El cubo de Rubik y la mecánica cuántica

Daniel E. Borrajo Gutiérrez
Universidad Complutense de Madrid

3 de febrero de 2019

Resumen

Investigamos el problema de la resolución óptima del cubo de Rubik de tamaño $N \times N \times N$ en computación cuántica y también discutimos algunas de las aplicaciones del formalismo matemático del mismo en mecánica cuántica.

Índice

1. Introducción

El cubo de Rubik es un rompecabezas de forma cúbica que consta de 26 piezas móviles que pueden permutarse mediante giros de caras. Estas piezas se clasifican en:

- 6 piezas centrales fijas con un color que determina el color de la cara en concreto;
- 12 aristas que constan de dos colores y además de poder permutarse admiten dos posibles orientaciones;
- 8 vértices que constan de tres colores y además de poder permutarse admiten tres posibles orientaciones.

El objetivo de este rompecabezas consiste en mezclarlo mediante giros de caras para posteriormente intentar devolverlo a su posición original, en la cual todas las caras tienen un único color.

Fue ideado en la década de 1970 por un profesor de arquitectura húngaro llamado Ernő Rubik. El primer prototipo data del año 1974 y era de madera y bastante grande, con lo que su funcionalidad era reducida. En realidad al principio Rubik no lo concibió con la idea de resolverlo, sino que lo introdujo con la intención de facilitar su labor docente. Pronto se dio cuenta de que podía devolverlo a la posición original e invirtió un mes en desarrollar un método de resolución. En 1975 obtuvo la primera patente para Hungría bajo el nombre de *cubo mágico*, denominación que seguiría siendo oficial hasta cinco años después, cuando se renombró con el nombre de su creador. En 1977 vio la luz en las jugueterías de Hungría y no fue hasta 1980 cuando se popularizó en el resto del mundo. El *boom* de este rompecabezas se dio en 1981, año en el que se vendieron centenares de millones de copias y se publicaron libros detallando su solución. En 1982 se dio el primer campeonato mundial de resolución del cubo de Rubik, cuyo ganador fue un joven americano de ascendencia vietnamita llamado Minh Thai con una marca de 22,95 segundos.

Desde entonces se han diseñado muchos rompecabezas inspirados en el famoso rompecabezas, como los cubos de tamaños 4×4×4 y 5×5×5 y superiores y con forma de tetraedro (*pyraminx*) y de dodecaedro (*megaminx*) de la mano de diseñadores como Uwe Mèffert. En 2004 se funda la *World Cube Association* (WCA), que desde entonces se encarga de organizar la mayoría de competiciones de resolución del cubo de Rubik a nivel mundial. Estas competiciones no se limitan a resolver estos rompecabezas lo más rápido posible, sino que también hay categorías cuanto menos igualmente interesantes como la resolución a ciegas (*BF, Blindfolded solving*) y en el menor número posible de movimientos (*FMC, Fewest Moves Challenge*). Pero el estudio del cubo de Rubik no se limita al ámbito lúdico: desde muy temprano diversos académicos han intentado desentrañar sus fundamentos matemáticos, centrándose principalmente en su estructura como grupo algebraico y el problema de su resolución óptima: este problema consiste en hallar las cadenas de movimientos que resuelven el cubo en el menor número posible de movimientos. El esfuerzo computacional para tal fin es enorme y por lo tanto abordamos la posibilidad de que este pueda reducirse notablemente con un ordenador cuántico.

Es particularmente valorada la obra de David Singmaster (1979), en la cual introduce una notación para los movimientos del cubo y describe el grupo algebraico subyacente y diversos subgrupos [1]. La notación es la siguiente:

- Un giro de 90° de la cara frontal en el sentido de las agujas del reloj se denota F (*Front*);
- Un giro de 90° de la cara trasera en el sentido de las agujas del reloj se denota B (*Back*);
- Un giro de 90° de la cara izquierda en el sentido de las agujas del reloj se denota L (*Left*);
- Un giro de 90° de la cara derecha en el sentido de las agujas del reloj se denota R (*Right*);
- Un giro de 90° de la cara superior en el sentido de las agujas del reloj se denota U (*Up*);

- Un giro de 90° de la cara inferior en el sentido de las agujas del reloj se denota D (*Down*);
- En caso de que el giro sea en el sentido opuesto a las agujas del reloj, se añade una prima: F'.
- Si el giro es de 180°, se añade un cuadrado o un dos delante: F^2 o F2.

