

Guillermo Zamora Andrés

*El Cubo de Rubik: Explorando sus
intrincados aspectos matemáticos.*

*Rubik's Cube: Exploring its Mathematical
Intricacies.*

Trabajo de Fin de Grado
Grado en Matemáticas
San Cristóbal de La Laguna, Junio de 2023

DIRIGIDO POR
Hipólito Hernández Pérez

Hipólito Hernández Pérez
Profesor Contratado Doctor
Departamento de Estadística e
Investigación Operativa
Facultad de Ciencias
Universidad de La Laguna

Agradecimientos

Mi investigación a lo largo de mi vida me ha llevado a desarrollar la siguiente conjetura:

Conjetura.

Sea X un chico despistado e inquieto.

Se dice que X será una buena persona si se dan las siguientes condiciones:

- 1. X tiene una familia que lo quiere y apoya.*
- 2. X tiene amistades fuertes.*
- 3. X se levanta, al menos, el mismo número de veces que X se cae.*

Aunque cabe decir que la conjetura será cierta si y solo si X valora y da gracias por tener ayuda en el camino.

Es una conjetura dado que no podemos probarlo para todos los casos posibles pero lo que sí puedo decir es que en mi caso espero que se cumpla ya que cumplo todas las condiciones de la conjetura, pero lo más importante es que:

Doy gracias a todos los que me han acompañado en mi vida y espero que puedan sentirse orgullosos de tenerme en sus vidas.

Guillermo Zamora Andrés
San Cristóbal de La Laguna, 22 de mayo de 2023

Resumen

Resumen

En este trabajo exploraremos la fascinante conexión entre este rompecabezas tridimensional y los principios matemáticos. Se introducirá la Teoría de Grupos y se explorarán los subgrupos generados por los movimientos del cubo. Además, se aborda la Teoría de Grafos y se presenta un modelo de programación entera para la resolución del cubo en Python a partir de un modelo en GLPK. Este artículo muestra cómo el Cubo de Rubik puede ser utilizado como una herramienta valiosa para la enseñanza de las matemáticas, la Teoría de Grupos y la Teoría de Grafos.

Palabras clave: *Cubo de Rubik, Aplicaciones de la Teoría de Grupos, Aplicaciones de la Teoría de Grafos .*

Abstract

In this work, we will explore the fascinating connection between this three-dimensional puzzle and mathematical principles. Group Theory will be introduced, and the subgroups generated by the cube's movements will be explored. Additionally, the Graph Theory will be addressed, and an integer programming model for solving the cube will be presented in Python based on a GLPK model. This article showcases how the Rubik's Cube can be utilized as a valuable tool for teaching mathematics, Group Theory, and Graph Theory.

Keywords: *Rubik's Cube, Group Theory applications, Graph Theory applications.*

Contenido

Agradecimientos	III
Resumen	V
Introducción	IX
1. Introducción al Cubo de Rubik	1
1.1. El Cubo de Rubik	1
1.2. Variantes del cubo y modificaciones	2
1.2.1. El Cubo 2x2x2	2
1.2.2. El Cubo 4x4x4	3
1.2.3. El Cubo 3x3x3 con engranajes	3
1.2.4. El Pyraminx	4
2. El Cubo de Rubik y la Teoría de Grupos	5
2.1. Nociones básicas de Teoría de Grupos	5
2.2. El grupo del cuadrado	10
2.3. Grupos y subgrupos relacionados con el Cubo de Rubik	13
2.3.1. El grupo de las Secciones Centrales	13
2.3.2. El Grupo de las Secciones Centrales al Cuadrado	14
2.3.3. El grupo de los Dos Cuadrados	14
2.3.4. El grupo Anti-sección	15
2.3.5. El grupo generado por Dos Movimientos	16
2.3.6. El Súper-grupo	16
2.3.7. Algunos procedimientos sencillos	16
2.4. El problema Matemático Fundamental	16
2.5. El grupo del Cubo de Rubik 3x3x3	22
2.5.1. Descripción matemática de los movimientos del cubo 3x3x3	23
2.6. Segundo Teorema Fundamental de la Teoría de Cubos	28
2.6.1. Algunas consecuencias	31
3. Teoría de Grafos dentro del Cubo de Rubik	33
3.1. Grafo de Cayley	34
3.2. Algoritmo de Dios	36
3.2.1. La historia del Número de Dios	36
3.3. Circuitos Hamiltonianos en el Cubo de Rubik	37
3.4. Observaciones sobre aplicaciones, NP-completo	38

3.5. Aproximación al algoritmo de Dios por Programación Entera	38
3.5.1. Modelos Matemáticos	38
Bibliografía	43
Anexos	45
A.1. Propuesta de Algoritmo de Dios en Python	45
Poster	51

Introducción

El Cubo de Rubik es un rompecabezas tridimensional que ha cautivado a personas de todas las edades desde su invención en 1974 por el escultor húngaro Ernő Rubik. A pesar de su simplicidad aparente, resolver este puzle requiere habilidades matemáticas y de pensamiento crítico, lo que lo convierte en una herramienta útil para la enseñanza de las matemáticas y la Teoría de Grupos. En este trabajo académico, exploraremos la relación entre el Cubo de Rubik y las matemáticas, centrándonos en los métodos de resolución, la Teoría de Grupos y la Teoría de Grafos.

En el primer capítulo se presenta una visión general del cubo de Rubik y se destacan algunas variantes intrigantes, como el cubo $2 \times 2 \times 2$, el cubo $4 \times 4 \times 4$, el cubo $3 \times 3 \times 3$ con engranajes y el Pyraminx. Además, se comparten curiosidades sobre el cubo y se explora su popularidad como un desafiante rompecabezas tridimensional. Este resumen ofrece un vistazo conciso a la diversidad y complejidad del mundo del cubo de Rubik.

En el segundo capítulo, nos adentraremos en la Teoría de Grupos, que es fundamental para la resolución del Cubo de Rubik. Explicaremos algunas nociones básicas de la Teoría de Grupos y diferentes subgrupos generados por determinados movimientos que se podrían utilizar para resolver el cubo más eficientemente. También hablaremos de los teoremas relacionados con la Teoría de Grupos que se aplican en la resolución del Cubo de Rubik.

Finalmente, en el tercer capítulo, exploraremos la Teoría de Grafos y la resolución del cubo por programación entera. Presentaremos un modelo de programación entera para resolver el Cubo de Rubik escrito en lenguaje GLPK. Además hemos escrito un código en Python apartir de él.

Introducción al Cubo de Rubik

1.1. El Cubo de Rubik

El Cubo de Rubik fue inventado en 1974 por Ernő Rubik, un profesor de arquitectura húngaro. Rubik más tarde utilizó el Cubo como un ejercicio de aprendizaje para enseñar a sus estudiantes sobre espacios tridimensionales. Poco sabía él que su “Cubo Mágico”, como lo llamó originalmente, se convertiría en uno de los rompecabezas más famosos del mundo de todos los tiempos.

Para la década de 1980, el Cubo de Rubik era una locura mundial, vendiendo millones de cubos cada año y cimentando su legado en la cultura popular. Presente en *Los Simpsons*, *The Big Bang Theory*, un vídeo musical de las *Spice Girls* y grandes películas de *Hollywood*, la popularidad del Cubo de Rubik siguió creciendo en todo el mundo.

Hoy en día, el Cubo de Rubik es considerado como uno de los juguetes más queridos y conocidos de todos los tiempos. Cada año se venden millones de cubos, que son resueltos y compartidos entre amigos, familias y amantes de los puzles por igual.

Dentro del ámbito matemático, el Cubo de Rubik ha sido objeto de estudio desde hace décadas. En particular, se han utilizado herramientas de la Teoría de Grupos y de grafos para entender mejor su estructura y resolverlo de manera sistemática. De hecho, el Cubo de Rubik ha servido como un caso de estudio interesante para la Teoría de Grupos y ha sido una fuente de inspiración para la creación de nuevos algoritmos y técnicas de resolución.

El estudio del Cubo de Rubik ha permitido descubrir simetrías y patrones dentro del cubo, que han sido utilizados para desarrollar métodos de resolución más eficientes. Por ejemplo, se han utilizado técnicas de descomposición de grupos para reducir el número de posiciones que se deben analizar, y la Teoría de Grafos para entender la estructura de los movimientos que se pueden realizar en el cubo.

En este trabajo matemático, expondremos el Cubo de Rubik y algunas de sus más famosas variantes. Además, se abordará la Teoría de Grupos y de Grafos aplicada al Cubo de Rubik, con el objetivo de entender mejor su estructura y desarrollar nuevas técnicas de resolución.

En resumen, el Cubo de Rubik es un objeto fascinante que ha capturado la imaginación de personas en todo el mundo durante décadas. A través del uso de herramientas matemáticas como la Teoría de Grupos y de Grafos, se ha logrado entender mejor su estructura y resolverlo de manera eficiente. En este trabajo, exploraremos algunos de estos métodos y teorías para profundizar nuestra comprensión del Cubo de Rubik y su lugar en la matemática moderna.

Pero antes de ahondar más en el aspecto matemático del Cubo de Rubik, vamos a ver algunas curiosidades del mismo:

1. En 1982, el Cubo de Rubik se convirtió en un verdadero fenómeno global, vendiendo más de 100 millones de unidades en todo el mundo.
2. El récord mundial de resolver el Cubo de Rubik es de solo 3.47 segundos, establecido por el competidor australiano Feliks Zemdegs en 2020.
3. En 2014, se descubrió que cualquier Cubo de Rubik se puede resolver en un máximo de 20 movimientos, lo que se conoce como el “Número de Dios”.
4. A pesar de ser un juguete, el Cubo de Rubik también se utiliza como herramienta educativa en la enseñanza de la Teoría de Grupos y de Grafos, así como en la mejora de las habilidades cognitivas.

1.2. Variantes del cubo y modificaciones

El Cubo de Rubik ha sido un rompecabezas fascinante para millones de personas en todo el mundo desde su creación en 1974. A lo largo de los años, ha habido muchas variaciones y modificaciones en el diseño original del Cubo de Rubik que han llevado a la creación de una gran cantidad de rompecabezas y puzles relacionados. Desde el pequeño y ágil cubo $2 \times 2 \times 2$ hasta el más complejo *Megaminx*, cada variante ofrece su propio desafío y diversión para los entusiastas del Cubo de Rubik. En esta sección, exploraremos algunas de las variantes más populares y emocionantes del Cubo de Rubik.

1.2.1. El Cubo $2 \times 2 \times 2$

El Cubo de Rubik $2 \times 2 \times 2$, también conocido como el *Pocket Cube*, es una variante más simple del Cubo de Rubik clásico $3 \times 3 \times 3$. Fue inventado por el profesor húngaro Ernő Rubik en 1981 y desde entonces ha sido un rompecabezas popular entre los entusiastas del Cubo de Rubik debido a su tamaño compacto y su nivel de dificultad relativamente menor en comparación con su contraparte más grande.

A pesar de tener solo 8 piezas y 24 pegatinas en total, el *Pocket Cube* tiene un total de 3.674.160 combinaciones posibles, lo que lo convierte en un rompecabezas interesante y desafiante para resolver. Aunque esta cantidad de combinaciones es significativamente menor que la del Cubo de Rubik de tamaño estándar, la complejidad del *Pocket Cube* no debe subestimarse, ya que puede tomar numerosos movimientos para llegar a una solución óptima.

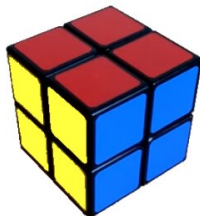


Figura 1.1: Cubo $2 \times 2 \times 2$

1.2.2. El Cubo 4x4x4

El Cubo de Rubik 4x4x4, también conocido como *Rubik's Revenge*, fue inventado por el húngaro Ernő Rubik en 1982. Es una variante del cubo 3x3x3 con la diferencia de que cuenta con dos capas intermedias, lo que lo hace más complejo y desafiante.

Debido al aumento de la cantidad de piezas y capas, el Cubo de Rubik 4x4x4 tiene una complejidad mucho mayor que el cubo 3x3x3. Aunque todavía es posible resolverlo aplicando los mismos principios del cubo 3x3x3, el número de posibles estados es mucho mayor, alcanzando la impresionante cantidad de 7.4×10^{45} estados distintos.

Dado que el cubo 4x4x4 es más complejo que su versión 3x3x3, algunos métodos de resolución no son directamente aplicables a este cubo. Sin embargo, muchos de los métodos utilizados para resolver el cubo 3x3x3 tienen variaciones que se pueden aplicar al cubo 4x4x4, como el método CFOP, el método Roux y el método ZZ. Además, se han desarrollado otros métodos específicos para el cubo 4x4x4, como el método Yau y el método Hoya. Estos métodos involucran diferentes técnicas y enfoques para la resolución del cubo y se basan en principios como la reducción de la paridad y la resolución por capas.

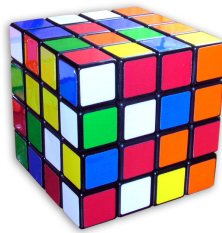


Figura 1.2: Cubo 4x4x4

1.2.3. El Cubo 3x3x3 con engranajes

El Cubo 3x3x3 con engranajes, también conocido como *Gear Cube*, es una variante del Cubo de Rubik que se caracteriza por tener engranajes en cada una de sus caras. Fue inventado por Oskar van Deventer, un conocido diseñador de rompecabezas, en 2009. A diferencia del Cubo de Rubik convencional, el *Gear Cube* tiene movimientos limitados debido a la presencia de los engranajes, lo que hace que su resolución sea más desafiante.

El Cubo 3x3x3 con engranajes tiene una complejidad mayor que el Cubo de Rubik convencional. Aunque ambos tienen 6 caras y el mismo número de piezas, en el *Gear Cube* la presencia de los engranajes reduce significativamente la cantidad de posibles movimientos que se pueden hacer. A pesar de esto, el número de estados posibles del *Gear Cube* es todavía muy alto, con alrededor de 41.472 combinaciones.

Para resolver el Cubo 3x3x3 con engranajes se utilizan métodos similares a los del Cubo de Rubik convencional, pero adaptados a las limitaciones de los engranajes. Algunos métodos populares incluyen el método *Keyhole*, que utiliza una técnica de inserción de piezas para resolver una cara del cubo antes de proceder a resolver las demás, y el método *Redux*, que adapta el método CFOP del Cubo de Rubik a la limitada cantidad de movimientos del *Gear Cube*.



Figura 1.3: Cubo 3x3x3 con engranajes resuelto



Figura 1.4: Cubo 3x3x3 con engranajes mezclado

1.2.4. El Pyraminx

El *Pyraminx*, también conocido como el *Tetraedron*, es un rompecabezas mecánico tridimensional inventado por Uwe Meffert en 1970. Este rompecabezas está formado por cuatro caras triangulares que pueden girar en cualquier dirección y se puede resolver a través de la combinación de los movimientos de las diferentes caras. A diferencia del Cubo de Rubik, el *Pyraminx* tiene una forma de tetraedro y solo tiene un centro, lo que lo hace más sencillo para principiantes. Sin embargo, a medida que se aumenta el número de capas, el *Pyraminx* se vuelve más complejo. El *Pyraminx* tiene un total de 933.120 estados posibles, lo que lo hace más fácil de resolver que el Cubo de Rubik. Existen varios métodos de resolución para el *Pyraminx*, que incluyen el método de capas y el método *Keyhole*, que se basa en resolver una parte del rompecabezas antes de completar el resto.

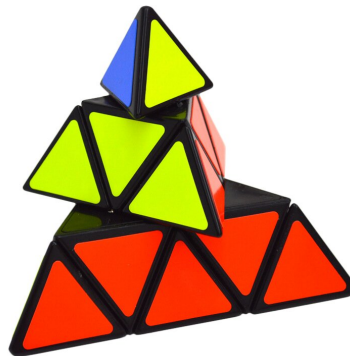


Figura 1.5: Pyraminx

El Cubo de Rubik y la Teoría de Grupos

Toda secuencia de movimientos modifica la colocación de las 54 (9 por 6 lados) caras coloreadas de los cubos unitarios (en realidad, podemos reducirlos a 48, puesto que las 6 caras de las piezas centrales no se desplazan de sitio). Esta modificación de situación se llama una permutación. Para poder entender que dibujos son los posibles y para expresar y estudiar otras cuestiones, necesitamos de terminología y algunas conclusiones acerca de las permutaciones y de los grupos de permutaciones.

2.1. Nociones básicas de Teoría de Grupos

Definición 2.1 (Grupo).

Un grupo (G, \circ) es un conjunto G en el que se ha definido una operación binaria interna \circ que satisface las siguientes propiedades:

1. Asociatividad: $\forall a, b, c \in G : a \circ (b \circ c) = (a \circ b) \circ c$.
2. Elemento neutro: $\exists e \in G : e \circ a = a \circ e = a$.
3. Elemento simétrico: $\forall a \in G, \exists a^{-1} \in G : a \circ a^{-1} = a^{-1} \circ a = e$.

Además, se dice que un grupo es abeliano o conmutativo cuando verifica también la propiedad conmutativa:

$$a \circ b = b \circ a \quad \forall a, b \in G.$$

Definición 2.2 (Permutación).

Una permutación de un conjunto X es una biyección de X en X . También decimos que una permutación es una reordenación de los elementos de X .

Ejemplo 2.3. Los reordenamientos de $X = \{1, 2, 3\}$ son:

$$\{1, 2, 3\}, \{1, 3, 2\}, \{2, 1, 3\}, \{2, 3, 1\}, \{3, 1, 2\}, \{3, 2, 1\}.$$

Sea $X = \{1, 2, 3, \dots, n\}$. Un reordenamiento de X es una lista sin repeticiones de todos sus elementos; y el número de permutaciones de X es exactamente $n!$.

Ahora bien, un reordenamiento de i_1, i_2, \dots, i_n de X determina una función $\alpha : X \rightarrow X$ tal que $\alpha(1) = i_1, \dots, \alpha(n) = i_n$. Claramente es una biyección. En el ejemplo anterior $\{2, 1, 3\}$ determina la función $\alpha(1) = 2, \alpha(2) = 1$ y $\alpha(3) = 3$.

Usaremos la siguiente notación:

$$\alpha = \begin{pmatrix} 1 & 2 & \dots & n \\ \alpha(1) & \alpha(2) & \dots & \alpha(n) \end{pmatrix}.$$

Una de las ventajas de ver las permutaciones como funciones, es la posibilidad de usar la composición de funciones como operación. Lo que nos lleva a la siguiente definición.

Definición 2.4 (Grupo de Simetrías de X).

La familia de todas las permutaciones de X la denotaremos por S_X y la llamaremos grupo de simetrías de X .

