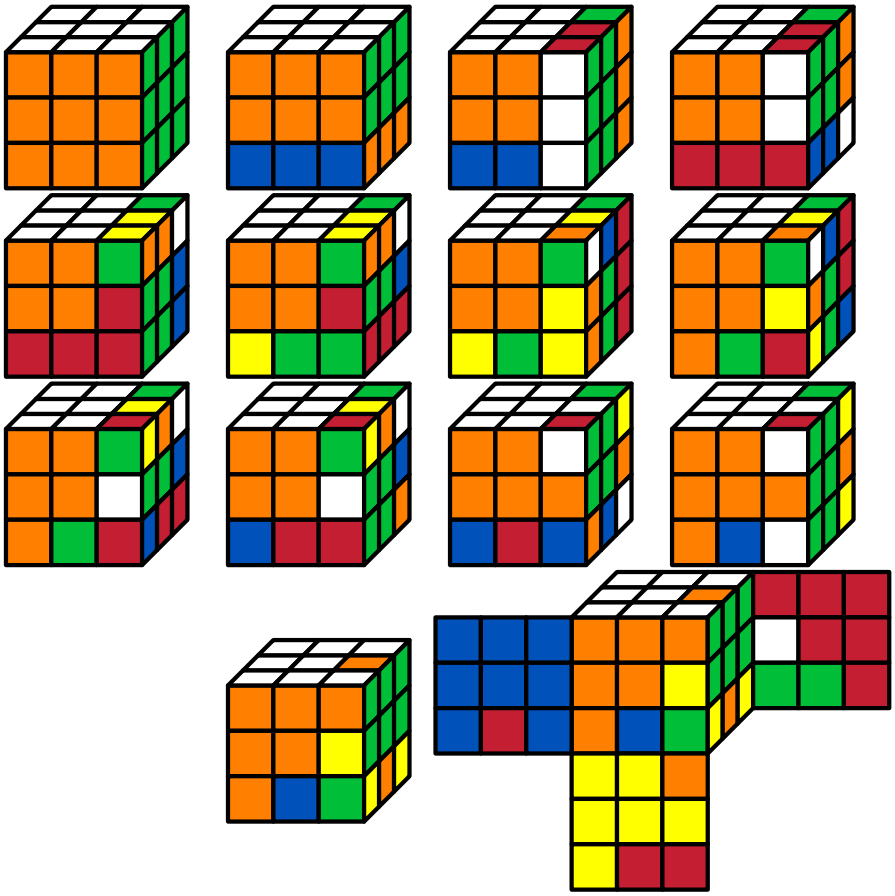

FIGURA A.3: Secuencia de movimientos de $(DR^{-1})^3(D^{-1}R)^3$ que mantiene inalterado el cubo excepto cambia la orientacion de los cubiletes esquina 7 y 8 en sentido antihorario y horario respectivamente.

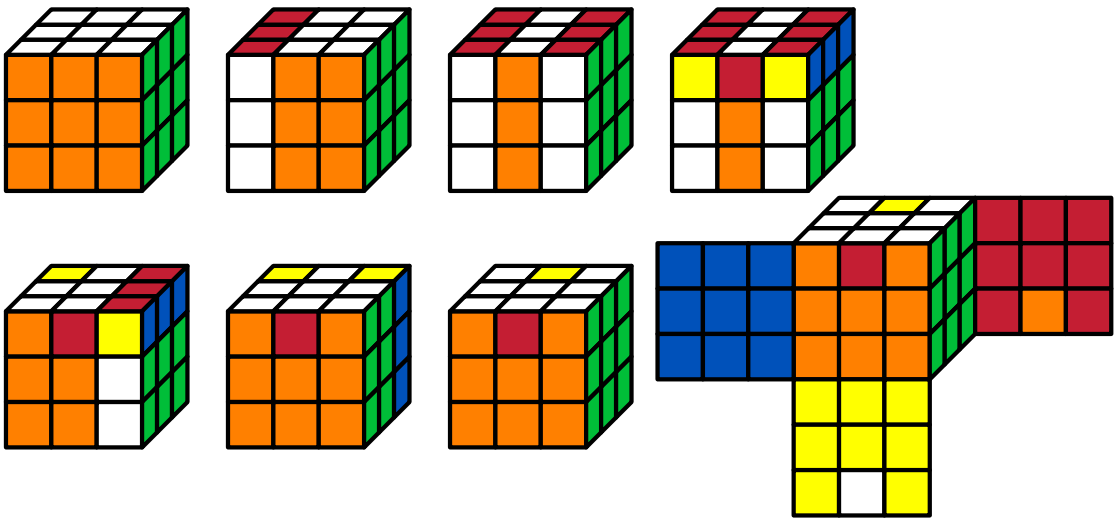

FIGURA A.4: Secuencia de movimientos de $LR^{-1}U^2L^{-1}RB^2$ que mantiene inalterado el cubo excepto que hace permutacion ciclica de los siguientes cubiletes borde: 1, 3 y 9.