2. El grupo del cubo de Rubik

El conjunto de secuencias de movimientos realizables en el cubo de Rubik $\mathbb{G}$, junto con la operación de composición de secuencias $*$ constituye un grupo algebraico. En efecto, satisface las propiedades de grupo:

i) Existe un elemento identidad e que consiste en no hacer ninguna secuencia y se suele identificar con el cubo en su posición resuelta.

ii) Dadas dos secuencias $A, B \in \mathbb{G}$, que pueden ser simplemente el giro de dos caras, la secuencia $A * B$ también es una secuencia del cubo: $A * B \in \mathbb{G}$.

iii) Como todas las caras pueden girar en ambos sentidos, cualquier secuencia es invertible, pues es una combinación de giros de caras: $\forall\ M \in \mathbb{G},\ \exists M' \in \mathbb{G} : M*M' = M'*M = e$, donde una prima denota una secuencia en sentido inverso.

iv) La propiedad asociativa también se satisface: $\forall\ A, B, C \in \mathbb{G},\ (A*B)*C = A*(B*C)$, que puede deducirse de los giros de caras básicos.

Este grupo es no abeliano: si consideramos una pieza del cubo, su posición final no será la misma si giramos primero la cara de la derecha y luego la superior (RU) que si giramos primero la superior y luego la derecha (UR $\neq$ RU). $\mathbb{G}$ es subgrupo del grupo simétrico S_{48}. La razón es que disponemos de 48 pegatinas que podemos permutar, aunque no todas las permutaciones son posibles. La teoría de representaciones del grupo simétrico tiene aplicaciones en mecánica cuántica, en concreto para el estudio de partículas idénticas. De hecho, todo grupo finito es un subgrupo de un cierto grupo simétrico (teorema de Cayley). También tenemos grupos discretos en cristalografía: las estructuras cristalinas presentan simetrías espaciales periódicas descritas por un cierto grupo y que nos permiten simplificar el problema.

Por definición, $\mathbb{G}$ es un grupo de permutación. La acción de $\mathbb{G}$ sobre un conjunto X es una función $f : \mathbb{G} \times X \mapsto X$ que cumple:

i) $f(e, x) = x, \quad \forall\ x \in X,$

ii) $f(A, f(B, x)) = f(AB, x), \quad \forall\ A, B \in \mathbb{G},\ x \in X.$

Si por ejemplo $X \subset \mathbb{R}^3$ es un conjunto formado por 48 puntos, que podemos identificar con las pegatinas de un cubo, la actuación del grupo de Rubik sería la de permutar los elementos de X de modo que se reordenen formando una posición física del cubo de Rubik dada una cierta secuencia.

El número total de posiciones del cubo es

$$|\mathbb{G}| = \frac{3^7 2^{11} 8! 12!}{2} \approx 4,3 \times 10^{19}. \tag{1}$$

3. *Toy model*: el cubo de tamaño $2\times2\times1$

El cubo de Rubik no trivial y no abeliano más sencillo es el de tamaño $2\times2\times1$ (fig. 1), que consta únicamente de cuatro lados que vuelven al estado original tras rotar un par de veces (estrictamente hablando no es un cubo). Este sistema tiene un total de $3! = 6$ posiciones (pues, obviando la orientación global, podemos dejar un vértice fijo y permutar los tres restantes). Para empezar vamos a ver algunas **representaciones** para este grupo. Una representación de un grupo algebraico consiste en identificar cada elemento con un objeto algebraico que pueda operar sobre un cierto espacio vectorial V:

$$\pi : G \mapsto \pi(G(V)).$$

Entonces $\pi(G(V))x = y,\ x, y \in V$. Por lo general estamos interesados en representaciones matriciales en las que cada elemento es una matriz diferente G de modo que $\forall G_i, G_j \in \mathbb{G},\ \pi(G_i)\pi(G_j) = G_k \in \mathbb{G}$. Primero veamos la representación regular para este grupo. Esta representación es, por así decirlo, la representación canónica para grupos discretos en términos de matrices de dimensión $|\mathbb{G}|$ y está definida para cualquier grupo discreto, si bien por lo general no es irreducible. En la representación regular podemos expresar estas 6 posiciones como matrices 6×6:

$$[D^{\text{reg}}(G_k)]_{ij} = \begin{cases} 1, & G_iG_j = G_k, \\ 0, & \text{en otro caso} \end{cases},$$

$$G_1^{\text{reg}} = \begin{pmatrix} 1&0&0&0&0&0\\ 0&1&0&0&0&0\\ 0&0&1&0&0&0\\ 0&0&0&1&0&0\\ 0&0&0&0&1&0\\ 0&0&0&0&0&1 \end{pmatrix}, \quad G_2^{\text{reg}} = \begin{pmatrix} 0&1&0&0&0&0\\ 1&0&0&0&0&0\\ 0&0&0&0&0&1\\ 1&0&0&0&0&0\\ 0&0&0&1&0&0\\ 1&0&0&0&0&0 \end{pmatrix},$$