Cuando $X = \{1, 2, 3, \dots, n\}$, S_X se denota por S_n (llamado el grupo simétrico de n elementos).

Como vimos en 2.3, el número de permutaciones de X es exactamente $n!$. Por lo tanto el número de elementos de S_n es $n!$.

Observación 1. La composición en S_3 no es conmutativa, por ejemplo considere las permutaciones

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \text{ y } \beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},$$

$$\text{entonces } \beta\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \text{ y } \alpha\beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

Definición 2.5 (Ciclo).

Sean i_1, i_2, \dots, i_r enteros distintos dos a dos de $\{1, 2, 3, \dots, n\}$. Si $\alpha \in S_n$ fija los otros $n - r$ elementos y

$$\alpha(i_1) = i_2, \alpha(i_2) = i_3, \dots, \alpha(i_{r-1}) = i_r, \alpha(i_r) = i_1,$$

entonces α es llamado un r -ciclo y lo denotaremos por

$$\alpha = (i_1 i_2 \dots i_r)$$

Observación 2. Veamos algunas observaciones sobre los ciclos:

- 1 Un 2-ciclo intercambia i_1 con i_2 y deja fijos el resto de elementos. Un 2-ciclo es llamado una trasposición.
- 2 Un 1-ciclo es la identidad.
- 3 Hay r diferentes notaciones para un r -ciclo

$$(i_1 i_2 \dots i_r) = (i_2 i_3 \dots i_r i_1) = \dots = (i_r i_1 \dots i_{r-2} i_{r-1}).$$

- 4 Un r -ciclo también lo podemos llamar ciclo de tamaño r o ciclo de orden r . Esto quiere decir que:

$$\text{Sea } \sigma \text{ un } r\text{-ciclo. Tenemos que } \sigma^r = \text{Id.}$$

Definición 2.6 (Soporte).

Sea $\alpha \in S_n$. Se define el soporte de α como:

$$\text{supp}(\alpha) = \{a \in X : \alpha(a) \neq a\} \subseteq X$$

Definición 2.7 (Permutaciones disjuntas).

Dos permutaciones $\alpha, \beta \in S_n$ son llamadas disjuntas si sus soportes tienen intersección vacía, es decir: Si $\text{supp}(\alpha) \cap \text{supp}(\beta) = \emptyset$. Dadas las permutaciones β_1, \dots, β_t diremos que son disjuntas si son disjuntas dos a dos.

Lema 2.1.1. Si $\alpha, \beta \in S_n$ son permutaciones disjuntas, entonces conmutan.

Demostración. Si $i \notin \text{supp}(\beta)$, digamos $\beta(i) = j \neq i$, entonces $j \in \text{supp}(\beta)$, ya que si $\beta(j) = j$ y $j \neq i$ es una contradicción. Como β es inyectiva y α y β son disjuntas, entonces $\alpha(i) = i$ y $\alpha(j) = j$ (puesto que β mueve tanto el elemento i como el j). Por lo tanto $\beta\alpha(i) = \beta(i) = j$ y $\alpha\beta(i) = \alpha(j) = j$. Análogamente para el caso en el que $i \in \text{supp}(\alpha)$. Por último, es claro que $\alpha\beta(i) = \beta\alpha(i)$ si $i \notin \text{supp}(\alpha) \cup \text{supp}(\beta)$.

Lema 2.1.2. Toda permutación $\alpha \in S_n$ es un ciclo o bien producto de ciclos disjuntos.

Demostración. Vamos a realizar la demostración por inducción sobre el número de elementos del soporte de α .

Sea k dicho número:

- I) Si $k = 0$, entonces $\alpha = (1)$, por lo tanto α es un ciclo.
- II) Si $k > 0$, sea i un elemento del soporte de α . Definimos $i_1 = \alpha(i), i_2 = \alpha(i_1), i_3 = \alpha(i_2), \dots, i_{r+1} = \alpha(i_r)$, donde r es el menor entero positivo tal que $i_{r+1} \in i, i_1, i_2, \dots, i_r$. Puesto que solo hay n elementos, en algún momento debe haber una repetición en la lista i, i_1, i_2, \dots, i_r . Veamos que $\alpha(i_r) = i_1$. Supongamos que $\alpha(i_r) = i_j$, con $i_j \in i_2, \dots, i_r$. Tenemos que $\alpha(i_{j-1}) = i_j$, pero esto es una contradicción puesto que α es inyectiva y $j - 1 < r$. Denotemos por $\sigma = (i_1 i_2 \dots i_r)$ un r -ciclo. Si $r = n$, entonces $\alpha = \sigma$; por lo tanto α es un ciclo. Si $r < n$, entonces σ fija cada punto en Y donde Y son los otros $n - r$ elementos de X , y $\alpha(Y) = Y$. Definimos α' como la permutación tal que $\alpha'(i) = \alpha(i) \forall i \in Y$, y deja fijo toda $i \notin Y$. Observamos que $\alpha = \sigma\alpha'$. Por hipótesis de inducción tenemos que $\alpha' = \beta_1 \dots \beta_t$, donde β_1, \dots, β_t son ciclos disjuntos. Puesto que σ, α' son disjuntos, entonces α es producto de ciclos disjuntos. □

Teorema 2.1.1. Sean $\alpha \in S_n$ y $\alpha = \beta_1 \dots \beta_t$ su factorización en ciclos disjuntos. Esta factorización es única salvo el orden.

Demostración. Sea $\alpha = \gamma_1 \dots \gamma_s$ otra factorización en ciclos disjuntos de tamaño mayor o igual que 2 (es decir, extraemos todos los 1-ciclos).

Observemos que si $i_1 \in \text{supp}(\beta_t)$, entonces $\beta_t^k(i_1) = \alpha^k(i_1), \forall k \geq 1$. Donde $\beta_t^k(i_1)$ representa los elementos que pertenecen al soporte de β_t .

Además algún γ_j debe mover a i_1 y puesto que ciclos disjuntos conmutan, podemos tomar $\gamma_j = \gamma_s$ y asumir que $i_1 \in \text{supp}(\gamma_s)$. En consecuencia $\beta_t^k(i_1) = \gamma_s^k(i_1), \forall k \geq 1$, por lo que $\beta_t = \gamma_s$ y por lo tanto:

$$\beta_1 \dots \beta_{t-1} = \gamma_1 \dots \gamma_{s-1}.$$

Ahora, usando un argumento inductivo con respecto al número de factores, se tiene que $s = t$ y los factores $\beta_i = \gamma_i$ para $i = 1, \dots, s$. □

Observación 3. Todo r -ciclo es producto de $r - 1$ trasposiciones.

$$(a_1 a_2 \dots a_r) = (a_1 a_2)(a_1 a_3) \dots (a_1 a_r)$$

En consecuencia, usando 2.1.1, todo $\alpha \in S_n$ es producto de trasposiciones.

Definición 2.8 (Permutación par e impar).

Una permutación $\alpha \in S$ es par si es el producto de un número par de trasposiciones, si no, es impar.

Lema 2.1.3. Sean $k, l \geq 0$, entonces

$$(a \ c_1 \dots c_k \ b \ d_1 \dots d_l)(a \ b) = (a \ c_1 \dots c_k)(b \ d_1 \dots d_l)$$

y

$$(a \ c_1 \dots c_k)(b \ d_1 \dots d_l)(a \ b) = (a \ c_1 \dots c_k \ b \ d_1 \dots d_l)$$

Demostración. El lado izquierdo manda $a \rightarrow c_1 \rightarrow c_1; c_i \rightarrow c_{i+1} \rightarrow c_{i+1}$ si $i < k$; $c_k \rightarrow b \rightarrow a; b \rightarrow d_1 \rightarrow d_1; d_j \rightarrow d_{j+1} \rightarrow d_{j+1}$ si $j < l$; $d_l \rightarrow a \rightarrow b$. La correspondiente evaluación de la derecha nos muestra que ambas permutaciones son iguales. Para la segunda ecuación simplemente multiplicamos ambos lados de la primera ecuación por (ab) por la izquierda.

Definición 2.9 (Signo de una permutación).

Sea $\alpha \in S_n$ y $\alpha = \beta_1 \dots \beta_t$ es una factorización completa en ciclos disjuntos, entonces el signo de α está definido como:

$$\text{sgn}(\alpha) = (-1)^{n-t}$$

Por el Teorema 2.1.1, sgn es una función bien definida. Si τ es una trasposición, entonces mueve dos elementos, i y j , y deja fijos todos los otros $n - 2$ elementos; por lo tanto

$$t = (n - 2) + 1 = n - 1, \text{ y entonces}$$

$$\text{sgn}(\tau) = (-1)^{n-(n-1)} = -1$$

Lema 2.1.4. Sean $\beta \in S_n$ y τ una trasposición, entonces

$$\text{sgn}(\tau\beta) = -\text{sgn}(\beta).$$

Demostración. Sea $\tau = (ab)$ y sea $\beta = \gamma_1 \dots \gamma_t$ una factorización completa de β en ciclos disjuntos. Si $ayb \in \text{supp}(\gamma_1)$, sin pérdida de generalidad, entonces $\gamma_1 = (ac_1 \dots c_k bd_1 \dots d_l)$ donde $k \geq 0$ y $l \geq 0$. Por el lema 2.1.3,

$$\tau\gamma_1 = (ac_1 \dots c_k)(bd_1 \dots d_l),$$

y entonces $\tau\beta = (\tau\gamma_1)\gamma_2 \dots \gamma_t$ es una factorización completa con un ciclo extra ($\tau\gamma_1$ que se separa en dos ciclos disjuntos). Por lo tanto, $\text{sgn}(\tau\beta) = (-1)^{n-(t+1)} = -\text{sgn}(\beta)$. La otra posibilidad es que $a \in \text{supp}(\gamma_1)$ con $\gamma_1 = (ac_1 \dots c_k)$ donde $k \geq 0$ y $b \in \text{supp}(\gamma_2)$ con $\gamma_2 = (bd_1 \dots d_l)$ donde $l \geq 0$, sin pérdida de generalidad. Pero ahora $\tau\beta = (\tau\gamma_1\gamma_2)\gamma_3 \dots \gamma_t$ y por el lema 2.1.3

$$\tau\gamma_1\gamma_2 = (ac_1 \dots c_k bd_1 \dots d_l).$$

Por lo tanto, la factorización completa de $\tau\beta$ tiene un ciclo menor que β y entonces

$$\text{sgn}(\tau\beta) = (-1)^{n-(t-1)} = -\text{sgn}(\beta).$$

Teorema 2.1.2. Para todos $\alpha, \beta \in S_n$,

$$\text{sgn}(\alpha\beta) = \text{sgn}(\alpha)\text{sgn}(\beta).$$

Demostración. Supongamos que $\alpha \in S_n$ tal que $\alpha = \tau_1 \dots \tau_m$ es una factorización de α en trasposiciones con m mínimo. Probaremos, por inducción sobre m , que $\text{sgn}(\alpha\beta) = \text{sgn}(\alpha)\text{sgn}(\beta) \forall \beta \in S_n$. El primer paso es precisamente el lema 2.1.3. Si $m > 1$, entonces la factorización $\tau_2 \dots \tau_m$ es también mínima: si $\tau_2 \dots \tau_m = \sigma_1 \dots \sigma_q$ siendo cada σ_j una trasposición y $q < m - 1$, entonces la factorización $\alpha = \tau_1\sigma_1 \dots \sigma_q$ contradice la suposición de m mínimo. Por lo tanto,

$$\begin{aligned} \text{sgn}(\alpha\beta) &= \text{sgn}(\tau_1 \dots \tau_m\beta) = -\text{sgn}(\tau_2 \dots \tau_m\beta) \text{ Lema 2.1.3} \\ &= -\text{sgn}(\tau_2 \dots \tau_m)\text{sgn}(\beta) \text{ por inducción.} \\ &= \text{sgn}(\tau_1 \dots \tau_m)\text{sgn}(\beta) \text{ por el Lema 2.1.3} \\ &= \text{sgn}(\alpha)\text{sgn}(\beta). \end{aligned}$$

□

Teorema 2.1.3.

- (I) Una permutación $\alpha \in S_n$ es par si y solo si $\text{sgn}(\alpha) = 1$.
- (II) Una permutación α es impar si y solo si es producto de un número impar de trasposiciones.

Demostración. (I) Hemos visto que $\text{sgn}(\tau) = -1$ para cada trasposición τ . Por lo tanto si $\alpha = \tau_1 \dots \tau_q$ es una factorización de α en trasposiciones, entonces el Teorema 2.1.2 nos dice que $\text{sgn}(\alpha) = \text{sgn}(\tau_1)\dots(\tau_q) = (-1)^q$. Entonces, $\text{sgn}(\alpha) = 1$ si y solo si q es par. Si α es par, entonces existe una factorización con q par, y entonces $\text{sgn}(\alpha) = 1$. En cambio, si $1 = \text{sgn}(\alpha) = (-1)^q$ entonces q es par y por lo tanto α es par.

- (II) Si α es impar, entonces no tiene factorización en un número par de trasposiciones, y entonces debe ser producto de un número impar de trasposiciones. En cambio, si $\alpha = \tau_1 \dots \tau_q$ con q impar, entonces $\text{sgn}(\alpha) = (-1)^q = -1$; por (i), α no es par, y por lo tanto α es impar.

□

Lema 2.1.5. Sea $\alpha \in S_n$ tal que $\alpha = \tau_1 \dots \tau_r = \gamma_1 \dots \gamma_s$ donde τ_i, γ_j son trasposiciones, entonces r y s tienen la misma paridad.

Demostración. Aplicando el Teorema 2.1.3, por (I) es claro que si $\text{sgn}(\alpha) = 1$ es por que r y s son pares y por (II) si $\text{sgn}(\alpha) = -1$ quiere decir que es producto de un número impar de trasposiciones; y por lo tanto r y s son impares.

Definición 2.10 (Subgrupo alternado).

Definimos el grupo alternado A_n como $A_n = \{\alpha \in S_n \text{ tal que } \alpha \text{ es par}\}$.

Proposición 2.1.1. El número de elementos de A_n es la mitad del de S_n , es decir $|A_n| = (n!)/2$.

Demostración. Fijemos en S_n una trasposición σ y consideremos la aplicación $f : S_n \rightarrow S_n$ tal que a una permutación ϕ le asocia $\phi\sigma$. Esta aplicación es una bisección. Además, ϕ es par si y solo si $\phi\sigma$ es impar, por lo que f esta restringida a una bisección de A_n en el conjunto de permutaciones impares, es decir S_n/A_n . Por tanto, estos dos conjuntos tienen el mismo número de elementos. Sin embargo, forman una partición de S_n , ya que son disjuntos y su unión es igual a S_n . \square

Propiedades 1 (Subgrupo Alternado). Sean $f, g \in S_n$. El subgrupo Alternado tiene las siguientes propiedades:

1. Si $f, g \in A_n \Rightarrow f \cdot g \in A_n$.
 2. Si $f, g \notin A_n \Rightarrow f \cdot g \in A_n$.
 3. Si $f \in A_n, g \notin A_n \Rightarrow f \cdot g \notin A_n$.
- Si $f \notin A_n, g \in A_n \Rightarrow f \cdot g \notin A_n$.

Podemos ver que se cumplen dichas propiedades haciendo uso del Teorema 2.1.2.

Proposición 2.1.2. Sea H el subgrupo de S_n generado por todos los 3-ciclos de S_n , entonces $H = A_n$.

Demostración. Como $\text{sgn} : S_n \rightarrow \pm 1$ es un homomorfismo, y como cualquier 3-ciclo es par, entonces cualquier producto de 3-ciclos es también par. Por lo tanto, $H \subset A_n$. Sea $g \in A_n$ entonces g debe ser par. Por lo cual, (dado que toda permutacion puede ser escrita como producto de 2-ciclos, 2.1.1) g debe estar compuesto por permutaciones de la forma $(ij)(lk)$ o $(ij)(jk)$. Pero $(ij)(kl) = (ijk)(jkl)$ y además $(ij)(jk) = (ijk)$. Por tanto, $g \in H$. Esto implica que $A_n \subset H$, y entonces $A_n = H$. \square

Definición 2.11 (Grupo cíclico de orden n).

Se denomina C_n al grupo cíclico de orden n , esto es,

$$C_n = \langle h | h^n = 1 \rangle .$$

El grupo C_m^n se denota por:

$$C_m^n = \langle h_1, \dots, h_m | h_i^n = 1, h_i h_j = h_j h_i, \forall 1 \leq i, j \leq m \rangle .$$

2.2. El grupo del cuadrado

Una simetría del cuadrado es un movimiento del cuadrado como cuerpo rígido que le devuelve a su lugar original, pero generalmente con los vértices en diferentes sitios.

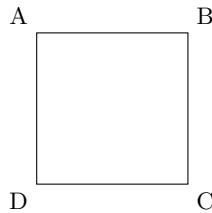


Figura 2.1

Designaremos nuestras dos simetrías del ejemplo:

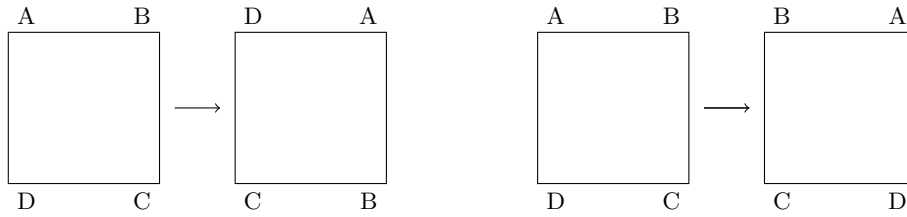


Figura 2.2

1. R: Rotación.

2. V: Reflexión Vertical.

Cada simetría del cuadrado da una permutación de las siglas A, B, C y D. Hay varias maneras de considerar esta permutación, que dependen de dos decisiones referidas a los puntos de vista. En primer lugar, podemos considerar que la acción “*se desplaza a*” o “*se reemplaza por*”. En segundo lugar, podemos considerar que la permutación actúa sobre las siglas o símbolos, independientemente de su paradero, o que actúa sobre el contenido de las posiciones, independientemente del símbolo que ocupe actualmente dicha posición. En último caso, utilizaremos las siglas para representar las posiciones de los vértices, y lo haremos aun más claro poniendo las siglas en la parte exterior del cuadrado según se ve en la Figura 2.1. La primera distinción es una dualidad equivalente a la dualidad entre una permutación y su inverso. La segunda distinción es más significativa y un punto de vista puede ser mucho más conveniente que el otro en un problema dado. Sin embargo, estas distinciones no se harán evidentes hasta que multipliquemos permutaciones más adelante.