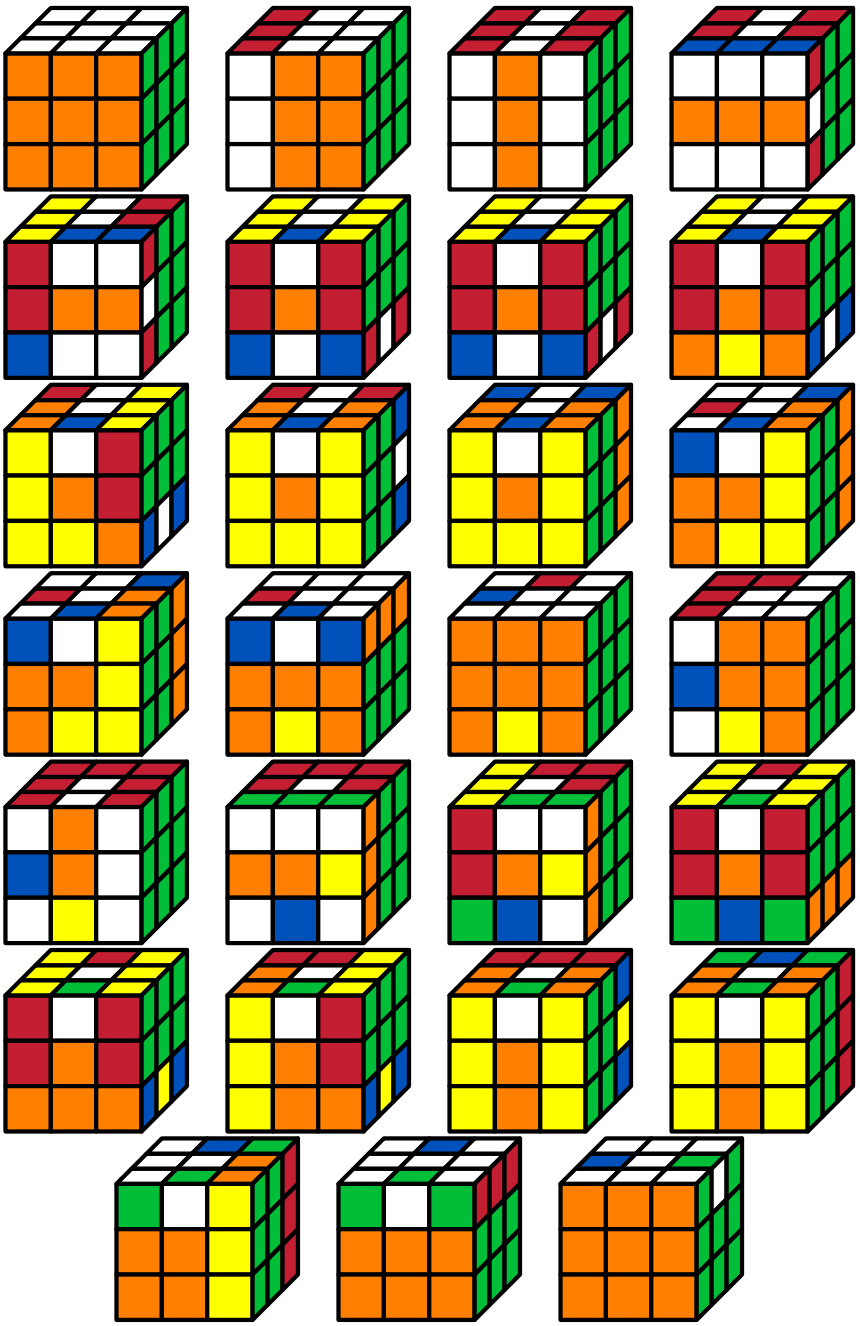

FIGURA A.5: Secuencia de movimientos de $LR^{-1}FLR^{-1}DLR^{-1}BLR^{-1}ULR^{-1}F^{-1}LR^{-1}D^{-1}LR^{-1}B^{-1}LR^{-1}U^{-1}$ que opera sobre los cubiletes esquina de la siguiente forma: cambia la orientacion de los cubiletes borde en el cubículo 2 y 4, sin afectar al resto de cubiletes.