$$G_3^{\text{reg}} = \begin{pmatrix} 0&0&1&0&0&0\\ 0&0&0&1&0&0\\ 1&0&0&0&0&0\\ 0&0&1&0&0&0\\ 0&0&0&0&0&1\\ 0&0&0&1&0&0 \end{pmatrix}, \quad G_4^{\text{reg}} = \begin{pmatrix} 0&0&0&1&0&0\\ 0&0&1&0&0&0\\ 0&0&0&0&1&0\\ 0&0&0&0&1&0\\ 0&1&0&0&0&0\\ 0&1&0&0&0&0 \end{pmatrix}, \tag{2}$$

$$G_5^{\text{reg}} = \begin{pmatrix} 0&0&0&0&1&0\\ 0&0&0&0&0&1\\ 0&0&0&1&0&0\\ 0&0&0&0&0&1\\ 1&0&0&0&0&0\\ 0&0&0&0&1&0 \end{pmatrix}, \quad G_6^{\text{reg}} = \begin{pmatrix} 0&0&0&0&0&1\\ 0&0&0&0&1&0\\ 0&1&0&0&0&0\\ 0&1&0&0&0&0\\ 0&0&1&0&0&0\\ 0&0&1&0&0&0 \end{pmatrix}.$$

Por supuesto, esta no es una representación irreducible porque podemos expresar cada elemento como una permutación de sólo 3 objetos, a los que podemos asignar matrices de

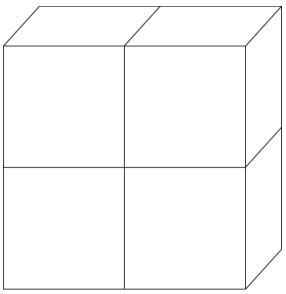

Figura 1: Cubo de Rubik de tamaño 2×2×1. Se denomina así por analogía con el cubo de Rubik tradicional, pues ni es un cubo ni su invención se adjudica a Rubik.

permutación 3×3:

$$
\begin{aligned}
[D^{\text{perm}}(G_k)]_{ij} &= \begin{cases} 1, & \pi_k(i) = j, \\ 0, & \text{en otro caso} \end{cases}, \\
G_1^{\text{perm}} &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad G_2^{\text{perm}} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \\
G_3^{\text{perm}} &= \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \quad G_4^{\text{perm}} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \\
G_5^{\text{perm}} &= \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad G_6^{\text{perm}} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.
\end{aligned}
\tag{3}
$$

Dados los 6 elementos de este grupo y un grupo de generadores $S = \{\mathrm{R}, \mathrm{U}\}$ que en este caso son las dos caras que podemos girar, podemos construir un grafo $\Gamma = (\mathbb{G}, S)$ conexo que conecte cada elemento con sus adyacentes (fig. 2). Este grafo, conocido como **grafo de Cayley**, tiene $V = 6$ vértices y $E = 6$ aristas. Es decir, dos vértices V_i y V_j están conectados por una arista $E(V_i, V_j)$ si $G_i\mathrm{R} = G_j$ o bien $G_i\mathrm{U} = G_j$. También podemos construir la **matrix de adyacencias** dada por los vértices adyacentes:

$$
\mathrm{Ady}(\Gamma)_{ij} = \begin{cases} 1, & \exists\ E(V_i, V_j), \\ 0, & \text{en otro caso} \end{cases}.
$$

Dividiendo por el número de generadores tenemos la siguiente matriz:

$$
M = \frac{1}{2} \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}.
$$

Esta matriz es doblemente estocástica, pues todas las filas y columnas suman 1: esto quiere decir que M define una **matriz de transición de un proceso de Markov** [2]. El proceso

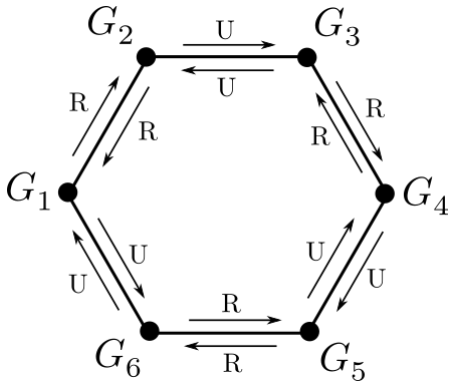

Figura 2: Grafo de Cayley Γ asociado al grupo del cubo $2\times2\times1$.

de Markov consiste en un trayecto aleatorio a través de un sistema discreto sin memoria. En concreto, podemos pensar en un **camino aleatorio** a través del grafo que resulta en una distribución de probabilidad. Si comenzamos por la posición resuelta,

$$p_0 = (1, 0, 0, 0, 0, 0)^t,$$

y tras k pasos:

$$p_k = M^k p_0. \tag{4}$$

p_k nos da la probabilidad de encontrar el cubo en cada posición tras k pasos. Una expresión de la forma (4) también aparece en el estudio de la cromodinámica cuántica a nivel no perturbativo en una red discretizada con el método computacional de cadenas de Markov con Monte Carlo [3, p. 13]. El teorema de Perron-Frobenius asegura que los autovalores de la matriz M satisfacen $|\lambda| \leq 1$ y además el autovalor de mayor valor es $\lambda = 1$ y es no degenerado. Esto nos dice que el sistema es **ergódico** (la probabilidad de pasar de un estado a otro es siempre no nula).