Podemos representar las permutaciones de acuerdo a la terminología usada en Teoría de Grupos para permutaciones como se describe en las definiciones 2.2 y en 2.5, esto es:

1. $R = (ABCD)$.
2. $V = (AB)(CD)$.

Ahora vamos a describir otro tipo de representación para una permutación, la cual será más informativa. Considérese una permutación cualquiera P . Las aplicaciones sucesivas de P se denotan P, P^2, P^3, \dots . Estas permutaciones desplazan (o reemplazan) una posición (o símbolo) A por $P(A), P^2(A), P^3(A), \dots$. Comenzando con una posición (o símbolo) cualquiera A , con el tiempo esta secuencia se repetirá (es decir, es cíclica). Debido a la naturaleza de 1 a 1 (o invertible) de una permutación, esta secuencia solo puede repetirse al regresar a A en algún punto, digamos $P^n(A) = A$, y $P^i(A) \neq A$ para $1 \leq i < n$. Lo representamos encerrando en paréntesis un ciclo completo, así $(AP(A)P^2(A) \dots P^{n-1}(A))$ es un n -ciclo. Por ejemplo, para R en el cuadrado obtenemos $(ABCD)$. Gráficamente podemos representar los ciclos como se ven en 2.3. Puesto que el punto de partida de un ciclo es arbitrario, el ciclo $(ABCD)$ es igual que el de $(BCDA)$, etc.

Si sobran símbolos (o posiciones), tomamos el más conveniente como principio de otro ciclo y continuamos hasta agotar todos los símbolos (o posiciones). Por ejemplo, para V , obtenemos dos 2-ciclos $(AB)(CD)$, los cuales dibujamos como en la Figura a) de 2.4, mientras que RV manda $(A)(BD)(C)$, que se ve en la Figura b) de 2.4. Normalmente omitimos los ciclos de longitud 1, así escribimos RV simplemente como (BD) , que se ve en la Figura c) de 2.4. Decimos que RV actúa solo sobre B y D , ya que los demás objetos permanecen fijos.

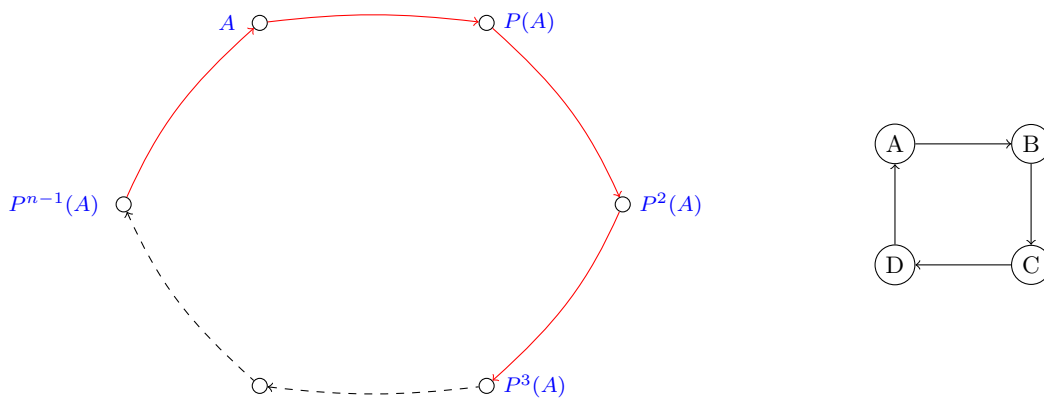


Figura 2.3: Representación gráfica de un n -ciclo y gráfico R en el cuadrado

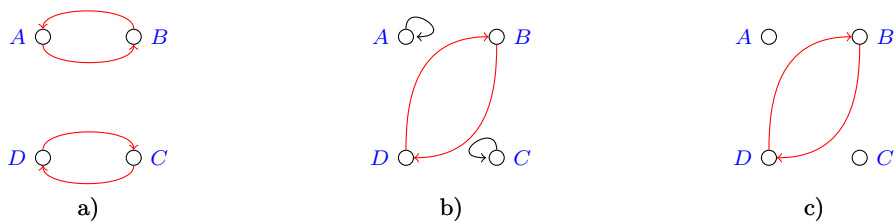


Figura 2.4: Representación gráfica de V y RV

El subgrupo de simetrías de un cuadrado

Cabe observar que el grupo de simetrías de un cuadrado tiene menos elementos que S_4 . Esto es debido a que no todas las permutaciones de 4 elementos, en nuestro caso relacionados con los vértices del cuadrado, son posibles cuando hablamos de las rotaciones y simetrías del cuadrado. Por ejemplo la permutación ϕ dada por:

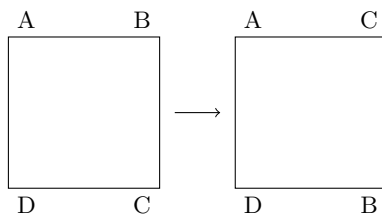


Figura 2.5

Por lo tanto debemos hablar del subgrupo de simetrías del cuadrado D_4 en vez del grupo S_4 . El subgrupo D_4 está contenido en S_4 pero, a diferencia de este último, D_4 solo tiene 8 elementos. Es fácil ver esta afirmación dado que el subgrupo D_4 está generado por una rotación y una simetría, dicho de otra manera:

$$D_4 = \{Id., R, R^2, R^3, V, RV, R^2V, R^3V\} = \langle R, V \mid R^4 = Id, V^2 = Id, RV = VR^3 \rangle .$$

2.3. Grupos y subgrupos relacionados con el Cubo de Rubik

Para poder comprender el comportamiento del cubo, sera útil estudiar al principio algunos subgrupos pequeños o sencillos y descubrir los procedimientos que desplazan solamente unas pocas piezas. A continuación daré unos ejemplos.

En general utilizaremos “*se desplaza a*” sobre posiciones al describir las permutaciones en el cubo, ya que los movimientos básicos de las seis caras del Cubo de Rubik denotados por R (*Right*), U (*Up*), D (*Down*), L (*Left*), B (*Back*), F (*Front*), se definen en términos de posiciones físicas. No obstante, existen ciertos subgrupos en que se puede emplear “*se reemplaza por*” sobre símbolos.

Ahora podemos utilizar nuestras seis letras para designar las seis caras, así como los subcubos que componen el Cubo de Rubik, por ejemplo: UR , UF , UL , UB son los 4 subcubos arista de la cara U y URF , UFL , ULB , UBR son los 4 subcubos esquina de la cara U . Podemos observar que UR y RU es el mismo subcubo. Acordamos indicar los colores o sentidos en los vértices en sentido horario. Utilizaremos estas letras tanto para designar las caras como los movimientos de 90° de la cara referente a dicha letra. Esto podría llevar a algun tipo de confusión cuando designemos un subcubo arista, por ejemplo UR (la arista que está en las caras U y R) o la composición de movimientos UR (aplicamos primero el movimiento U y luego el movimiento R), si llega esta situación, se especificará su utilidad.

Veamos ahora los movimientos en el cubo. Consideramos permutaciones utilizando “*se desplaza a*” actuando sobre posiciones. La representación cíclica del movimiento R es $(FR UR BR DR)(URF BRU DRB FRD)$ y la representación cíclica de RU es $(FR UF UL UB UR BR DR)(URF RFU FUR)(BRU DRB FRD UFL ULB UBR\dots)$. Aquí topamos con una complejidad en la notación. El segundo ciclo de RU comprende tres ternas que se refieren al mismo vértice del cubo, pero en diferentes orientaciones. Es decir, RU gira URF en un tercio de vuelta en el sentido horario (visto desde el exterior del cubo). Lo escribimos simplemente como (URF) , donde el subíndice denota un giro en el sentido horario. En otras palabras, $+$ indica que cada sigla se desplaza a la siguiente en la secuencia ADF . Lo llamaremos un 1-ciclo torcido (o con torsión). El tercer ciclo de RU tendría 15 componentes, pero ellos comprenden tres repeticiones de los primeros 5 vértices y cada repetición se obtiene girando las anteriores un tercio de vuelta en el sentido anti-horario. Denotamos este 5-ciclo torcido por $(BRU DRB FRD UFL ULB)$. Significa que la quinta potencia de este ciclo sera $(BRU)_-(DRB)_-(FRD)_-(UFL)_-(ULB)_-$. También podemos tener ciclos torcidos para aristas, pero como una arista solo tiene dos lados, $+$ y $-$ son iguales, escribiremos $(FR)_+$ para $(FR RF)$, etc.

2.3.1. El grupo de las Secciones Centrales

Sujetando el cubo en la posición normal, imagínese girando tanto la cara R (*Right*) como la cara L (*Left*) hacia fuera. Es equivalente a girar la “sección” central hacia usted y se denotaría por $RL^{-1}(= L^{-1}R)$. Considérese el subgrupo generado por los movimientos de sección. Es conveniente al trabajar en este grupo dejar que R denote el movimiento de sección que acabamos de describir (es decir, RL^{-1} en nuestra notación original), Observe que $R = L^{-1}$ en esta notación de modo que se genera este grupo por los tres movimientos de sección R, U, F .

Este grupo no es muy grande y contiene algunos dibujos elegantes. Un examen superficial demuestra que cada cara siempre presenta el dibujo que se ve en 2.6, en donde

a, b, c, d son cuatro colores (no necesariamente distintos). Es más, la cara opuesta a esta tendrá el mismo dibujo, habiendo sido reemplazado cada color por su contrario. (Los colores contrarios son R-L, F-B, U-D.) Denotamos el color opuesto de a por a' , por ejemplo, $R' = L$. Con algo de juego sistemático se pueden obtener dibujos con las seis caras mostrando $a = b = c$ o con las seis caras presentando $a = d = b' = c'$ (cara en “X” o en cruz). o con cuatro caras de lunares y dos lisas (es decir, $a = b = c = d$), o con cuatro caras exponiendo $a' = b = c = d$ (“+” o “más” o cara de cruz griega) y dos caras en “X”. No obstante, no se pueden obtener todos los dibujos parecidos a 2.6.

a	b	a
c	d	c
a	b	a

Figura 2.6

El subgrupo donde $a = b = c$ en las 6 caras corresponde al mover los ejes de coordenadas determinados por los centros de las caras con respecto al resto del cubo. Este grupo es el mismo que el de las simetrías directas pares del cubo y consta de 12 elementos (aunque necesitemos algún detalle más para completar el razonamiento).

Para trabajar con este grupo, podemos observar que los ocho vértices del cubo siempre mantienen la misma relación entre sí. Por lo tanto, podemos considerarlos fijos, con solo las secciones centrales desplazándose. Así podemos referirnos a una cara por sus vértices en lugar de por su centro. Con respecto a las coordenadas de vértice, tenemos tres secciones ortogonales que actúan sobre conjuntos disjuntos de aristas, y que nos dan 4^3 movimientos de arista. Una sección actúa como un 4-ciclo sobre los centros de las caras, lo cual es una simetría directa impar de los centros de las caras. Sin embargo, para que las aristas se alineen con los vértices, se debe girar cada sección un múltiplo de 4 unidades y de este modo el subgrupo con $a = b = c$ contiene solamente permutaciones pares de los centros de las caras. De hecho, el mismo análisis que el del principio de la sección 2.4 demuestra que este grupo consta de $4^3 \cdot \frac{24}{2} = 768$ elementos.

2.3.2. El Grupo de las Secciones Centrales al Cuadrado

Consideramos el subgrupo generado por los cuadrados de las secciones, es decir $\langle R^2, U^2, F^2 \rangle$ en la notación de la subsección anterior.

Es un grupo conmutativo de 8 elementos, y todo elemento es de orden 2.

2.3.3. El grupo de los Dos Cuadrados

Consideramos el subgrupo generado por los cuadrados de dos caras adyacentes, por ejemplo $\langle F^2, R^2 \rangle$ en nuestra notación usual.

Este grupo consta de 12 elementos. Las columnas FL , FR y RB se trasladan como unidades mientras que se intercambian las parejas (RU, RD) y (FU, FD) .

2.3.4. El grupo Anti-sección

Son movimientos como $RL (= LR)$ en nuestra notación original. Consiste en girar la cara L hacia usted. Si denotamos este movimiento anti-sección por R , tenemos $R = L$ en este grupo. El cuadrado de la sección correspondiente. La estructura de este grupo es, en su mayor parte, desconocida, pero contiene algunos dibujos con cuatro caras “diagonales” (2.7 Figura A) y dos caras lisas, con cuatro caras en “Z” (2.7 Figura B) y dos caras lisas, con seis caras de “2L” (2.7 Figura C), con cuatro caras “+” y dos caras lisas, y con cuatro caras “diagonales” y dos caras “+”.

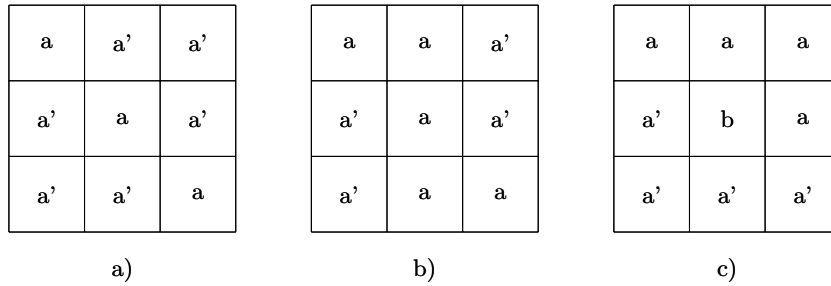


Figura 2.7: Dibujos del grupo Anti-sección

Un examen del efecto de un movimiento anti-sección demuestra que las cuatro aristas en una sección se quedan en ella, pero se cambian de orden. Por ejemplo: después de la anti-sección R , la sección RL (es decir, la sección entre las caras R e L) no se modifica, mientras que las aristas en la sección FB cambian de UR, RD, DL, LU a FR, RB, FL, LB y las aristas en la sección UD cambian de FR, RL, BL, LF a DR, RU, DL, LU . Si consideramos las secciones como fijas y los centros de las caras como móviles (parecido a lo que hicimos en el grupo de sección), entonces nuestras anti-secciones llevan cada sección a si misma. Por ejemplo, la anti-sección R lleva las aristas de la sección UD

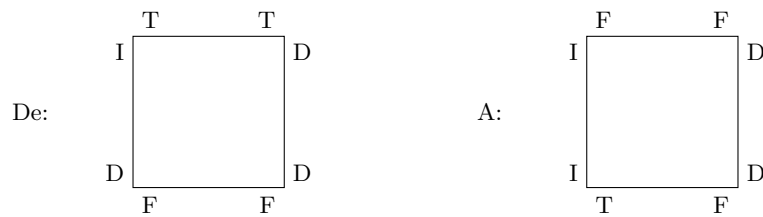


Figura 2.8: Movimiento de aristas por la anti-sección R

Es decir, se han intercambiado dos de las aristas por reflexión. Un poco de experimentación demostrará que una sección solo puede tener seis posibles configuraciones (cuando fijemos, por ejemplo, la arista FR). Se puede reconocer la sección UD , pues es la única que no contiene ni R 's ni D 's. Sin embargo, es más fácil considerar los vértices. Aunque los vértices de una cara no permanecen iguales, presentan como mucho dos colores y serán colores opuestos. Por lo tanto, podemos identificar las caras R e L por ser las que tienen R e L en sus vértices. La sección RL permanecerá entre las caras R y L . Puesto que la anti-sección R es igual que la anti-sección L , no importa, de las dos caras R, L cual es R y cual es L , ni afecta cual es la sección RL .

2.3.5. El grupo generado por Dos Movimientos

Es el subgrupo generado por dos movimientos adyacentes, por ejemplo, $\langle F, R \rangle$ en nuestra notación usual.

2.3.6. El Súper-grupo

En este grupo se tiene en consideración los centros. Aunque no se desplacen, se giran. El giro total de D en un procedimiento (medido en unidades de 90°) es simplemente la suma de los exponentes de R en todo el procedimiento. Esta suma debe ser considerada en módulo 4, puesto que 4 giros es igual que ninguno. Por ejemplo, para $P_1 = (F^2R^2)^3$, R ha girado 6 unidades, que es lo mismo que 2 unidades.

La suma de todo giro de cara en toda permutación que es Identidad (olvidándose de los centros) debe ser par, puesto que la Identidad es una permutación par sobre los vértices. Ahora tenemos $(RU)^{105} = Identidad$, de modo que tenemos una Identidad (olvidándose de los centros) que gira dos centros adyacentes 105 veces, lo cual es 1 (*mod* 4). Combinando varias de ellas, se obtiene un grupo de “centros” de $\frac{4^6}{2} = 2^{11} = 2048$ elementos, que actúan independientemente de los demás movimientos. De aquí que el súper-grupo conste de

$$\begin{aligned} 2^{11} \cdot N &= \frac{8! \cdot 12!}{2} \cdot \frac{3^3}{3} \cdot \frac{2^{12}}{2} \cdot \frac{4^6}{2} = 2^{38} 3^{14} 5^3 7^2 11 = \\ &= 88.580.102.706.155.225.088.000 \approx 8,9 \times 10^{22} \text{elementos} \end{aligned} \quad (2.1)$$

A razón de un elemento por microsegundo, un ordenador tardaría unos $2,8 \times 10^9$ años para contar todas las posiciones, es decir, aproximadamente la tercera parte de la edad del universo.

2.3.7. Algunos procedimientos sencillos

Se pueden hallar rápidamente, usando los grupos anteriores, procedimientos (es decir, secuencias de movimientos) que intercambian dos parejas de aristas, dejando todo lo demás en su sitio, y que intercambian dos parejas de vértices, dejando las demás piezas (o solamente las demás aristas) fijas, aunque no es posible hallar un procedimiento que intercambie una sola pareja de aristas o vértices. Es posible hallar procedimientos que intercambien una pareja de vértices y una pareja de aristas, aunque no serán sencillos.

2.4. El problema Matemático Fundamental

El problema es el de recomponer el cubo desde cualquier posición aleatoria en la de origen, donde cada cara tiene un solo color. Inversamente, es también el problema de llegar desde la posición de origen a cualquiera y de aquí también el problema de ir de un dibujo a otro.

Para resolver este problema, necesitamos proceder en dos direcciones. Primeramente, al examinar el cubo y su grupo, descubrimos cuales son las posiciones posibles y, segundo, demostramos que podemos realizar todas ellas. Nos concentramos ahora en la cuestión de describir las posiciones posibles.

El grupo de todas las posibles permutaciones es el siguiente: los vértices pueden permutarse entre sí de cualquier manera dando lugar a $8!$ posibilidades, y las 12 aristas se pueden permutar entre sí en cualquiera de $12!$ maneras, con excepción de que la permutación total de vértices y aristas debe ser par. Es más, con independencia del movimiento de las piezas, podemos invertir las orientaciones de dos aristas cualesquiera y podemos torcer dos vértices cualesquiera en direcciones contrarias. Esto significa que podemos orientar como queramos todos los vértices y aristas menos uno; la orientación de este último es obligatoria. Con esto se llega a un total de:

$$N = \frac{8! \cdot 12!}{2} \cdot \frac{3^3}{3} \cdot \frac{2^{12}}{2} = 43.252.003.274.489.856.000 = 2^{27} \cdot 3^{14} \cdot 5^3 \cdot 7^2 \cdot 11$$

posiciones diferentes. Un ordenador podría contar una posición por microsegundo, de forma que tardaría aproximadamente 1,4 millones de años en contarlas todas. El numerador de N es el número total de maneras en que se puede reconstruir el cubo. El denominador de 12 significa que existen 12 órbitas distintas de posiciones construibles. Una órbita es el conjunto de todas las posiciones accesibles desde una posición dada por aplicación de nuestro grupo. No se puede salir de una órbita para introducirse en otra por medio del grupo de movimientos. Inicialmente, se podría esperar que todas las posiciones construibles fuesen realizables desde SALIDA, pero vemos que el grupo de posiciones posibles solo es la doceava parte de lo que podríamos esperar.

Conociendo las posiciones posibles, podemos ver ahora que es factible llegar a todas ellas empleando los sencillos movimientos descritos en secciones anteriores. Obsérvese que podemos utilizar nuestros procedimientos sencillos para producir cualquier permutación par de aristas, cualquier inversión de dos aristas y cualquier torsión de dos vértices en direcciones contrarias.

En primer lugar, consideremos las aristas. Basta demostrar que tenemos todas las parejas de 2-ciclos o todas las parejas de 3-ciclos, ya que estos generan las permutaciones pares. Se pueden trasladar cuatro (o tres) piezas-arista cualesquiera a cuatro (o tres) posiciones-arista cualesquiera en pocos movimientos. Es más, la última pieza puede estar en cualquiera de sus dos orientaciones. Después de hacerlo, podemos aplicar nuestro procedimiento básico a las cuatro (o tres) posiciones e invertir los movimientos anteriores para trasladar las posiciones a su lugar de origen. De este modo efectuamos una pareja de 2-ciclos (o un 3-ciclo) sobre las posiciones originales. (En la Teoría de Grupos este procedimiento se llama conjugación. La expresión general para P conjugado por Q es QPQ^{-1} . El conjugado de una permutación es una permutación con la misma estructura de ciclo. Básicamente un conjugado hace la misma acción con objetos diferentes.)

Un procedimiento para las aristas es

$$P_1 = P_1(F, R) = (F^2 R^2)^3 = (R^2 F^2)^3 \quad (2.2)$$

que es dos 2-ciclos: $(FU FD)(RU RD)$. Obsérvese que $P_1^2 = \text{Identidad}$, es decir $P_1^{-1} = P_1$, y $P_1(F, R) = P_1(R, F)$. Se ve este procedimiento en 2.9 y 2.10, la última siendo una versión esquemática de la primera.

Un breve estudio de la permutación dada por $(UF)_+(DF)_+$ y del razonamiento anterior nos permite deducir que se puede lograr una inversión de dos aristas cualesquiera.

Antes de continuar con los vértices, examinemos el proceso de conjugación más detalladamente. Como ilustración, consideremos los pormenores del problema dado

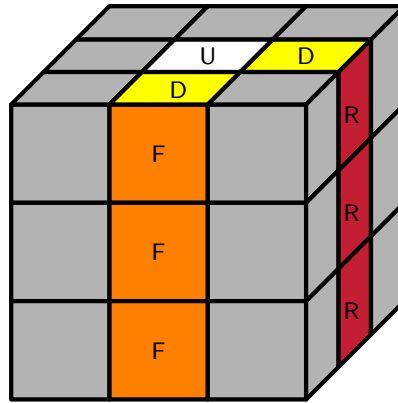


Figura 2.9

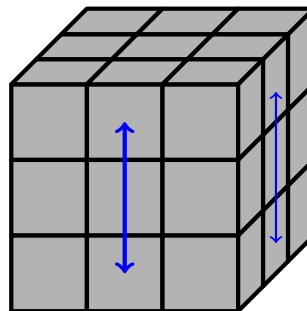
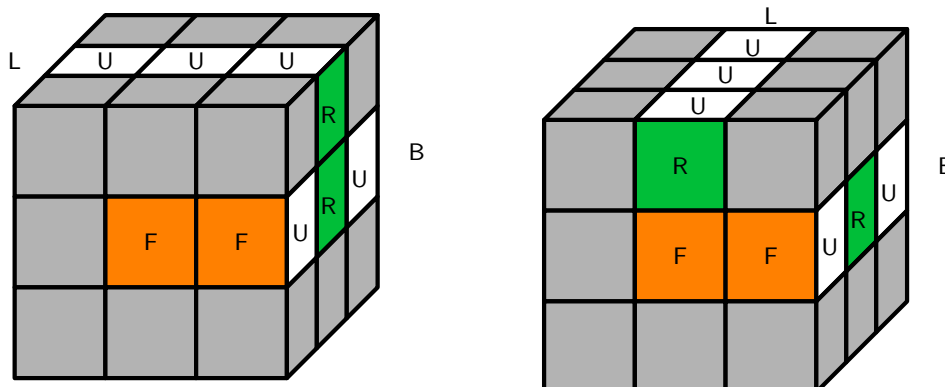


Figura 2.10

por obtener $(UF, UB)(UR, UL)$ utilizando P_1 . Aplicando FB^{-1} a la posición de SALIDA se produce la Figura 2.11 A, luego U da la Figura 2.11 B. Ahora estamos en condiciones de aplicar $P_1(R, U) = (R^2U^2)^3$, resultando la Figura 2.11 C. Entonces $U^{-1}BF^{-1}$ produce la Figura 2.11 D, que es el dibujo que buscamos. Por lo tanto, la solución del problema es

$$FB^{-1}U(R^2U^2)^3U^{-1}BF^{-1} = QPQ^{-1} \tag{2.3}$$

de donde $P = P_1(R, U) = (R^2U^2)^3$ y $Q = FB^{-1}U$. El proceso de conjugación juega un papel importante en la Teoría de Grupos y su clara utilidad en nuestro problema refleja su utilidad en general. Utilizando los razonamientos anteriormente señalados y el resultado del problema que acabamos de estudiar, podemos realizar todas las posibles manipulaciones de aristas.



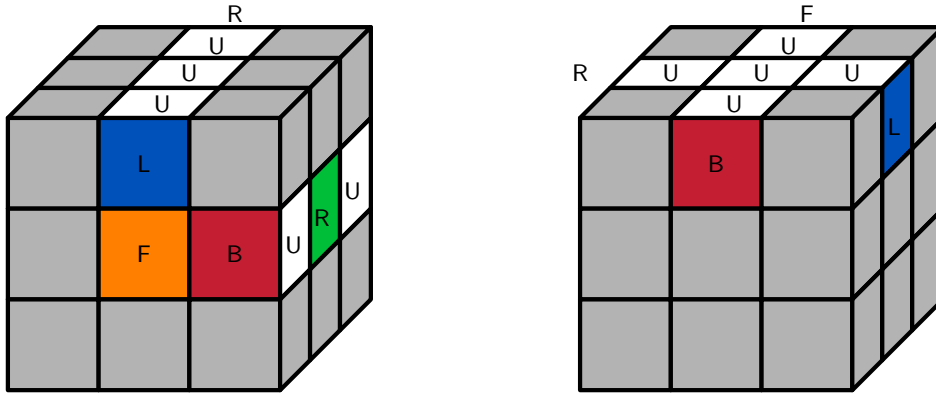


Figura 2.11: A, B, C y D

Ahora pues, podemos estudiar los vértices. Basta demostrar que tenemos todos los 3-ciclos o todas las parejas de 2-ciclos. Uno de ellos es suficiente, ya que podemos trasladar cuatro (o tres) piezas-vértice cualesquiera a cuatro (o tres) posiciones-vértice. Además, hemos de ver que podemos torcer una pareja de vértices cualesquiera en direcciones contrarias y será suficiente con ver que somos capaces de torcer una pareja cualquiera. Esencialmente, tenemos la misma clase de solución que para las aristas. A continuación se verá que existe la posibilidad de realizar los procedimientos por poco eficaces que estos sean.

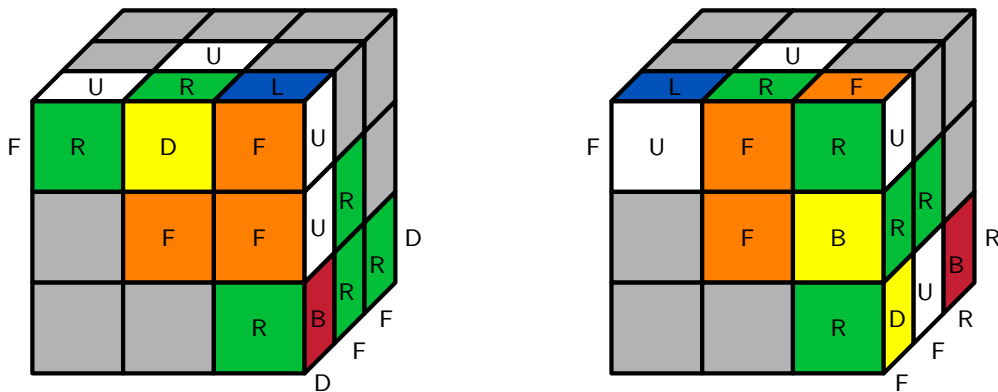
El procedimiento propuesto se basa en lo siguiente:

$$P_2 = P_2(F, R) = FRF^{-1}R^{-1} = (FLU, FUR)_+(FRD, DRB)_-(FU, FR, DR) \tag{2.4}$$

$$P_2 = P_2^2 = (FLU)_+(FUR)_+(FRD)_-(DRB)_-(FU, FR, DR) \tag{2.5}$$

$$P_2 = P_2^3 = (FLU, URF)(FRD, BDR) \tag{2.6}$$

Se ven los detalles en 2.12, y en 2.13 los esquemas.



Observe que $P_2^6 = Identidad$ y que $P_2(F, R)^{-1} = P_2(R, F)$. Al combinar P_2 con los procedimientos de aristas o al utilizar P_4 , podemos mover los vértices como queramos. Combinando dos P_3 y algunos procedimientos de arista, podemos torcer dos vértices adyacentes en direcciones contrarias. Como los procedimientos de aristas son fáciles de realizar utilizando P_1 , preferí originalmente poner bien todos los vértices utilizando P_2 y P_3 , sin hacer caso de las aristas, y después colocar estas con P_1 .

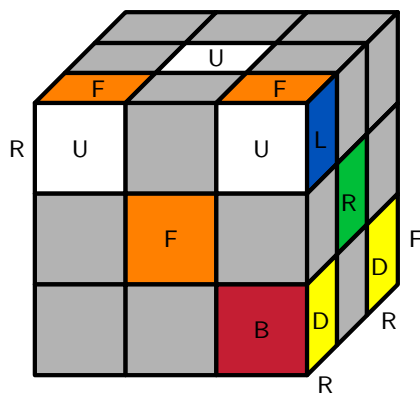


Figura 2.12

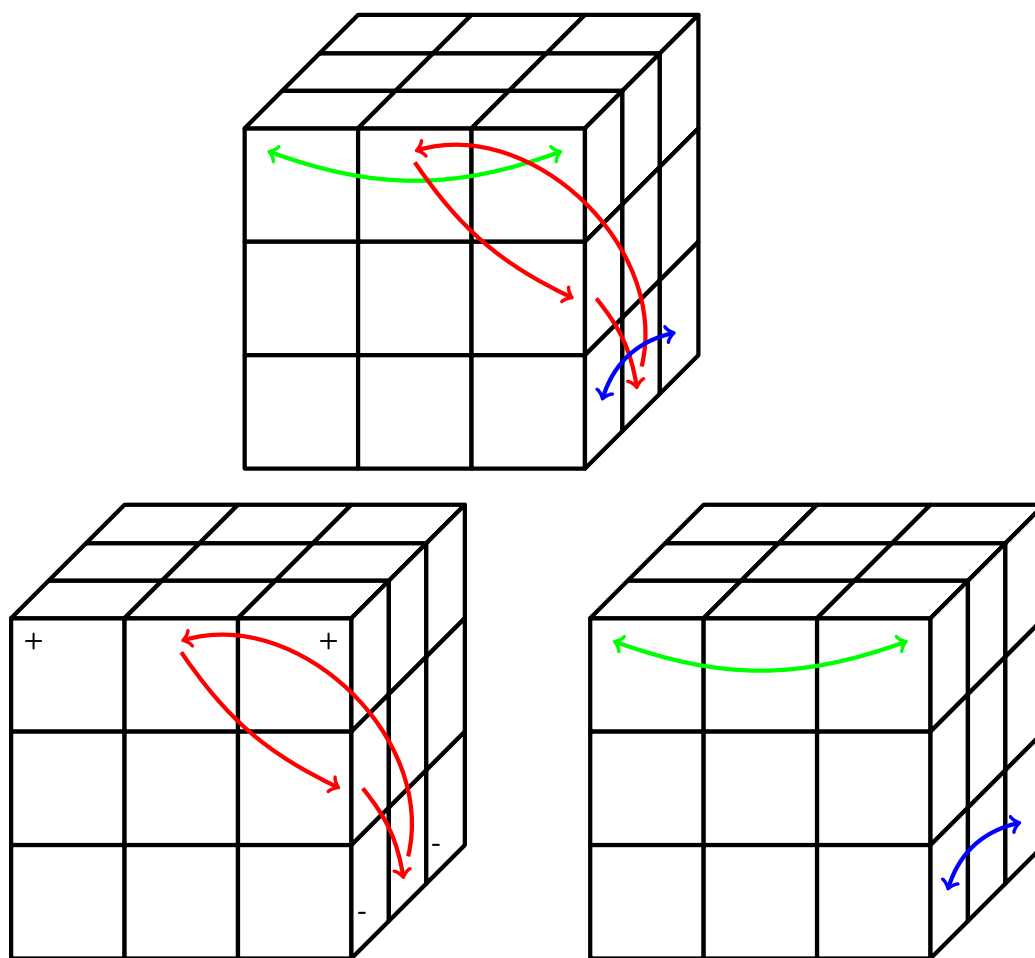


Figura 2.13

Ahora resumiremos un procedimiento para recomponer el cubo en la posición de SALIDA. No es muy eficaz, pero demuestra que es posible.

- 1 Colocar en su sitio todos los vértices inferiores (no requiere ningún procedimiento especial).
- 2 Si los vértices superiores forman una permutación impar, aplicar U .
- 3 Aplicar varias P_2 para colocar los vértices superiores en las posiciones correctas (varias P_2 implica varios conjugados de P_2 , etcétera).
- 4 Aplicar varias P_3 para torcer los vértices en las orientaciones correctas.
- 5 Aplicar varias P_1 para poner las aristas en sus lugares con las orientaciones correctas.

Encuentro que este algoritmo requiere muy poca memoria, ya que P_1 y P_2 son procedimientos sencillos, pero algunas veces las operaciones de conjugación son lo suficientemente complicadas como para tener que apuntarlas. Este procedimiento tiene como número máximo de movimientos requeridos para resolver el cubo 277. (Es decir, es un recuento muy pesado y puede ser algo impreciso.) Por movimiento, quiero decir un giro cualquiera o su cuadrado o su inverso, ya que todos ellos son movimientos individuales de la mano.

En la Teoría de Grupos, un producto $PQP^{-1}Q^{-1}$ se llama conmutador. $PQP^{-1}Q^{-1} = Id$ si y solo si $PQ = QP$, de forma que el conmutador es una indicación de si P y Q conmutan. Por lo tanto, el procedimiento P_2 es un conmutador en nuestro grupo.

Nos queda verificar la afirmación de que nos es posible invertir las aristas solamente en parejas y que únicamente podemos torcer los vértices como hemos indicado. Es un procedimiento bastante pesado, pero espero que el siguiente razonamiento sea lo suficientemente claro como para convencerles. Lo importante es que consideremos nuestras posiciones de vértice y arista en unas orientaciones determinadas y fijas, de modo que podamos examinar como un giro afecta a las orientaciones. Escribimos las 12 parejas de aristas y los 8 triples de vértices en alguna secuencia arbitraria como:

$$UF, UL, UB, UR, \dots, UFL, ULB, UBR, URF, \dots$$

Esta secuencia concreta facilita el examen del movimiento U . Aplicando U se permutaran las piezas, pero no se cambiará ninguna de las orientaciones de las parejas de triples. Sin embargo, no podemos esperar que las orientaciones siempre sean tan convenientes. Veamos lo que pasa si se varía la orientación de un vértice, por ejemplo, si se reemplaza ULB por LBU . A continuación del cambio, la acción de U sobre los vértices U es:

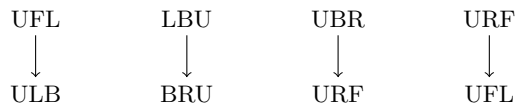


Figura 2.14

Vemos que la imagen de UFL no es LBU , sino es LBU desplazado un lugar hacia adelante, y que la imagen de LBU no es UBR , sino UBR desplazado un lugar hacia atrás. Si denotamos estos desplazamientos por $+1$ o -1 , tenemos que la suma de las modificaciones es 0. Técnicamente, hemos de considerar las modificaciones (*mod* 3), es decir, 3 desplazamientos de $+1$ nos llevan de nuevo a 0, por lo tanto $-1 = +2$, etc. Los

desplazamientos corresponden a las rotaciones de los vértices en 120° alrededor de su diagonal principal.

Ahora bien, puesto que la suma de los desplazamientos de orientación es 0 para un cambio cualquiera de orientación, debe ser 0 para dichos cambios, es decir, sera 0 para las orientaciones de los triples de los vértices. Simétricamente, es válido para cualquiera de nuestros seis giros básicos y, por lo tanto, es una propiedad conservada por los miembros de nuestro grupo. Puesto que la posición de SALIDA era una posición en que la suma de los desplazamientos de orientación fue de 0, cualquier posición posible debe tener una suma de 0 desplazamientos. Concretamente, si realizamos un dibujo en que cada vértice esta correctamente en su sitio, vemos con facilidad los desplazamientos de orientación como la suma de la torsión de los vértices, y por lo tanto el total de torsión de los vértices debe sumar a 0. Siempre se toma este total (*mod* 3).