4. El cubo de Rubik $3\times3\times3$

Es en este punto donde las cosas se ponen interesantes. Como ahora el número de elementos es enorme, una representación regular es intratable, pero podemos emplear una representación $8 \otimes 12$ de dimensión 96 que consiste en matrices de permutación para los 8 vértices y las 12 aristas, con la orientación adecuada de ambas. Las aristas admiten dos orientaciones distintas y los vértices tres. Para describirlas, vamos a recurrir al anillo modular $\mathbb{F}_7$, pues, para los vértices multiplicamos por 2 para cada orientación:

$$\begin{aligned} 1 \quad &\text{mód } 7 = 1, \\ 2 \quad &\text{mód } 7 = 2, \\ 4 \quad &\text{mód } 7 = 4, \\ 8 \quad &\text{mód } 7 = 1, \\ &\vdots \end{aligned}$$

y para aristas multiplicamos por 6:

$$\begin{aligned} 1 \mod 7 &= 1, \\ 6 \mod 7 &= 6, \\ 36 \mod 7 &= 1, \\ &\vdots \end{aligned}$$

Además, las posibles orientaciones cumplen unas ciertas restricciones que debemos tener en cuenta: por ejemplo, no podemos tener una única arista desorientada. Veamos un ejemplo interesante: todo elemento de $\mathbb{G}$ constituye un subgrupo cíclico, es decir, que aplicado d veces vuelve a la posición original. Este número d es conocido como el orden del ciclo y el elemento con el orden mayor es $T = \mathrm{RU}^2\mathrm{D}'\mathrm{BD}'$, con orden 1260. En forma matricial:

$$\pi : (3^7 : S_8) \times (2^{11} : S_{12})(\mathbb{F}_7).$$

$$T = \mathrm{RU}^2\mathrm{D}'\mathrm{BD}' = \begin{pmatrix} 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 \\ 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 \end{pmatrix} \otimes \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 6 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 6 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$T^{1260} = \mathbb{1}.$$

Aunque no lo vamos a probar, esta representación es irreducible. El grafo de Cayley correspondiente al cubo de Rubik tiene un total de $V = |\mathbb{G}|$ vértices. Vamos a asignarle como conjunto de generadores el giro de caras permitiendo que un doble giro se considere un único movimiento. A esto se le conoce como HTM (*Half-Turn Metric*):

$$S_{\mathrm{HTM}} = \{\mathrm{L}, \mathrm{L}', \mathrm{L2}, \mathrm{R}, \mathrm{R}', \mathrm{R2}, \mathrm{U}, \mathrm{U}', \mathrm{U2}, \mathrm{D}, \mathrm{D}', \mathrm{D2}, \mathrm{F}, \mathrm{F}', \mathrm{F2}, \mathrm{B}, \mathrm{B}', \mathrm{B2}\}.$$

Tenemos un total de 18 generadores, lo cual quiere decir que de cada vértice salen 18 aristas. Otra opción sería considerar únicamente giros de 90 grados, de modo que un doble giro se considere como dos movimientos (QTM, *Quarter-Turn Metric*):

$$S_{\mathrm{QTM}} = \{\mathrm{L}, \mathrm{L}', \mathrm{R}, \mathrm{R}', \mathrm{U}, \mathrm{U}', \mathrm{D}, \mathrm{D}', \mathrm{F}, \mathrm{F}', \mathrm{B}, \mathrm{B}'\}.$$

Nosotros vamos a considerar únicamente el conjunto HTM. Aunque no podemos representar este grafo tan grande, podemos investigar sus propiedades.