Un razonamiento similar demuestra que la suma de las inversiones de las aristas debe ser 0 (*mod* 2), es decir, el número de inversiones de aristas siempre es par.

Tenemos a continuación algunos nuevos procedimientos parciales con estructuras bastante fáciles y que se pueden combinar de diversas formas útiles. Las combinaciones más importantes son las siguientes:

P es un procedimiento que actúa mínimamente sobre una cara o sección, como un mono-inversor o “mono-twist”. Si P actúa mínimamente sobre la cara U entonces $PU^n P'U^{-n}$ actuara solamente sobre U .

P es un procedimiento que traslada las piezas de una cara a otra. Si P traslada todas las piezas U a D , entonces $PD^n P'$ actuara solo sobre U .

En cualquier caso, si P es de orden 2, entonces $P^2 = \text{Identidad}$, $P = P'$ y las cosas se simplifican.

1. $R_a U^2 R'_a$ intercambia las columnas verticales RF e LB y las aristas adyacentes UF, UB . Este procedimiento es de orden 2.
2. $R^2 B^2 R^2 U^2 R_s$ traslada todas las piezas U a la cara B , con dos aristas invertidas.
3. $R^2 F_s^2 L^2$ traslada todas las piezas U a la cara D , con dos aristas intercambiadas. Es de orden 2.
4. $FDF^2 D^2 F^2 D'F' = M$ solamente intercambia $(URF, FLU) = (C, D+)$ en la cara U y es de orden 2. Es una manera fácil de poner los vértices U en su sitio una vez que estén en una permutación par.
5. $BR'D^2 RB'$ solo intercambia $(ULB, RFU) = (A, C)$ en la cara U y es de orden 2. Aunque sea un “mono-twist” no es muy útil. Sin embargo, $BR'D^2 RB'U^2$ produce AC_- y muchos 2-ciclos. De aquí que su cuadrado produzca A_-C . En algunos círculos se refieren a este procedimientos como “Dúo-twist de Rubik”.
6. $L'FD^2 LF^2 D'F$ solamente traslada $(A.C_-)D_-$ en la cara U . Le permite construir cierto número de movimientos de torsión.

2.5. El grupo del Cubo de Rubik 3x3x3

En esta sección, vamos a describir matemáticamente los movimientos del Cubo de Rubik 3x3x3. Para un mejor entendimiento, a partir de ahora denotaremos al grupo del Cubo de Rubik por R_3 .

Observación 4. *El grupo R_3 está contenido en S_{54} .*

Toda secuencia de movimientos modifica la colocación de las 54 (9 por 6 lados) caras coloreadas de los cubos unitarios (en realidad, podemos reducirlos a 48, puesto

que las 6 caras de las piezas centrales no se desplazan de sitio). Si vemos esto como un problema únicamente de la colocación de estas caras coloreadas estaríamos ante S_4 puesto que sería permutación de 54 elementos donde todos pueden ser intercambiados con todos. Pero este no es el caso del Cubo de Rubik puesto que, por ejemplo, las aristas están formadas por dos de estas caras coloreadas que no pueden ser separadas mediante ninguno de los movimientos que se pueden realizar en el cubo. Por lo tanto, el conjunto de los posibles estados del cubo tiene que estar contenido en el conjunto de las posibles permutaciones de 54 elementos.

Observación 5. El cubo tiene 6 caras y nosotros podemos realizar un movimiento tanto horario como anti-horario en cada una de las caras. Aunque dada la definición del movimiento horario de una de las caras como producto de dos ciclos de orden 4 dada anteriormente podemos sacar varias conclusiones muy importantes:

1. El movimiento en sentido horario de cualquiera de las caras es un movimiento de orden 4, esto es, $T^4 = Id$, $\forall T \in \{R, L, U, D, B, F\}$. Esto quiere decir que el movimiento en sentido antihorario de una cara, por ejemplo R , denotado por R^{-1} , sería lo mismo que decir R^3 . Por lo tanto podemos ver que :

$$R_3 = \langle R, L, U, D, B, F \rangle .$$

Además, podemos ver que no es abeliano ya que, por ejemplo, R y F al no ser disjuntos no conmutan. Los pares que conmutan son aquellos que son disjuntos (en nuestro caso serían los movimientos de caras contrarias):

$$UD = DU, \quad LR = RL \quad y \quad BF = FB.$$

2. Cada movimiento básico del cubo esta definido por un producto de dos ciclos disjuntos de orden 4. Si analizamos bien este producto podemos observar que se trata de un ciclo que mueve aristas en aristas y otro ciclo que mueve vértices en vértices.

2.5.1. Descripción matemática de los movimientos del cubo 3x3x3

En este apartado, vamos a describir matemáticamente los movimientos del Cubo de Rubik 3x3x3. Como veremos a continuación, esto nos llevara eventualmente a la descripción del grupo del Cubo de Rubik como un subgrupo de índice 12 como un producto directo de dos semi-productos.

Antes de nada, vamos a ver un Teorema que necesitaremos más adelante.

Teorema 2.5.1 (Primer Teorema Fundamental de la Teoría del Cubo de Rubik). Empezando con un cubo resuelto, identificamos las siguientes caras con un “+” invisible

1. cara U del subcubo arista UF .
2. cara U del subcubo arista UR .
3. cara F del subcubo arista FR .
4. todas las caras que pueden ser obtenidas desde las anteriores mediante un movimiento del grupo de las secciones.

Identificamos las caras U y D de cada subcubo esquina con un “+” invisible. Estos signos “+” son denominados “marcas de referencia estándar”. Cada movimiento g del Cubo de Rubik genera una nueva colección de etiquetas “+”, denominadas “marcas relativas a g ”. Entonces una posición del Cubo de Rubik está unívocamente determinada por el siguiente proceso de toma de decisiones:

- a) ¿Cómo están permutadas los subcubos aristas?
- b) ¿Cómo están permutados los subcubos centrales?
- c) ¿Cómo están permutados los subcubos esquina?
- d) ¿Cuáles de las “aristas con marcas relativas” están dadas la vuelta (en relación a la “marca de referencia estándar”)?
- e) ¿Cuáles de las “esquinas con marcas relativas” están rotadas con respecto a la “marca de referencia estándar” y, de ser así, por cuánto están rotadas (120° o 240° en sentido horario, en relación a las “marca de referencia estándar”)?

Notación

Primero, orientamos todas las esquinas y aristas como en el “Primer Teorema Fundamental de la Teoría del Cubo de Rubik”. Esto lo representamos de la siguiente manera, excepto que hemos reemplazado los signos “+” del “Primer Teorema Fundamental de la Teoría del Cubo de Rubik” por cuadrados blancos:

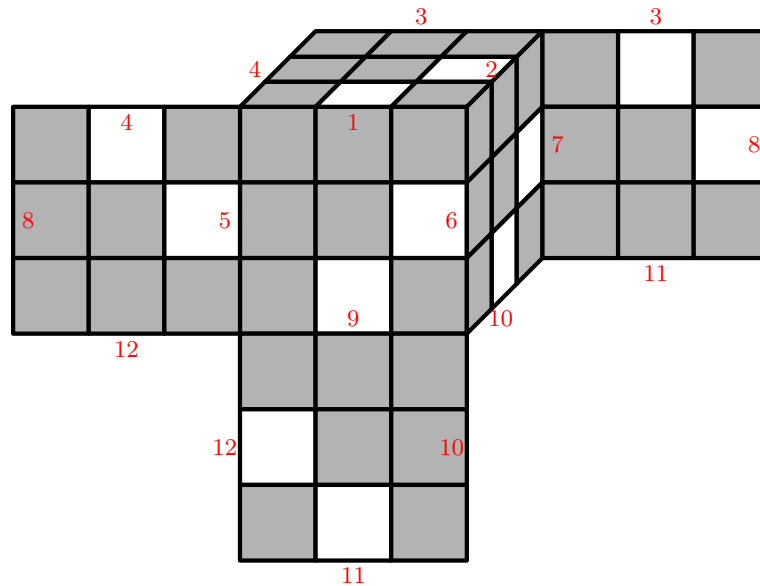


Figura 2.15

Sea $G = \langle R, L, U, D, F, B \rangle$ el grupo del Cubo de Rubik 3x3x3 y sea H el grupo generado por R, L, U, D, F, B “ampliado” y todos los movimientos “ilegales” (siendo estos últimos aquellos donde está permitido desarmar y volver a armar el cubo pero no remover ninguna pegatina).

Sea V el conjunto de vértices del cubo (que hemos identificado con el conjunto de subcubos esquina del Cubo de Rubik) y sea

$$\rho : H \rightarrow S_V \tag{2.7}$$

el homomorfismo que asocia a cada movimiento del Cubo de Rubik la correspondiente permutación de vértices.

Sea E el conjunto de aristas del cubo (que hemos identificado con el conjunto de subcubos arista del Cubo de Rubik) y sea

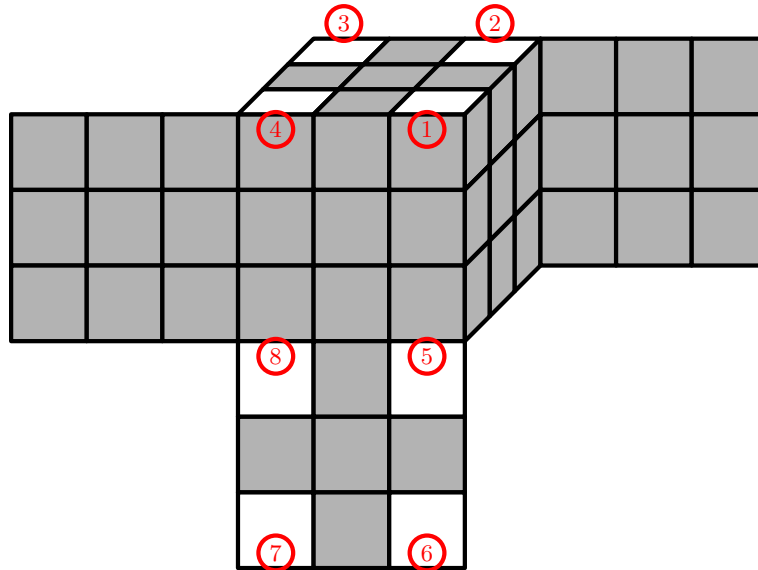


Figura 2.16

$$\sigma : H \rightarrow S_E \tag{2.8}$$

el homomorfismo que asocia a cada movimiento del Cubo de Rubik la correspondiente permutación de aristas.

Orientaciones de las esquinas

Sea $v : H \rightarrow C_3^8$ la función que asocia a cada movimiento $g \in H$ la correspondiente orientación de esquina. Más concretamente, sea $g \in H$ y digamos que g mueve la esquina i a la esquina j . Entonces $v_i(g) \in C_3$ es la orientación a la que el vértice i -ésimo es enviada por g , donde los vértices están identificados como en 2.16 y las orientaciones es el número de giros en sentido horario de 120° que se requieren para girar la “marca relativa” “+” obtenida de haber movido la esquina i a j usando el movimiento g a la “marca estándar de referencia” “+” en la esquina j .

Ejemplo 2.12.

X	$\vec{v}(X)$
F	$(2,0,0,1,1,0,0,2)$
U	$(0,0,0,0,0,0,0,0)$
$F * U$	$(2,0,0,1,1,0,0,2)$
$U * F$	$(2,0,0,1,1,0,0,2)$
D	$(0,0,0,0,0,0,0,0)$
B	$(0,1,2,0,0,2,1,0)$
R	$(1,2,0,0,2,1,0,0)$
L	$(0,0,1,2,0,0,2,1)$

Observación 6. Los efectos del movimiento $g \in H$ en las orientaciones de las esquinas también pueden ser vistos como un cambio en la etiqueta “+”. Nótese que un movimiento $g \in H$ tiene dos efectos en las esquinas:

a) Una permutación $\rho(g) \in S_V$ de los vértices.

b) Una reorientación de los vértices que se mueven en (a).

En particular, para $g, h \in H$, la orientación $\vec{v}(gh)$ solo puede diferir de $\vec{v}(g)$ en las coordenadas correspondientes a los vértices permutados por h .

Ahora verificaremos que la orientación “relativa” $\vec{v}(gh) - \vec{v}(g)$ es la misma orientación $\vec{v}(h)$, siempre y cuando se tenga en cuenta el efecto de g en los vértices: $\vec{v}(h) = \rho(g)(\vec{v}(gh) - \vec{v}(g))$ por ejemplo.

Lema 2.5.1. $\vec{v}(gh) = \vec{v}(g) + \rho(g)^{-1}(\vec{v}(h))$.

Demostración. Los movimientos gh orientan el i -ésimo subcubo esquina mediante $v_i(gh)$ y permuta los vértices mediante $\rho(gh)$ por definición.

Por otro lado, gh aplicará primero g y después h . El movimiento g reorienta el i -ésimo subcubo esquina mediante $v_i(g)$ y envía el i -ésimo vértice al $\rho(g)$ -ésimo vértice.

Para estudiar el posterior efecto de h en esto, restemos $\vec{v}(g)$ a $\vec{v}(gh)$, para volver a nuestra orientación original (añadiremos de nuevo $\vec{v}(g)$ más adelante). Llamaremos a esta posición el “cubo modificado” por ahora.

El movimiento h primero orienta el i -ésimo subcubo esquina del “cubo modificado” mediante $v_j(h)$ y lo permuta al vértice $\rho(h)(j)$. El i -ésimo subcubo del cubo modificado viene (por medio de g) desde el $\rho(g)^{-1}$ i -ésimo subcubo del cubo original. Por consiguiente, el i -ésimo subcubo esquina del “cubo modificado” es , mediante h , reorientado por $v_{\rho(g)^{-1}(i)}(h)$. Para esto debemos añadir $v_i(g)$ para conseguir el efecto global de gh en el i -ésimo vértice del original:

$$v_i(gh) = v_i(g) + v_{\rho(g)^{-1}(i)}(h), \tag{2.9}$$

para cada $1 \leq i \leq 8$, lo cual implica el resultado del Lema. □

Orientaciones de las aristas

Sea $w : H \rightarrow C_2^{12}$ la función que asocia la correspondiente orientación de esquinas a cada movimiento $g \in H$. Más concretamente, sea $g \in H$, decimos que g manda la esquina i a la esquina j . Entonces $w_i(g) \in C_2$ es la orientación a la que manda g el i -ésimo vértice, donde los vértices están identificados como en 2.15 y donde la orientación es el número de giros de 180° requeridos para girar la “orientación relativa” “+” obtenida mediante el movimiento de la esquina i a j usando el movimiento g en la “marca de referencia estándar” “+” en la esquina j .

Ejemplo 2.13.

X	$\vec{w}(X)$
F	(1,0,0,0,0,0,0,0,1,0,0,0)
U	(1,0,1,0,0,0,0,0,0,0,0,0)
$F * U$	(1,0,1,0,1,0,0,0,1,0,0,0)
$U * F$	(1,1,1,0,0,0,0,0,1,0,0,0)
D	(0,0,0,0,0,0,0,0,0,1,0,1)
B	(0,0,0,0,0,0,1,1,0,0,0,0)
R	(0,1,0,0,0,1,1,0,0,1,0,0)
L	(0,0,0,0,1,0,0,0,1,0,0,0)

Observación 7. Los efectos del movimiento $g \in H$ en las orientaciones de las aristas puede ser tenido en cuenta como una reidentificación de las marcas “+”.

Notemos que el movimiento $g \in H$ tiene dos efectos en las aristas:

- a) Una permutación $\sigma(g) \in S_E$ de las aristas.
 b) Una reorientación de las aristas que fueron movidas en (a).

En particular, para $g, h \in H$, la orientación $\vec{w}(gh)$ solo puede diferir de $\vec{w}(g)$ en las coordenadas que corresponden a las aristas permutadas por h .

Ahora podemos decir que

$$\vec{w}(gh) = \vec{w}(g) + \sigma(g)^{-1}(\vec{w}(h)), \quad (2.10)$$

por ejemplo, que

$$w_i(gh) = w_i(g) + w_{\sigma(g)^{-1}(i)}(h), \quad (2.11)$$

para cada $1 \leq i \leq 12$. La prueba para esto es similar a la prueba del Lema anterior.

El producto semi-directo

Considérese el siguiente producto directo de dos productos semi-directos:

$$H' = (C_3^8 \rtimes S_V) \mathbf{x} (C_2^{12} \rtimes S_E). \quad (2.12)$$

Observación 8. Esto también puede ser escrito en la notación de productos corona como el siguiente producto directo de dos productos corona:

$$H' = (S_V \mathbf{wr} C_3^8) \times (S_E \mathbf{wr} C_2^{12}). \quad (2.13)$$

Como conjunto, podemos pensar en H como un elemento perteneciente a $C_3^8 \times S_V \times C_2^{12} \times S_E$. Si representásemos los elementos h, h' de H como $h = (v, r, w, s)$, $h' = (v', r', w', s') \in C_3^8 \times S_V \times C_2^{12} \times S_E$ entonces la operación del grupo estaría dada por:

$$h * h' = (v, r, w, s) * (v', r', w', s') = (v + P(r)(v'), rr', w + P(s)(w'), ss'). \quad (2.14)$$

Consideremos la función

$$\begin{aligned} \kappa : H &\rightarrow (C_3^8 \rtimes S_V) \mathbf{x} (C_2^{12} \rtimes S_E) \\ g &\longmapsto (v(g), \rho(g), w(g), \phi(g)). \end{aligned} \quad (2.15)$$

Proposición 2.5.1. κ es un isomorfismo, $H \cong H'$.

Demostración. Dado que

$$\begin{aligned} &(\vec{v}(g), \rho(g), \vec{w}(g), \sigma(g)) * (\vec{v}(h), \phi(h), \vec{w}(h), \sigma(h)) \\ &= (\vec{v}(g) + P(\rho(g))(\vec{v}(h)), \rho(g)\rho(h), \vec{w}(g) + P(\sigma(g))(\vec{w}(h)), \sigma(g)\sigma(h)), \end{aligned} \quad (2.16)$$

la aplicación κ es un homomorfismo. Y ya que podemos conseguir cualquier reorientación y permutación mediante algún movimiento ilegal, κ debe ser sobreyectiva. Por el “Primer Teorema Fundamental de la Teoría de Cubos”, el núcleo de κ es trivial (esto es una manera bonita de decir que si ningún subcubo es permutado o reorientado, entonces el cubo no cambia). \square

2.6. Segundo Teorema Fundamental de la Teoría de Cubos

Primero vamos hacer unos resultados previos. Identificamos, como en la sección anterior, cada $g \in G$ con una cuaterna

$$(\vec{v}(g), \rho(g), \vec{w}(g), \sigma(g))$$

donde

1. $\rho(g)$ es la permutación correspondiente del conjunto de vértices V del cubo.
2. $\sigma(g)$ es la permutación correspondiente al conjunto de aristas E del cubo.
3. $v(g), w(g)$ son “orientaciones” definidas en la sección 2.5.

Observación 9. Sea S_n el grupo simétrico de n letras. Identificamos S_V con S_8 y S_E con S_{12} .

Ejemplo 2.14. Sea G el grupo del Cubo de Rubik generado por los movimientos básicos R, L, U, D, F, B . Para cada movimiento $g \in G$, sea $\rho(g)$ la correspondiente permutación del conjunto de vértices V y sea $\sigma(g)$ la correspondiente permutación del conjunto de aristas E del cubo. Sea S_n el grupo simétrico de n letras e identifiquemos S_V con S_8 y S_E con S_{12} . Entonces:

- a) $\rho : G \rightarrow S_8$ es un homomorfismo.
- b) $\sigma : G \rightarrow S_{12}$ es un homomorfismo.

Por este ejemplo, sabemos que:

- a) $\rho : G \rightarrow S_8$ es un homomorfismo.
- b) $\sigma : G \rightarrow S_{12}$ es un homomorfismo.

Observación 10. Dada una cuaterna (v, r, w, s) , donde r, s son permutaciones de las esquinas y aristas, respectivamente, como hemos visto y

$$v \in C_3^8, \quad w \in C_2^{12}, \quad (2.17)$$

¿qué condiciones se deben dar en r, s, v, w para que corresponda con un posible estado del Cubo de Rubik?

La respuesta la tenemos con el siguiente teorema, de acuerdo con [Berlekamp, Conway and Guy \(1982\)](#).

Teorema 2.6.1 (Segundo Teorema Fundamental de la Teoría de Cubos). Una cuaterna (v, r, w, s) como la definida anteriormente ($r \in S_8, s \in S_{12}, v \in C_3^8, w \in C_2^{12}$) corresponde a un posible estado del Cubo de Rubik si y solo si

- a) $\text{sgn}(r) = \text{sgn}(s)$, (“igualdad de paridad en las permutaciones”).
- b) $v_1 + \cdots + v_8 \equiv 0 \pmod{3}$, (“conservación del total de giros”).
- c) $w_1 + \cdots + w_{12} \equiv 0 \pmod{2}$, (“conservación del total de giros de 180° ”).

Demostración. Primero vamos a probar la implicación \Leftarrow , el solo si. Para ello, suponemos que $(v, r, w, s) \in S_V \times S_E \times C_3^8 \times C_2^{12}$ representa una (legalmente obtenida) posición del Cubo de Rubik. Desde este punto vamos a probar (a)-(c).

Sea $g \in G$ el elemento que mueve el Cubo de Rubik desde la posición resuelta hasta la posición asociada a esta cuaterna. Entonces $r = \rho(g)$ y $s = \sigma(g)$. Sabemos que

g puede ser descrita como una palabra (concatenación de letras) en referencia a los movimientos básicos R, L, U, D, F, B . Sea $g = X_1 \dots X_k$, donde cada X_i es alguno de los movimientos básicos R, L, U, D, F, B . Observemos que si X es alguno de los movimientos básicos entonces $sgn(\rho(X)) = sgn(\sigma(X))$. Como sgn, ρ , y σ son homomorfismos, se sigue que

$$sgn(r) = sgn(\rho(g)) = \prod_{i=1}^k sgn(\rho(X_i)) = \prod_{i=1}^k sgn(\sigma(X_i)) = sgn(\sigma(X)) = sgn(s) \quad (2.18)$$

Esto prueba (a).

Hemos verificado (b) para los movimientos básicos en el ejemplo propuesto en la subsección “orientaciones de las esquinas”. Nótese que:

- I) La condición de conservación de los giros en (b) es cierta para (v_1, \dots, v_8) si y solo si es cierta para cualquier permutación $P(p)(v) = (v_{(1)p}, \dots, v_{(8)p})$.
- II) Si (v_1, \dots, v_8) y (v'_1, \dots, v'_8) satisfacen cada una la condición de conservación de giros de (b), entonces su suma también la cumplirá.

Como hemos visto anteriormente, escribiendo g como una palabra en los movimientos básicos R, L, U, D, F, B , decimos que $g = X_1 \dots X_k$, donde cada X_i es alguno de los movimientos básicos R, L, U, D, F, B . Suponemos que esta expresión es mínima en el sentido de que elegimos los X_i de manera que k es lo más pequeño posible. Este k se denomina “longitud” de g (esta longitud es la misma que la distancia desde g hasta la identidad en el grafo de Cayley de G).

Ahora probaremos (b) mediante inducción sobre la longitud. Ya hemos probado con anterioridad para todas las palabras de longitud $k = 1$.

Supongamos $k > 1$. Dada la fórmula sobre la orientación del producto de dos movimientos en términos de las dos orientaciones de los movimientos, tenemos que:

$$\vec{v}(X_1 \dots X_{k-1} X_k) = \rho(X_1 \dots X_{k-1})^{-1}(\vec{v}(X_k)) + \vec{v}((X_1 \dots X_{k-1})). \quad (2.19)$$

El término $\rho(X_1 \dots X_{k-1})^{-1}(\vec{v}(X_k))$ satisface la condición de conservación de los giros de (b) por (i). El término $\vec{v}((X_1 \dots X_{k-1}))$ satisface la condición de conservación de los giros de (b) por hipótesis de inducción. Su suma satisface la condición de conservación de los giros de (b) por (ii). Esto prueba (b).

La prueba de (c) es muy similar a la prueba de (b), excepto que se utilizaría el ejemplo de la sección “Orientaciones de las aristas” en vez del ejemplo de la sección “Orientaciones de las esquina”.

Ahora, debemos probar la implicación “ \Rightarrow ”. En otras palabras, suponiendo (a), (b) y (c) debemos ver que existe un correspondiente estado del Cubo de Rubik.

Primero, vamos a probar un caso especial. Supongamos que r y s son ambos la Identidad y que $(w_1, \dots, w_{12}) = (0, \dots, 0)$.

Existe un movimiento que tuerce exactamente dos subcubos esquina y mantiene las orientaciones y posiciones de todos los otros subcubos. Por ejemplo, el movimiento $g = (R^{-1}D^2RB^{-1}U^2B)^2$ tuerce el subcubo esquina URF mediante un giro de 120° en sentido horario, el subcubo esquina BDL mediante un giro de 240° en sentido horario, y mantiene la orientación y posición de todos los otros subcubos. Este movimiento puede ser fácilmente modificado, mediante una conjugación apropiada, para obtener

un movimiento que tuerza cualquier par de subcubos esquina, y mantenga la orientación y posición del resto de subcubos. Estos movimientos generan todos los posibles octetos que satisfacen la condición de conservación de giros de (b). Esto prueba la implicación “ \Rightarrow ” en el caso de que r y s sean ambos la Identidad y que $(w_1, \dots, w_{12}) = (0, \dots, 0)$.

Tras esto, vamos a probar otro caso especial. Supongamos que r y s son ambos la Identidad y que $(v_1, \dots, v_8) = (0, \dots, 0)$.

Existe un movimiento que gira exactamente dos subcubos arista y mantiene las orientaciones y posiciones del resto de subcubos. Por ejemplo, el movimiento $g = LFR^{-1}F^{-1}L^{-1}U^2RURU^{-1}R^2U^2R$ gira el subcubo arista UF , el subcubo arista UR y mantiene las orientaciones y posiciones del resto de subcubos. Este movimiento puede ser fácilmente modificado, mediante una conjugación apropiada, para obtener un movimiento que gire cualquier par de subcubos arista y mantenga las posiciones y orientaciones del resto de subcubos. Estos movimientos generan todas las duodécuplas que satisfacen la condición de conservación de giros de 180° de (c). Esto prueba la implicación “ \Rightarrow ” en el caso de que r y s sean ambos la Identidad y que $(v_1, \dots, v_8) = (0, \dots, 0)$.

Como consecuencia de estos dos casos especiales, podemos deducir que la implicación “ \Rightarrow ” es cierta en el caso de que r y s sean ambos la Identidad.

Finalmente, probemos un último caso especial. Supongamos que $(w_1, \dots, w_{12}) = (0, \dots, 0)$ y que $(v_1, \dots, v_8) = (0, \dots, 0)$. Consideremos las siguientes tres observaciones:

1. Dados cualquiera tres subcubos arista, existe un movimiento que es un 3-ciclo sobre estos subcubos arista que mantiene la orientación y posición del resto de subcubos.
2. Dados cualquiera tres subcubos esquina, existe un movimiento que es un 3-ciclo sobre estos subcubos esquina que mantiene la orientación y posición del resto de subcubos.
3. Dados cualquier par de subcubos esquina y cualquier par de subcubos arista, existe un movimiento que es un 2-ciclo, o trasposición, sobre dichos subcubos arista, y un 2-ciclo sobre dichos subcubos esquina y mantiene la orientación y posición del resto de subcubos.

Por la proposición 2.1.2, sabemos que A_E está generado por los 3-ciclos de aristas descritos en 1. y que A_V esta generado por los 3-ciclos de esquinas descritos en 2. En otras palabras, podemos construir un estado del Cubo de Rubik asociado a cualquier cuaterna $(r, s, 0, 0)$, siempre y cuando $r \in A_V$ y $s \in A_E$. El subgrupo $A_E \times A_V$ tiene orden 4 en $S_E \times S_V$ ya que $|S_n/A_n| = 2$. El tercer tipo de movimientos, los 2-ciclos esquina-arista, no corresponden con un elemento del subconjunto $A_E \times A_V$ del grupo del Cubo de Rubik dado que un 2-ciclo de aristas es una permutación impar de las aristas. Por lo tanto si suponemos que el subgrupo $S_E \times S_V$ generado por todos los tres tipos de movimientos, obtendremos o bien todo $S_E \times S_V$ o bien algun subgrupo de índice 2 que contiene a $A_E \times A_V$. La primera posibilidad puede ser descartada ya que contradice la condición de paridad de (a). El único subgrupo de índice dos de $S_E \times S_V$ que contiene a $A_E \times A_V$ es el subgrupo de elementos que satisfacen la condición de paridad de (a).

Se sigue de esto mismo que la implicación “ \Rightarrow ” es verdad en el caso de que ambos v y w sean cero.

El teorema es una consecuencia de estos casos especiales por la siguiente afirmación:

Siempre existe un movimiento, sin importar el estado del Cubo de Rubik en el que se encuentre, que no permuta ningún subcubo pero si “soluciona ”la orientación del cubo para hacer que ambas v y w sean cero.

□

Corolario 1.

$$R_3 = \{g = (v, r, w, s) \in H \mid (a), (b), (c) \text{ del teorema anterior}\}.$$

2.6.1. Algunas consecuencias

Ahora reformularemos el hecho anterior sobre el grupo del Cubo de Rubik desde un punto de vista que nos permita contar más fácilmente el número de elementos que tiene.

Sea

$$\begin{aligned} G_0 &= \{(v, r, w, s) \mid r \in S_8, s \in S_{12}, \\ &v = (v_1, v_2, \dots, v_8), v_i \in \{0, 1, 2\}, v_1 + \dots + v_8 \equiv 0(\text{mod}3), \\ &w = (w_1, w_2, \dots, w_{12}), w_i \in \{0, 1\}, w_1 + \dots + w_{12} \equiv 0(\text{mod}2)\}. \end{aligned} \quad (2.20)$$

Definimos la operacion binaria $*$: $G_0 \times G_0 \rightarrow G_0$ dada por:

$$(v, r, w, s) * (v', r', w', s') = (v + P(r)(v'), r * r', w + P(s)(w'), s * s').$$

Esta operación define una estructura de grupo sobre G_0 . G_0 es un subgrupo del grupo ampliado de R_3 de índice 6.

Teorema 2.6.2. *Existe un isomorfismo*

$$G_0 \cong (C_3^7 \rtimes S_8) \times (C_2^{11} \rtimes S_{12}),$$

donde C_n es el grupo cíclico de n elementos y \rtimes denota el producto semi-directo y donde C_n^k ($n = 2, 3, k = 7, 11$) esta identificado con el subgrupo de C_n^{k+1} definido por

$$\{v = (v_1, v_2, \dots, v_k) \mid v_i \in \{0, 1, n - 1\}, v_1 + \dots + v_k \cong 0(\text{mod}n)\}.$$

En particular,

$$|G_0| = |S_8||S_{12}||C_2^{11}||C_3^7| = 8! \cdot 12! \cdot 2^{11} \cdot 3^7.$$

Teorema 2.6.3. *El grupo del Cubo de Rubik G es el núcleo del homomorfismo*

$$\Phi : G_0 \rightarrow \{1, -1\}$$

$$(v, r, w, s) \rightarrow \text{sgn}(r)\text{sgn}(s).$$

En particular, $G < G_0$ es normal de índice 2 y

$$|G| = 8! \cdot 12! \cdot 2^{10} \cdot 3^7.$$

Cabe recalcar que el grupo conmutador G_1 de G es el subgrupo que esta formado por todos los productos finitos de los conmutadores

$$[g, h] = g * h * g^{-1} * h^{-1},$$

donde g, h son elementos aleatorios de G .

Teorema 2.6.4. $|G_1| = |G|/2$.

De hecho, podemos hallar explícitamente G_1 .

Teorema 2.6.5.

$$G_1 = \{g \in G \mid \text{sgn}(\rho(g)) = \text{sgn}(\sigma(g)) = 1\}.$$

Llegamos a esto debido al hecho de que el subgrupo conmutador de S_n es A_n , para $n > 4$.

El último teorema descrito implica que $|G/G_1| = 2$. Desde aquí podemos deducir que G_1 es un subgrupo normal de G .

Teoría de Grafos dentro del Cubo de Rubik

En este capítulo vamos a introducir una interpretación gráfica de un grupo de permutaciones, el grafo de Cayley, para luego interpretarlo en el caso especial de un puzle de permutaciones.

Para empezar, vamos a definir qué es un grafo.

Definición 3.1 (Grafo). *Un grafo es un par de conjuntos contables (V, E) , donde*

1. V es un conjunto contable de elementos individuales llamados vértices.
2. E es un subconjunto de pares sin ordenar $\{\{v_1, v_2\} : v_1, v_2 \in V\}$ llamados aristas.

Un grafo se dibuja simplemente uniendo estos puntos que representan vértices con un segmento de línea si pertenecen a la misma arista.

Definición 3.2 (Grafo dirigido). *Un grafo dirigido es un par de conjuntos contables (V, E) , donde*

1. V es un conjunto contable de vértices.
2. E es un subconjunto de pares ordenados $\{(v_1, v_2) : v_1, v_2 \in V\}$ llamados aristas.

Un grafo dirigido se dibuja simplemente uniendo los puntos que representan vértices con una flecha si pertenecen a la misma arista (v_1, v_2) , la flecha se origina en v_1 y se dirige apuntando a v_2 .

Si $e = \{v_1, v_2\}$ pertenece a E entonces decimos que e es una arista de v_1 a v_2 (o de v_2 a v_1).

Definición 3.3 (Camino). *Si v y w son vértices, un camino desde v a w es una secuencia finita de aristas que empiezan en v y terminan en w :*

$$e_0 = \{v, v_1\}, e_1 = \{v_1, v_2\}, \dots, e_n = \{v_n, w\} \quad (3.1)$$

Definición 3.4 (Grafo conectado). *Si existe un camino desde v hasta w entonces decimos que v está conectado con w . Decimos que un grafo (V, E) está conectado si cualquier pareja de vértices están conectados. El número de aristas que salen desde un vértice v se denomina grado (o valencia) de v , y lo denotamos como $\text{grado}(v)$.*

Definición 3.5 (Grado de un vértice). *El número de aristas que salen desde un vértice v se denomina grado (o valencia) de v , y lo denotamos como $\text{grado}(v)$.*

Ejemplo 3.6. Sean

$$V = \{A, B, C\}, E = \{\{A, B\}, \{A, C\}, \{B, C\}\},$$

entonces podemos dibujar el grafo (V, E) como
Cada vértice tiene valencia 2.

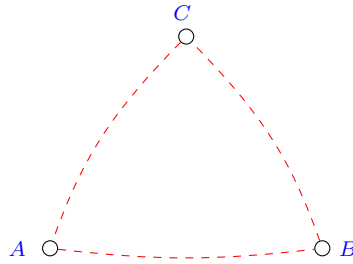


Figura 3.1

Definición 3.7 (Distancia entre vértices). Si v y w son vértices conectados el uno con el otro en un grafo (V, E) , entonces definimos la distancia de v a w , denotándolo por $d(v, w)$, por

$$d(v, w) = \min_{v, w \in V \text{ conectados}} \#\{\text{aristas en un camino de } v \text{ a } w\}$$

Por convenio, Si v y w no están conectados entonces decimos que $d(v, w) = \infty$.

Definición 3.8 (Diámetro de un grafo). El diámetro de un grafo es la mayor distancia posible:

$$\text{diam}((V, E)) = \max_{v, w \in V} d(v, w).$$

En la figura 3.1 del ejemplo 3.6, el diámetro del grafo es 1.

3.1. Grafo de Cayley

Definición 3.9 (Grafo de Cayley). Sea G el grupo de permutaciones,

$$G = \langle g_1, g_2, \dots, g_n \rangle < S_X.$$

El grafo de Cayley de G con respecto a $X = \{g_1, g_2, \dots, g_n\}$ es el grafo (V, E) cuyos vértices V son elementos de G y cuyas aristas están determinadas por la siguiente condición:

Si x e y pertenecen a $V = G$, entonces existe una arista desde x hasta y (o desde y hasta x) si y solo si $y = g_i * x$ o $x = g_i * y$, para algún $i = 1, 2, \dots, n$.

Definición 3.10 (Grafo dirigido de Cayley). Sea G el grupo de permutaciones,

$$G = \langle g_1, g_2, \dots, g_n \rangle < S_X.$$

El grafo de Cayley dirigido de G con respecto a $X = \{g_1, g_2, \dots, g_n\}$ es el grafo dirigido (V, E) cuyos vértices V son los elementos de G y cuyas aristas están determinadas por la siguiente condición:

Si x e y pertenecen a $V = G$ entonces, existe una arista desde x hasta y si y solo si $y = g_i * x$, para algún $i = 1, 2, \dots, n$.

Lema 3.1.1. Sea $\Gamma_G = (V, E)$ el grafo de Cayley asociado al grupo de permutaciones $G = \langle g_1, g_2, \dots, g_n \rangle$. Sea $N = |g_1, g_1^{-1}, g_2, g_2^{-1}, \dots, g_n, g_n^{-1}|$. Entonces, para todo $v \in V$, $\text{grado}(v) = N$.