4.1. El número de Dios

Partiendo de un vértice inicial V_1, que vamos a tomar como el estado resuelto, queremos saber cual es la menor distancia entre V_1 y otro vértice dado V_r:

$$\min \ell(V_1, V_r),$$

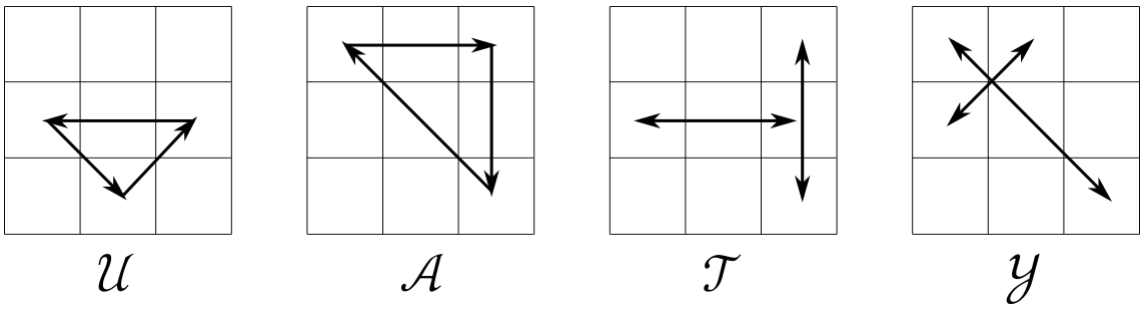

Figura 3: Base de generadores escogida para el subgrupo de PLL.

donde ℓ es el número de aristas que debemos recorrer para llegar a V_r. También nos puede interesar el número D que sería el mayor de estos números:

$$D = \max_r \min \ell(V_1, V_r).$$

Esta cantidad es el **diámetro del grafo de Cayley**. En nuestra terminología, es el *número de Dios del cubo de Rubik*: ¿cuál es el número máximo de movimientos necesario para resolver el cubo de forma óptima desde cualquier posición? Como veremos, este número resulta ser 20. Hay aproximadamente 490.000.000 posiciones que requieren no menos de 20 movimientos para su resolución. Este problema va a ser el punto de partida de nuestra última sección.

4.2. Aplicación: el subgrupo de PLL

El subgrupo de PLL (*Permutation Last Layer*) consiste en las 72 posibles permutaciones de la última cara del grupo. Este número es suficientemente pequeño para un análisis práctico, pero no demasiado pequeño como para que sea trivial. Si tomamos como nuestro conjunto de generadores permutaciones $\mathcal{U}$ que sólo permuta aristas, $\mathcal{A}$ que sólo permuta vértices, $\mathcal{T}$, que intercambia dos aristas y dos vértices formando una T e $\mathcal{Y}$, que intercambia dos aristas y dos vértices formando una Y, $S = \{\mathcal{U}, \mathcal{U}', \mathcal{A}, \mathcal{A}', \mathcal{T}, \mathcal{Y}\}$ (fig. 3), obtenemos el Grafo de Cayley correspondiente. En este caso podemos describir los elementos de este subgrupo como matrices de permutación 8×8 (recordemos que tenemos 4 vértices y 4 aristas y el centro está fijo).

Para este subgrupo, el número de Dios es $D = 6$. Podemos partir de una posición arbitraria y movernos arbitrariamente por el correspondiente gráfico empleando en cada paso uno de los posibles generadores hasta llegar a la identidad, es decir, la posición resuelta, con las siguientes condiciones:

- Todas las posiciones son posibles y equiprobables;
- El sistema no tiene memoria, lo cual quiere decir que en el camino puede volver a pasar por la misma posición más de una vez.

Si computamos este camino aleatorio con $N = 10.000$ intentos, obtenemos una longitud promedio de $\ell = 121$ pasos. Esta longitud es excesiva si la comparamos con el correspondiente número de Dios, pero podemos mejorarla un poco con el *método de Montecarlo*: como para nuestros objetivos no todas las posiciones tienen el mismo interés, sino que

lo que buscamos es que las posiciones más próximas a la identidad sean más probables, vamos a asignarle a cada posición una cantidad, que en analogía con la física vamos a denotar *energía*, que nos da una medida de la probabilidad de saltar a dicha posición. El concepto de energía para el cubo de Rubik no es tan descabellado si pensamos en la energía como relacionada con la entropía, que es una medida de desorden. Entonces, la posición ordenada, la identidad, tendría energía mínima, mientras que la energía máxima se correspondería con las posiciones más distantes. Como trabajamos con matrices, una posible primera opción es definir la energía según la traza de estas matrices: para una cierta posición i con matriz asociada M_i:

$$E_i \stackrel{\text{def}}{=} \text{tr}(\mathbb{1}) - \text{tr}(M_i). \tag{5}$$

Intuitivamente vemos que si hay muchas piezas permutadas, habrá menos unos en la diagonal, de modo que la traza será menor. También definimos la *temperatura* T de este subgrupo como la energía promedio:

$$T \stackrel{\text{def}}{=} \frac{1}{72} \sum_{i=1}^{72} E_i. \tag{6}$$

En nuestro caso $T = 5$. Entonces, la probabilidad que le asignamos a una posición i viene dada por:

$$P_i \stackrel{\text{def}}{=} e^{-E_i/T}. \tag{7}$$

Notemos que, en efecto, esta cantidad está acotada entre 0 y 1. Esta expresión es similar a la que tenemos en física estadística, por ejemplo, para sumar a redes de espines: si el número de espines es muy grande ($\sim 10^{23}$), es imposible sumar a todos ellos, de modo que sólo sumamos a los que tienen más energía para converger lo antes posible al resultado deseado. En nuestro caso, lo que vamos a hacer es lo siguiente:

- En cada paso vamos a tomar una dirección al azar;
- Calculamos la energía de la posición i a la que potencialmente nos vamos a dirigir;
- Lanzamos un número real aleatorio P comprendido entre 0 y 1;
- Si $e^{-E_i/T} > P$, pasamos a dicha posición y añadimos en uno el número de pasos, de lo contrario buscamos otra posición al azar de entre las que están conectadas con la actual.
- Repetimos el proceso hasta resolver el cubo.

Para $N = 10.000$ intentos, obtenemos una longitud media de $\ell_{MC} = 71$ pasos. Sigue siendo bastante, pero supone una clara mejora con el caso anterior en el que teníamos 121 pasos.

- Ejercicio para el lector: esta longitud coincide con el número de posiciones de partida posibles (pues nunca partimos de la identidad): ¿este resultado es casual, o en efecto la longitud promedio coincide con el número de estados de partida?

También podemos calcular la matriz de adyacencias de dimensión 72 y obtener la probabilidad $p_0(k)$ de encontrarnos en la identidad tras un número k de pasos, la cual se representa en la fig. 4

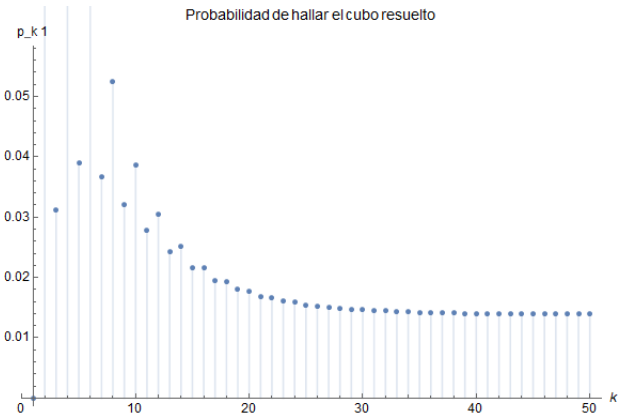

Figura 4: Partiendo del estado resuelto del subgrupo de PLL, probailidad de regresar a esta posición tras k pasos en un camino aleatorio.

4.3. Aplicación: *Lattice QCD*

La cromodinámica cuántica (QCD) como teoría cuántica de campos ha resultado ser un modelo muy exitoso en la descripción de quarks y gluones a altas energías, donde la constante de acoplo es pequeña (libertad asintótica) y por lo tanto la teoría admite un desarrollo perturbativo. No obstante, para el estudio a bajas energías, como el caso de estados ligados de hadrones, la constante de acoplo es arbitrariamente alta y por lo tanto estamos en un régimen no perturbativo. No obstante, podemos recurrir a una técnica alternativa a la teoría de perturbaciones que consiste en aproximar la integral de caminos por un retículo o red discretizada (*lattice*) en el cual en cada nodo el campo tiene un valor determinado [4, cap. 9]. Como vimos, el vector de probabilidades asociadas a cada estado tras k pasos viene dado por

$$p_k = M^k p_0, \tag{8}$$

con M la matriz de adyacencias asociada a este proceso. En el límite de un número infinito de pasos esperamos hallar el equilibrio térmico, es decir [3, p. 14]:

$$p^{(\mathrm{eq})} = \lim_{k\to\infty} M^k p_0, \tag{9}$$

en cuyo caso el proceso de Markov se denomina *estacionario*. La probabilidad $p_j^{(\mathrm{eq})}$ en el equilibrio de cada estado j está relacionada con su energía H_j como

$$p_j^{(\mathrm{eq})} = e^{-\beta H_j}, \tag{10}$$

donde $\beta \overset{\text{def}}{=} (k_B T)^{-1}$ es el factor de Boltzmann. Este puede ser el punto de partida para construir una red discretizada en equilibrio sobre la que sumar para obtener cantidades físicamente medibles, como secciones eficaces, en QCD no perturbativa. Con este método también se recupera el estado experimentalmente observado conocido como *confinamiento*. El primer paso consiste en pasar al espacio euclídeo con una **rotación de Wick** $t \to i\tau$, en cuyo caso en las coordenadas (τ, x, y, z) la métrica es $(1, 1, 1, 1)$. Para las funciones de correlación o funciones de Green a n puntos tendríamos una integral de caminos de la forma:

$$\int \mathcal{D}\Phi \; e^{i\int_0^t L(t')dt'} \longrightarrow \int \mathcal{D}\Phi \; e^{-\int_0^\tau H(\tau')d\tau'}, \tag{11}$$

con H el hamiltoniano. Entonces cada configuración de los campos debe sumarse pesada con un factor energético, expresión que nos recuerda bastante a la física estadística. Esta integral de caminos o integral funcional $\mathcal{D}\Phi$ no está bien definida por lo general y la única manera de obtener información útil de la misma consiste en: o bien desarrollar (11) considerando la interacción como una perturbación, o bien discretizando el espaciotiempo como un retículo en cuatro dimensiones con celdas de lado a:

$$\int \mathcal{D}\Phi \; e^{-\int \mathcal{H}(x) d^4x} \longrightarrow \prod_i \int d\Phi(x_i) \prod_j \exp\left\{-\mathcal{H}\left(\Phi(x_j), \frac{\Phi(x_j + a) - \Phi(x_j)}{a}\right)\right\}.$$

Si tomamos N puntos de integración, tenemos que evaluar un total de N^4 integrales. Por supuesto, podemos recurrir a un método de Montecarlo y evaluar las integrales que más contribuyen a las funciones de correlación hasta converger al resultado esperado. En la práctica, si tomamos una red no muy grande con $N = 32$, tenemos aproximadamente 10^6 integrales y se pueden obtener resultados que coinciden con los medidos experimentalmente con un error no superior a 1 %. Para asegurarnos de que la discretización de la red no afecta cualitativamente a los resultados debemos asegurarnos de que el lado a es mucho más pequeño que la longitud de correlación ξ, es decir, $\xi \gg a$; Esto se consigue si $a \to 0$, pero otra opción más conveniente es estudiar fenómenos críticos para los cuales $\xi \to \infty$.

5. El cubo de Rubik y la computación cuántica

Desde su popularización en los años 80, uno de los problemas más interesantes relativos al cubo de Rubik ha sido el de resolverlo de forma óptima: dada una cierta posición, ¿cuál es el número mínimo de movimientos necesario para resolverlo? hace poco se demostró [5] que el siguiente problema de decisión: *dada una posición del cubo de Rubik de tamaño $N \times N \times N$, ¿una cierta secuencia lo resuelve de manera óptima?* es de tipo NP-completo. También estamos interesados en conocer el número de Dios de un cierto cubo. Para el cubo $3 \times 3 \times 3$ se han obtenido cotas superiores e inferiores mejores con el paso del tiempo, pero para obtener el valor exacto, 20, fue necesario un algoritmo de fuerza bruta: resolver de manera óptima todas las posiciones posibles (salvo simetrías) y dar el valor máximo. Este procedimiento es una secuencia de una gran cantidad de problemas NP-completos que llevó un total de 35 años de computación con un superordenador [6].

Si bien existe la creencia extendida de que un ordenador cuántico puede resolver cualquier problema en un tiempo mucho menor que un ordenador clásico, la realidad es la de que, especialmente si P $\neq$ NP, se espera que el ordenador cuántico sólo sea ligeramente más veloz que uno clásico salvo para la resolución de un escaso número de problemas para los cuales existen algoritmos cuánticos como los de Grover y Shor [7, § 6.4]. En concreto, no se ha demostrado que el problema de la factorización de números enteros sea NP-completo y se cree que no lo es. La idea de esta propuesta es la de estudiar la potencia computacional de un ordenador cuántico a la hora de resolver problemas complejos y ejecutar algoritmos de fuerza bruta: ¿podría obtener el número de Dios en un tiempo razonable, quizás pocas horas, o deberíamos esperar un tiempo de computación de, digamos, 20 años?

5.1. Clases de complejidad

Si estudiamos formalmente un algoritmo para resolver un problema de decisión, su complejidad viene determinada según el rendimiento de una máquina de Turing determi-

nada [7, § 3.2]. Clásicamente tenemos las siguientes clases de complejidad principales:

- P (*Polynomial time*): el conjunto de algoritmos con los cuales una máquina de Turing clásica y determinista puede resolver un problema de decisión en un tiempo polinómico, es decir: si podemos asignar a este algorimo un número natural N que mide cómo escala el problema cuando aumente su complejidad, entonces el tiempo de ejecución o el número de operaciones requeridas está acotado superiormente por $P(N) = a_0 + a_1 N + a_2 N^2 + \cdots$ y se denota $O(P(N))$.
- NP (*Non-deterministic Polynomial time*): el conjunto de algoritmos con los cuales una máquina de Turing clásica pero **no determinista** (es decir, puede realizar de forma paralela y simultánea un número arbitrario de cálculos) puede resolver un problema de decisión en un tiempo polinómico.
- PSPACE (*Polynomial space*): el conjunto de algoritmos con los cuales una máquina de Turing puede resolver un problema de decisión con un número polinómico de bits, sin importar el tiempo de ejecución.
- EXP (*Exponential time*): el conjunto de algoritmos con los cuales una máquina de Turing clásica y determinista puede resolver un problema de decisión en un tiempo exponencial, es decir, acotado superiormente por $O(\exp(N))$.
- PP (*Probabilistic Polynomial time*): es el conjunto de problemas que una máquina de Turing **probabilística** puede resolver en un tiempo polinómico.
- BPP (*Bounded-error Probabilistic Polynomial time*): es el conjunto de problemas que una máquina de Turing probabilística puede resolver en un tiempo polinómico con probabilidad de error acotada por $P = 1/2$.
- ZPP (*Zero-error Probabilistic Polynomial time*): es el conjunto de problemas que una máquina de Turing probabilística puede resolver en un tiempo polinómico con probabilidad de error nula.