Demostración. Supongamos que no es cierto. Entonces existe un $v \in V = G$ con $\text{grado}(v) < N$ o $\text{grado}(v) > N$.

Primero, notamos que, para cada $h \in g_1, g_1^{-1}, g_2, g_2^{-1}, \dots, g_n, g_n^{-1}$, el conjunto $v, h * v$ es una arista de Γ_G . Esto viene de la definición del grafo de Cayley.

Si $r = \text{grado}(v) > N$ entonces, por definición del grafo de Cayley, existen distintos $v_1, \dots, v_r \in V$ con $v = h_i * v_i$ para todo $1 \leq i \leq r$, donde los h_1, \dots, h_r son elementos distintos de $g_1, g_1^{-1}, g_2, g_2^{-1}, \dots, g_n, g_n^{-1}$. Esto contradice la definición de N .

Si $r = \text{grado}(v) < N$ entonces, por definición del grafo de Cayley, existen distintos $h_i, h_j \in g_1, g_1^{-1}, g_2, g_2^{-1}, \dots, g_n, g_n^{-1}$, con $v = h_i * v_i$ tales que $h_i * v = h_j * v$. Como G es un grupo y $V = G$ (como conjuntos), podemos cancelar las v de ambos lados de la ecuación $h_i * v = h_j * v$, contradiciendo la suposición de que h_i es distinto de h_j . □

Ejemplo 3.11. Sea

$$G = \langle s_1, s_2 \rangle = S_3,$$

donde $s_1 = (1, 2)$, y $s_2 = (2, 3)$. Entonces el grafo de Cayley de G con respecto a $X = \{s_1, s_2\}$ se puede ver como:

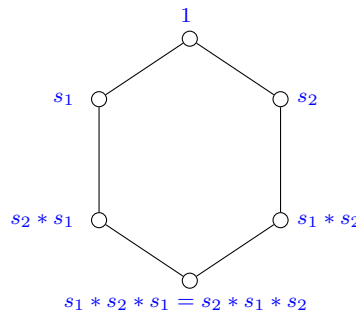


Figura 3.2: Grafo de Cayley de S_3

Sea

$$G = \langle s_1, s_2 \rangle = S_3, \tag{3.2}$$

donde $s_1 = (1, 2)$, y $s_2 = (2, 3)$. Entonces el grafo de Cayley dirigido de G con respecto a $X = \{s_1, s_2\}$ se puede ver como:

Ejemplo 3.12. Sea

$$G = \langle R, L, U, D, F, B \rangle = S_{54}$$

el grupo del Cubo de Rubik 3x3x3. Cada posición del cubo corresponde con un elemento del grupo G (por ejemplo, el movimiento que tendrías que hacer para conseguir una posición concreta). Dicho de otra manera, cada posición del cubo corresponde con un vértice del grafo de Cayley. Cada vértice de este grafo tiene valencia 12.

Además, una solución del Cubo de Rubik es simplemente un camino en el grafo desde el vértice asociado a la posición actual del cubo hasta el vértice asociado al elemento identidad. El número de movimientos en la solución más corta posible es simplemente la distancia desde el vértice asociado a la posición actual del cubo al vértice asociado con el elemento identidad. El diámetro del grafo de Cayley de G es el número de movimientos de la mejor solución en el peor escenario.

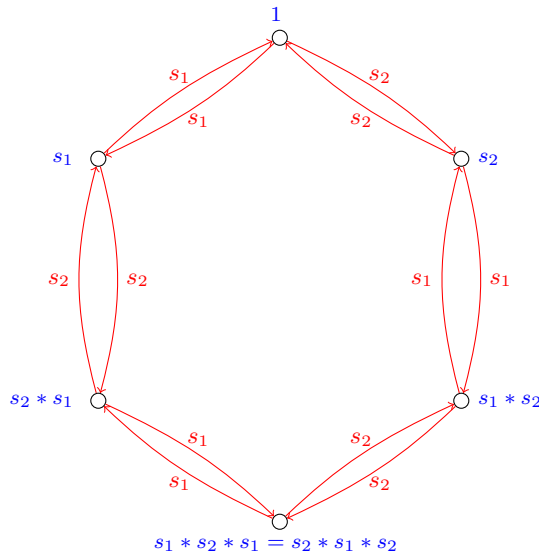


Figura 3.3: Grafo dirigido de Cayley de S_3

3.2. Algoritmo de Dios

Problema 1. Sea G el grupo de permutaciones de un puzle. Encuentra el diámetro del grafo de Cayley de G

Este problema está sin resolver para muchos puzles y parece ser muy difícil en términos computacionales. Los casos donde está resuelto son:

Puzle	Diámetro
“Pyraminx”	11
Cubo de Rubik 2x2x2	14
Cubo de Rubik 3x3x3	20

Tabla 3.1: Diámetros de puzles

Problema 2. Sea G el grupo de un puzle de permutaciones y sea v un vértice del grafo de Cayley de G . Encuentra un algoritmo para determinar el camino desde v hasta el vértice v_0 asociado a la identidad teniendo una distancia igual a la distancia desde v hasta v_0 .

Este problema es bastante más complicado. El algoritmo, de existir, se llama “Algoritmo de Dios”. Una buena referencia para el progreso reciente en el algoritmo de Dios para varios puzles relacionados con el Cubo de Rubik se puede encontrar en la página web de “Cubeman”.

3.2.1. La historia del Número de Dios

En 1980, se estableció una cota inferior para el Número de Dios analizando el número de secuencias de movimientos esencialmente distintas de 17 movimientos o menos, y hallando que había muchas menos secuencias que posiciones del Cubo de Rubik. La primera cota superior fue probablemente alrededor de 80 por el algoritmo en uno de los primeros libros de soluciones para el Cubo de Rubik. Esta tabla sacada de Rokicki (2010) resume los resultados posteriores:

Fecha	Inf.	Sup.	Brecha	Notas y enlaces
Julio, 1981	18	52	34	Morwen Thistlethwaite prueba que 52 son suficientes.
Diciembre, 1990	18	42	24	Hans Kloosterman mejora esto a 42 .
Mayo, 1992	18	39	21	Michael Reid muestra que 39 son siempre suficientes.
Mayo, 1992	18	37	19	Dik Winter lo reduce a 37 un día después.
Enero, 1995	18	29	11	Michael Reid baja la cota superior a 29 analizando el algoritmo de Kociemba en dos fases .
Enero, 1995	20	29	9	Michael Reid prueba que la posición <i>superflip</i> (esquinas correctas, aristas bien ubicadas pero torcidas) requiere 20 .
Diciembre, 2005	20	28	8	Silviu Radu muestra que 28 son siempre suficientes.
Abril, 2006	20	27	7	Silviu Radu mejora esta cota a 27 .
Mayo, 2007	20	26	6	Dan Kunkle y Gene Cooperman prueban que 26 son suficientes.
Marzo, 2008	20	25	5	Tomas Rokicki reduce la cota superior a 25 .
Abril, 2008	20	23	3	Tomas Rokicki y John Welborn reducen la cota superior a solo 23 .
Agosto, 2008	20	22	2	Tomas Rokicki y John Welborn continúan bajando la cota a 23 .
Julio, 2010	20	20	0	Tomas Rokicki, Herbert Kociemba, Morley Davidson, and John Dethridge prueban que el Número de Dios para el Cubo de Rubik es exactamente 20 .

Tabla 3.2: Evolución de las cotas inferiores y superiores del Número de Dios.

En todo lo referente a la información que facilitamos sobre el Número de Dios tenemos que tener en cuenta que estamos hablando en lo que se denomina “métrica de 180° ” (aquí se cuentan como movimiento cualquier tipo de rotación de una misma cara). Existe otro sistema que se denomina “métrica de 90° ” la cual en la página web [cube20.org](#) se demostró en 2014 por Tomas Rokicki y Morley Davidson que el Número de Dios para este tipo de métrica es 26.

3.3. Circuitos Hamiltonianos en el Cubo de Rubik

Definición 3.13 (Circuito Hamiltoniano). Sea Γ un grafo. Un circuito Hamiltoniano en Γ es una secuencia de aristas formando un camino en Γ que pasa por cada vértice exactamente una vez. (Si se piensa en los vértices como ciudades y en las aristas como carreteras, entonces el circuito Hamiltoniano es un tour visitando cada ciudad exactamente una vez).

El siguiente problema sin resolver fue primeramente mencionado en este contexto por A. Schwenk:

Problema 3. Sea G el grupo del puzle del Cubo de Rubik $3 \times 3 \times 3$.

¿Tiene el grafo de Cayley de G un circuito Hamiltoniano?

En otras palabras, ¿podemos “visitar” cada posición posible del Cubo de Rubik exactamente una vez, usando cada vez únicamente uno de los generadores básicos: R, L, U, D, F, B ?

Este es un caso especial de un problema más general sin resolver:

Para un grupo de permutaciones arbitrario con más de dos elementos, no se sabe si el grafo de Cayley es Hamiltoniano.

Un ejemplo de esto mismo donde sí se sabe la respuesta es el siguiente:

Ejemplo 3.14. Sea G el grupo S_n con generadores dados por el conjunto de todas las trasposiciones:

$$G = S_n, X = \{(i, j) | 1 \leq i < j \leq n\}.$$

Hay muchas más trasposiciones que las necesarias para generar S_n , ya que el subconjunto de las trasposiciones de la forma $(i, i + 1), 1 \leq i \leq n - 1$, es suficiente para generar S_n . El algoritmo de Steinhaus–Johnson–Trotter nos muestra que existe un circuito Hamiltoniano en el grafo de Cayley de S_n con respecto a X . Podemos ver una versión del mismo en [Johnson \(1963\)](#).

3.4. Observaciones sobre aplicaciones, NP-completo

La ciencia computacional utiliza los grafos de Cayley para modelar redes interconectadas para procesos en paralelo. El problema de encontrar un algoritmo eficiente para resolver rápidamente el rompecabezas de tamaño $m \times n$ es conocido por ser desafiante. Se asemeja a la búsqueda del camino más corto entre dos puntos en un grafo, lo cual suele ser un problema computacionalmente fácil. La dificultad radica en que el número de vértices y aristas no crece de manera polinómica con respecto al tamaño del rompecabezas (es decir, $n \times m$). Por lo tanto, requiere enfoques específicos y adaptados a esta complejidad para encontrar una solución eficiente.

Hay categorías de problemas llamados problemas “NP-completos”. Sin entrar en demasiados detalles, lo que nos haría tener que explayarnos demasiado, esta es una categoría de problemas que son en algún sentido “igualmente difíciles” de resolver. Si puedes encontrar un algoritmo de “tiempo polinómico” para resolver uno de ellos entonces puedes encontrar uno para resolver cualquier otro problema de esta categoría también. Por ejemplo [Gary and Johnson \(1979\)](#) y [Berlekamp, Conway and Guy \(1982\)](#) tienen una lista de juegos y puzzles cuyas soluciones son problemas NP-completos.

3.5. Aproximación al algoritmo de Dios por Programación Entera

El Cubo de Rubik tiene (en la versión estándar) $3 \times 3 \times 3$ subcubos coloreados. Como se menciona en [Korf \(1997\)](#), en cada movimiento cualquier plano de subcubos $3 \times 3 \times 1$ se puede rotar 90° , 180° o 270° en relación al resto del cubo. El objetivo del juego es encontrar secuencias de movimientos que devuelvan como resultado que cada cara del cubo tenga un único color. El problema que vamos a estudiar a continuación es encontrar una estrategia resolutive (secuencia de movimientos) que requiera el mínimo número de movimientos para conseguir el objetivo. Esta estrategia se llama “Algoritmo de Dios”. Existen varios algoritmos que fueron propuestos por [Kociemba \(1992\)](#), [Korf \(1997\)](#), [Rokicki \(2008\)](#) y muchos otros. Sin embargo, como pudimos ver en la sección anterior, no fue hasta Julio de 2010 que Tomas Rokicki, Herbert Kociemba, Morley Davidson, and John Dethridge prueban que el Número de Dios para el Cubo de Rubik es exactamente [20](#).

3.5.1. Modelos Matemáticos

Un Cubo de Rubik estándar $3 \times 3 \times 3$ puede ser representado como la Figura [3.4](#). Hemos identificado todos los subcubos del 1 al 54 y vamos a denominarlo “Mapa del Cubo de Rubik”. En la imagen que aparece debajo, $A - I$ y $I - XII$ representan las leyendas de la tabla. Usaremos los superíndices $+$ y $-$ para los movimientos correspondientes (por ejemplo, A^+ significa un giro de izquierda a derecha de 90° de la línea A

y XII^- significa un giro de arriba hacia abajo de 90° de la columna XII). Obsérvese que más de una línea o columna puede ser afectada por un único movimiento, por ejemplo, E^+ afecta únicamente a la fila E, pero V^- afecta tanto a la columna V como a la columna XI.

-	+	I	II	III	IV	V	VI	VII	VIII	IX	X	XI	XII
↔													
A					1	2	3						
B					4	5	6						
C					7	8	9						
D													
E	10	11	12	13	14	15	16	17	18	19	20	21	
F	22	23	24	25	26	27	28	29	30	31	32	33	
G	34	35	36	37	38	39	40	41	42	43	44	45	
H					46	47	48						
I					49	50	51						
					52	53	54						

Figura 3.4: Mapeo del Cubo de Rubik [Aksop \(2009\)](#)

Usaremos dos conjuntos de variables de decisión.

El primer conjunto de variables de decisión controla el patrón actual del cubo y está definido de la siguiente manera:

$$x_{i,t} : \{ \text{El índice del color del subcubo identificado en } i \text{ en el momento } t. \} \quad (3.3)$$

Como existen 6 colores diferentes en el Cubo de Rubik, $x_{i,t}$ puede tomar valores enteros de 1 a 6. El segundo conjunto de variables de decisión controla los movimientos y está definido de la siguiente manera:

$$y_{i,t} = \begin{cases} 1, & \text{si el momento } t \text{ es un movimiento } i \\ 0, & \text{en otro caso} \end{cases} \quad (3.4)$$

donde el movimiento i -ésimo está definido de la siguiente manera:

i	1	2	3	4	5	6	7	8	9
movimiento	A^+	A^-	B^+	B^-	C^+	C^-	D^+	D^-	E^+
i	10	11	12	13	14	15	16	17	18
movimiento	E^-	F^+	F^-	IV^+	IV^-	V^+	V^-	VI^+	VI^-

Entonces $y_{3,t}$ significa que el t -ésimo movimiento es B^+ . Definamos un nuevo conjunto llamado “Mapeo ” de la siguiente manera:

$$Mapeo = (k, i, j) \in [1, \dots, 18] \times [1, \dots, 54]^2 \quad (3.5)$$

Esto quiere decir que el subcubo en la posición i del mapa del Cubo de Rubik se moverá a la posición j si realizamos el movimiento k . Así, un modelo matemático para el “Algoritmo de Dios” se describe de la siguiente manera:

$$\text{mín} \sum_{i=1}^{18} \sum_{t=1}^{54} t \cdot y_{i,t} \quad (3.6)$$

$$\forall t \in 1, \dots, 53, \forall (k, i, j) \in Mapeo$$

$$x_{i,t} - 6 \cdot (1 - y_{k,t}) \leq x_{j,t+1} \leq x_{i,t} + 6 \cdot (1 - y_{k,t}) \quad (3.7)$$

$$x_{j,t} - 6 \cdot (1 - y_{k+1,t}) \leq x_{i,t+1} \leq x_{j,t} + 6 \cdot (1 - y_{k+1,t}) \quad (3.8)$$

$$x_{i,t} - 6 \cdot \left[y_{k,t} + y_{k+1,t} + \sum_{\substack{(l,i,n) \in \text{Mapeo} \\ l \neq k}} (y_{l,t} + y_{l+1,t}) \right] \leq x_{i,t+1} \\ \leq x_{i,t} + 6 \cdot \left[y_{k,t} + y_{k+1,t} + \sum_{\substack{(l,i,n) \in \text{Mapeo} \\ l \neq k}} (y_{l,t} + y_{l+1,t}) \right] \quad (3.9)$$

$$\forall t = 1, \dots, 54$$

$$\sum_{i=1}^{18} y_{i,t} \leq 1 \quad (3.10)$$

Logramos un nuevo patrón en el mapa del Cubo de Rubik con las restricciones 3.7 y 3.8 si hacemos un movimiento positivo o negativo a $x_{i,j}$ respectivamente. Las restricciones de 3.9 hacen que $x_{i,t} = x_{i,t+1}$ si el subcubo i no se mueve en el movimiento t -ésimo. La última restricción satisface que solo se haga un movimiento del cubo por iteración.

Hemos ejecutado el código en Python que proporcionamos en A.1 con Gurobi y hemos obtenido los siguientes resultados:

Tam. ini	Seed	Tiempo	Objetivo	Movimientos	Tam. ini	Seed	Tiempo	Objetivo	Movimientos
4	0	1.0	2	[8, 1]	6	0	1.5	4	[16, 15, 8, 1]
4	1	50.4	4	[3, 8, 2, 4]	6	1	51.3	4	[3, 8, 2, 4]
4	2	1.7	4	[11, 2, 1, 2]	6	2	35.7	6	[9, 5, 11, 2, 1, 2]
4	3	8.4	4	[11, 4, 17, 7]	6	3	682.6	6	[2, 15, 11, 4, 17, 7]
4	4	2.5	4	[12, 3, 7, 9]	6	4	29.0	6	[4, 15, 12, 3, 7, 9]
4	5	17.2	4	[0, 16, 11, 8]	6	5	1672.8	6	[7, 14, 0, 16, 8, 11]
4	6	191.1	4	[1, 8, 15, 2]	6	6	12.0	4	[4, 8, 15, 2]
4	7	58.7	4	[1, 12, 4, 10]	6	7	924.2	6	[17, 2, 1, 12, 4, 10]
4	8	2.1	4	[4, 12, 7, 11]	6	8	46.0	6	[1, 6, 4, 12, 7, 11]
4	9	2.2	4	[4, 8, 11, 14]	6	9	621.6	6	[5, 4, 0, 11, 8, 14]
5	0	0.9	3	[16, 8, 1]	7	0	19.1	5	[15, 12, 16, 8, 1]
5	1	34.5	5	[15, 3, 8, 2, 4]	7	1	35.2	5	[15, 3, 8, 2, 4]
5	2	28.7	5	[5, 11, 2, 2, 1]	7	2	29.2	5	[5, 11, 2, 2, 1]
5	3	337.1	5	[15, 11, 4, 17, 7]	7	3	5060.4	7	[0, 2, 15, 11, 4, 17, 7]
5	4	12.9	5	[15, 12, 3, 7, 9]	7	4	2494.3	7	[2, 4, 15, 12, 3, 7, 9]
5	5	110.0	5	[14, 0, 16, 11, 8]	7	5	3721.2	7	[1, 7, 14, 0, 16, 8, 11]
5	6	0.9	3	[8, 15, 2]	7	6	125.5	5	[15, 4, 8, 15, 2]
5	7	9.3	5	[2, 1, 12, 4, 10]	7	7	5892.0	7	[3, 17, 2, 1, 12, 4, 10]
5	8	12.4	5	[6, 4, 12, 11, 7]	7	8	2863.7	7	[2, 1, 6, 4, 12, 11, 7]
5	9	287.2	5	[5, 4, 11, 8, 14]	7	9	3183.6	7	[10, 5, 4, 0, 8, 11, 14]

Conclusiones

El presente trabajo exploró la fascinante conexión entre el Cubo de Rubik, un rompecabezas tridimensional, y los principios matemáticos subyacentes.

La Teoría de Grupos desempeñó un papel fundamental en la resolución del Cubo de Rubik, con la identificación de diferentes subgrupos generados por los movimientos del cubo. Se destacaron dos teoremas clave que contribuyen a la comprensión de la Teoría de Grupos y su aplicación en la resolución del Cubo de Rubik.

En el campo de la Teoría de Grafos, se exploró el concepto del “Número de Dios” en relación con el Cubo de Rubik. Este número representa la cantidad mínima de movimientos necesarios para resolver cualquier configuración del cubo, y su estudio proporciona información valiosa sobre la complejidad del rompecabezas.

Además, se presentó un modelo de programación entera en Python, basado en el lenguaje GLPK, para resolver el Cubo de Rubik. Los resultados obtenidos a partir de la ejecución de este programa brindaron una visión práctica de la aplicabilidad de la programación entera en la resolución del cubo.

En conjunto, este trabajo ha demostrado cómo el Cubo de Rubik puede utilizarse como una herramienta valiosa en la enseñanza de las matemáticas, la Teoría de Grupos y la Teoría de Grafos. Los hallazgos obtenidos contribuyen a la comprensión de los principios matemáticos involucrados y su aplicación en la resolución de problemas complejos.

Bibliografía

- Aksop, C. (2009). God's algorithm for Rubik's Cube an integer programming approach. In International Mathematical Forum (Vol. 4, No. 45, pp. 2217-2222). Citeseer.
- Berlekamp, E. R., Conway, J. H., Guy, R. K. (1982). Winning Ways. Vol. 2: Games in Particular.
- Gary, M. R., Johnson, D. S. (1979). Computers and Intractability: A Guide to the Theory of NP-completeness.
- Joyner, W. D. (1996). Mathematics of the Rubik's cube. Spring semester, 7, 1-275.
- Kociemba, H. (1992). Close to God's algorithm. Cubism for Fun, 28(April), 10-13.
- Korf, R. E. (1997, July). Finding optimal solutions to Rubik's Cube using pattern databases. In AAAI/IAAI (pp. 700-705).
- Rokicki, T. (2008). Twenty-five moves suffice for Rubik's cube. arXiv preprint arXiv:0803.3435.
- Rokicki, T. (2010). God's number is 20. "<http://www.cube20.org/>".
- Singmaster, D. (1981). Notas sobre el cubo de Rubik: texto fundamental sobre el gran maestro. Altalena.
- Johnson, S. M. (1963). Generation of permutations by adjacent transposition. Mathematics of computation, 17(83), 282-285.

A

Anexos

A.1. Propuesta de Algoritmo de Dios en Python

```
# Instalamos las librerías que vamos a usar
import random
import numpy as np
import math
import matplotlib.pyplot as plt
import random

!pip install ortools
from ortools.linear_solver import pywraplp

# Esta función imprime un estado del cubo de Rubik en un formato
más amigable
def imprime_rubik(conf) :
    for fila in range(3) :
        print('_____', end='')
        for i in range(2) :
            print('', conf[fila*3+i], end=',')
            print('', conf[fila*3+2])
    for fila in range(3) :
        for i in range(11) :
            print('', conf[9+fila*12+i], end=',')
            print('', conf[9+fila*12+11])
    for fila in range(3) :
        print('_____', end='')
        for i in range(2) :
            print('', conf[45+fila*3+i], end=',')
            print('', conf[45+fila*3+2])
    print()

# Parametros
moves = 18 # Diferentes movimientos posibles (consideramos
también los giros de 180°)
max_moves = 8 # Cota superior del número de movimientos
hasta resolverlo
cells = 54 # 6x9 celdas coloreadas
M = range(moves)
T = range(max_moves)
```

```
T0 = range(max_moves-1)
I = range(cells)
EPS = 0.1
```

```
# Movimiento 1 = B, Movimiento 2 = B-
# Movimiento 3 = , Movimiento 4 = B-
# Movimiento 1 = B, Movimiento 2 = B-
# Movimiento 1 = B, Movimiento 2 = B-
# Movimiento 1 = B, Movimiento 2 = B-
```

```
Mapeo = [
    [1, 1, 18], [1, 2, 30], [1, 3, 42], [1, 10, 3],
    [1, 22, 2], [1, 34, 1], [1, 18, 54], [1, 30, 53],
    [1, 42, 52], [1, 52, 10], [1, 53, 22], [1, 54, 34],
    [1, 19, 43], [1, 20, 31], [1, 21, 19], [1, 31, 44],
    [1, 33, 20], [1, 43, 45], [1, 44, 33], [1, 45, 21],
    [3, 4, 17], [3, 5, 29], [3, 6, 41], [3, 11, 6],
    [3, 23, 5], [3, 35, 4], [3, 17, 51], [3, 29, 50],
    [3, 41, 49], [3, 49, 11], [3, 50, 23], [3, 51, 35],
    [3, 47, 12], [3, 48, 24], [3, 49, 36], [5, 7, 16],
    [5, 8, 28], [5, 9, 40], [5, 12, 9], [5, 24, 8],
    [5, 36, 7], [5, 16, 48], [5, 28, 47], [5, 40, 46],
    [5, 48, 12], [5, 47, 27], [5, 46, 39], [5, 13, 15],
    [5, 14, 27], [5, 15, 39], [5, 25, 14], [5, 27, 38],
    [5, 37, 13], [7, 10, 13], [7, 11, 14], [7, 12, 15],
    [7, 13, 16], [7, 14, 17], [7, 15, 18], [7, 16, 19],
    [7, 17, 20], [7, 18, 9], [7, 19, 10], [7, 20, 11],
    [7, 1, 3], [7, 2, 6], [7, 3, 9], [7, 4, 2],
    [7, 6, 8], [7, 7, 1], [7, 8, 4], [7, 9, 7],
    [9, 22, 25], [9, 23, 26], [9, 24, 27], [9, 25, 28],
    [9, 26, 29], [9, 27, 30], [9, 28, 31], [9, 29, 32],
    [9, 30, 33], [9, 31, 22], [9, 32, 23], [9, 33, 24],
    [11, 34, 37], [11, 35, 38], [11, 36, 39], [11, 37, 40],
    [11, 38, 41], [11, 39, 42], [11, 40, 43], [11, 41, 44],
    [11, 42, 45], [11, 43, 34], [11, 44, 35], [11, 45, 36],
    [11, 46, 48], [11, 47, 51], [11, 48, 54], [11, 49, 47],
    [11, 51, 53], [11, 52, 46], [11, 53, 49], [11, 54, 52],
    [13, 1, 45], [13, 4, 33], [13, 7, 21], [13, 13, 1],
    [13, 25, 4], [13, 37, 7], [13, 21, 52], [13, 33, 49],
    [13, 45, 46], [13, 46, 13], [13, 49, 25], [13, 52, 37],
    [13, 10, 34], [13, 11, 22], [13, 12, 10], [13, 22, 35],
    [13, 24, 11], [13, 34, 36], [13, 35, 24], [13, 36, 12],
    [15, 2, 44], [15, 5, 32], [15, 8, 20], [15, 14, 2],
    [15, 26, 5], [15, 38, 8], [15, 20, 53], [15, 32, 50],
    [15, 44, 47], [15, 47, 14], [15, 50, 26], [15, 53, 38],
    [17, 3, 43], [17, 6, 31], [17, 9, 19], [17, 15, 3],
    [17, 27, 6], [17, 39, 9], [17, 19, 54], [17, 31, 51],
```



```

[17, 43, 48], [17, 48, 15], [17, 51, 27], [17, 54, 39],
[17, 16, 18], [17, 17, 30], [17, 18, 42], [17, 28, 17],
[17, 30, 41], [17, 40, 16], [17, 41, 28], [17, 42, 40] ]

resuelto = [6, 6, 6,
            6, 6, 6,
            6, 6, 6,
            3, 3, 3, 5, 5, 5, 1, 1, 1, 4, 4, 4,
            3, 3, 3, 5, 5, 5, 1, 1, 1, 4, 4, 4,
            3, 3, 3, 5, 5, 5, 1, 1, 1, 4, 4, 4,
            2, 2, 2,
            2, 2, 2,
            2, 2, 2 ]

# Restamos 1 a todas las celdas de mapeo para numerar las
celdas de 0 a 53 en lugar de 1 a 54.
print(Mapeo)
for i in range(len(Mapeo)) :
    for j in range(3) :
        Mapeo[i][j] -= 1
#print(Mapeo)

# En esta matriz almacenamos como cambian las posiciones despu s
de cada uno de los movimientos
# Es decir si matrix[k,i] = j significa que despu s de aplicar
el movimiento k
# la celda en la posici n i pasa a la posici n j (pudiendo ser
las mismas posiciones i y j)
# Utilizando esta estructura de datos solo es necesaria la
restricci n (3.15)
matrix = np.zeros((moves, cells), int)
for k in M :
    for i in I :
        matrix[k,i] = i
for s in Mapeo :
    matrix[s[0],s[1]]=s[2]
    matrix[s[0]+1,s[2]]=s[1]

#print(matrix)

# Configuraci n inicial
#conf_ini = [6, 6, 3,
#            3, 6, 6,
#            4, 5, 5,
#            1, 2, 2, 3, 3, 3, 2, 1, 5, 6, 3, 5,
#            1, 3, 2, 5, 5, 6, 5, 1, 1, 5, 4, 2,
#            2, 4, 1, 6, 4, 3, 4, 1, 2, 1, 2, 1,
#            4, 3, 6,
```

```

#           6, 2, 4,
#           5, 4, 4 ]

# Este c digo lo podemos ejecutar si queremos partir desde una
# posici n aleatoria
# despu s de n (pocos) movimientos barajando el cubo
def genera_conf_inicial(n, seed = 0) :
    random.seed(seed)
    conf_ini = np.zeros(cells , int)
    temp = np.zeros(cells , int)

    for i in I :
        conf_ini[i] = resuelto[i]

    for l in range(n) :
        k = random.randint(0,moves-1)
        for i in I :
            temp[i] = conf_ini[i]
        for i in I :
            conf_ini[i] = temp[matrix[k,i]]
    return conf_ini

# conf_ini = genera_conf_inicial(6, 0)

# imprime_rubik(conf_ini)
# imprime_rubik(resuelto)

# Aqu est la parte m s importante del c digo con el
# modelo matem tico
# Que utiliza el vector conf_ini como elemento de partida
# para resolverlo
def modelo_Rubik() :

    #solver = pywraplp.Solver('Rubik',
    pywraplp.Solver.CBC_MIXED_INTEGER_PROGRAMMING)
    solver = pywraplp.Solver('Rubik',
    pywraplp.Solver.GUROBLMIXED_INTEGER_PROGRAMMING)

    solver.SetTimeLimit(7200000)

    x = { (i,t) : solver.IntVar(1, 6, 'x[%i,%i]' % (i,t))
    for i in I for t in T }
    y = { (m,t) : solver.BoolVar('y[%i,%i]' % (m,t))
    for m in M for t in T }

```

```

solver.Minimize( solver.Sum( y[m,t] for m in M for t in T ) )

# Fijamos la posici n inicial
[ solver.Add(x[i,0] == conf_ini[i]) for i in I]
# Fijamos la posici n final
[ solver.Add(x[i,max_moves-1] == resuelto[i]) for i in I]

# En cada paso (periodo) realizamos a lo sumo un movimiento
[ solver.Add(solver.Sum(y[k,t] for k in M ) <= 1) for t in T]

# Si realizamos el movimiento k en el periodo t e cambio de color
en cada celda
# viene dado por la informaci n almacenada en matriz
[ solver.Add(x[i,t] - 6*(1 - y[k,t]) <= x[matrix[k,i],t+1])
for k in M for i in I for t in T0]
[ solver.Add(x[i,t] + 6*(1 - y[k,t]) >= x[matrix[k,i],t+1])
for k in M for i in I for t in T0]

# Si no hacemos ning n movimiento el cubo se mantiene igual
[ solver.Add(x[i,t] - 6*(solver.Sum(y[k,t] for k in M ))
<= x[i,t+1]) for i in I for t in T0]
[ solver.Add(x[i,t] + 6*(solver.Sum(y[k,t] for k in M ))
>= x[i,t+1]) for i in I for t in T0]

# Restricci n que evita algunas simetr as
[ solver.Add(solver.Sum(y[k,t] for k in M ) >= solver.Sum(y[k,t+1]
for k in M )) for t in T0]

# Lo solucionamos
global status
status = solver.Solve()

global time
time = solver.WallTime()/1000
global obj
obj = solver.Objective().Value()

global sec_mov
sec_mov = []
if status == pywraplp.Solver.OPTIMAL:
    for t in T :
        for m in M :
            if y[m,t].solution_value() > EPS :
                sec_mov.append(m)

# A partir de aqu utilizamos bucles para resolver varios ejemplos
de este problema,

```

```

# variando el n emro de movimientos que realizamos para barajar el
cubo y variando la semilla aleatoria.
# Los resultados se escriben en un fichero
fichero_resultados = "results.txt"

f = open(fichero_resultados , 'a')
f.write("Tam\ini\tseed\tstatus\tTiempo\tObjetivo\t
Movimientos\tSec_ini\n")
f.close()

for tam in range(4,8) :
    for s in range(10) :
        conf_ini = genera_conf_inicial(tam, s)
        print('Resolviendo un Rubik barajado ', tam, ' veces ,
con semilla ', s)
        modelo_Rubik()
        f = open(fichero_resultados , 'a')
        f.write(str(tam))
        f.write("\t")
        f.write(str(s))
        f.write("\t")
        f.write(str(status))
        f.write("\t")
        f.write(str(time))
        f.write("\t")
        f.write(str(obj))
        f.write("\t")
        f.write(str(sec_mov))
        f.write("\t")
        f.write(str(conf_ini))
        f.write("\n")
        f.close()

```

Rubik's Cube: Exploring its Mathematical Intricacies

Guillermo Zamora Andrés

Facultad de Ciencias • Sección de Matemáticas
 Universidad de La Laguna
 alu0101167060@ull.edu.es

Abstract

In this work, we will explore the fascinating connection between this three-dimensional puzzle and mathematical principles. Through different chapters, the methods of solving the Rubik's Cube will be examined. Group Theory will be introduced, and the subgroups generated by the cube's movements will be explored. Additionally, the Graph Theory will be addressed, and an integer programming model for solving the cube will be presented in Python based on a GLPK model. This article showcases how the Rubik's Cube can be utilized as a valuable tool for teaching mathematics, Group Theory, and Graph Theory.

1. The Rubik's Cube and its variants

In this chapter we will explore the cube-solving methods for the standard Rubik's Cube.

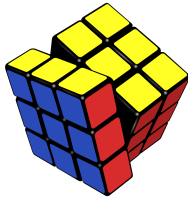


Figure 1: Rubik's Cube.

We will also get a bit into the Rubik's Cube most famous variants as:



Figure 2: Rubik's Revenge.

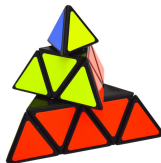


Figure 2: Pyraminx.

2. Rubik's Cube and Group Theory

Theorem 2.1 (Second Fundamental Theorem of Cube Theory)

A 4-tuple (v, r, w, s) ($r \in S_8, s \in S_{12}, v \in C_3^8, w \in C_2^{12}$) corresponds to a possible position of the Rubik's Cube if and only if

- $sgn(r) = sgn(s)$, ("equal parity as permutations").
- $v_1 + \dots + v_8 \equiv 0 \pmod{3}$, ("conservation of total twists").
- $w_1 + \dots + w_{12} \equiv 0 \pmod{2}$, ("conservation of total flips").

Corollary 1

$$R_3 = \{g = (v, r, w, s) \in H \mid (1), (2), (3) \text{ in the above theorem hold}\}.$$

2.1 Some consequences

Theorem 2.2 There is an isomorphism

$$G_0 \cong (C_3^7 \rtimes S_8) \times (C_2^{11} \rtimes S_{12}),$$

where C_n is the cyclic group with n elements and \rtimes denotes the semi-direct product and where C_n^k ($n = 2, 3, k = 7, 11$) is identified with the subgroup of C_n^{k+1} defined by

$$\{v = (v_1, v_2, \dots, v_k) \mid v_i \in \{0, 1, n-1\}, v_1 + \dots + v_k \equiv 0 \pmod{n}\}.$$

In particular,

$$|G_0| = |S_8| |S_{12}| |C_2^{11}| |C_3^7| = 8! \cdot 12! \cdot 2^{11} \cdot 3^7.$$

3. Graph Theory inside Rubik's Cube

Definition 1 (Cayley digraph) Let G be a permutation group,

$$G = \langle g_1, g_2, \dots, g_n \rangle < S_X.$$

The Cayley digraph of G with respect to $X = \{g_1, g_2, \dots, g_n\}$ is the digraph (V, E) whose vertices V are the elements of G and whose edges are determined by the following condition:

If x and y belong to $V = G$ then there is an edge from x to y if and only if $y = g_i * x$, for some $i = 1, 2, \dots, n$.

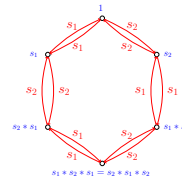


Figure 3: Grafo dirigido de Cayley de S_3

References

- [1] Aksop, C. (2009). Godás algorithm for Rubik's Cube an integer programming approach. In International Mathematical Forum (Vol. 4, No. 45, pp. 2217-2222). Citeseer.
- [2] Joyner, W. D. (1996). Mathematics of the Rubik's cube. Springer semester, 7, 1-275.
- [3] Singmaster, D. (1981). Notas sobre el cubo de Rubik: texto fundamental sobre el gran maestro. Altalena.