Partiendo de estas definiciones podemos concluir que estos conjuntos satisfacen las cadenas de desigualdades

$$\mathrm{P} \subseteq \mathrm{ZPP} \subseteq \mathrm{NP} \subseteq \mathrm{PP} \subseteq \mathrm{PSPACE} \subseteq \mathrm{EXP},$$
$$\mathrm{ZPP} \subseteq \mathrm{BPP} \subseteq \mathrm{PP}.$$

A día de hoy no se sabe si P = NP o bien si P $\subsetneq$ NP y es uno de los mayores problemas abiertos en matemáticas, para cuya resolución se ofrece un millón de dólares. Se dice que un problema es de tipo NP-completo (o de dificultad NP) si es equivalente al problema del *ciclo hamiltoniano* o cualquier otro problema de tipo NP. Como hemos dicho, el problema de la resolución óptima del cubo de Rubik de tamaño $N \times N \times N$ es de este tipo.

Cuando disponemos de una máquina de Turing cuántica tenemos que considerar nuevas clases de complejidad [7, §4.5.5] [8, p. 419] con análogos clásicos:

- P $\longrightarrow$ QP (*Quantum Polynomial time*);
- BPP $\longrightarrow$ BQP (*Bounded-error Quantum Polynomial time*);
- ZPP $\longrightarrow$ ZQP (*Zero-error Quantum Polynomial time*),

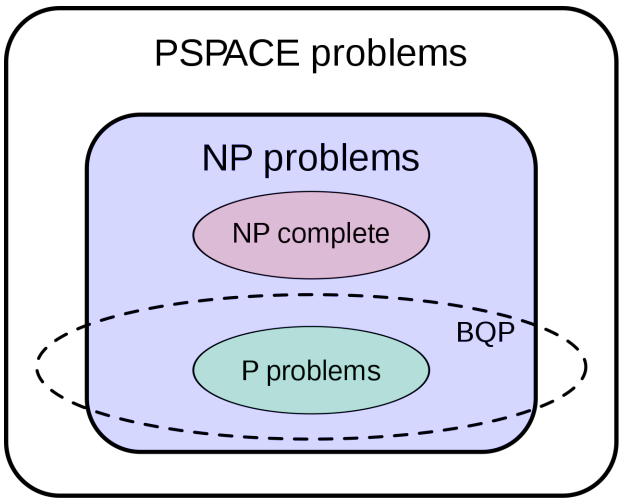

Figura 5: Inclusión de la clase de complejidad cuántica BQP en PSPACE.

con cadenas de desigualdades

$$\mathrm{P} \subsetneq \mathrm{QP},$$
$$\mathrm{BPP} \subseteq \mathrm{BQP} \subseteq \mathrm{PSPACE}.$$

La clase BQP es el conjunto de problemas que un computador cuántico puede resolver de manera mucho más eficiente que uno clásico y su relación con NP y PSPACE es algo difusa (fig. 5).

5.2. El problema de la minimización

Hemos visto que podemos identificar el cubo de Rubik con un grupo que tiene asociado un grafo de Cayley. Entonces, el problema de resolver el cubo desde una posición dada se reduce a minimizar el camino entre un vértice dado del grafo y el vértice inicial. Clásicamente, el mejor algoritmo del que disponemos es el **algoritmo de Dijkstra** (1956), con un rendimiento en el peor de los casos de

$$O(E + V \log V),$$

con E el número de aristas y V el número de vértices del grafo. En nuestro caso $V = |\mathbb{G}|$. Se han propuesto versiones cuánticas de este problema basadas en el algoritmo de Grover y técnicas similares, con complejidad:

- $O\left(\sqrt{VE}\log^2 V\right)$ (Dürr, Heiligmann, Høyer, Mhalla, 2004 [9]);
- $O\left(\sqrt{VE}\log V\right)$ (Furrow, 2006 [10, §5.1]).

Como vemos, estos algoritmos y en especial el segundo suponen una notable mejora con respecto al algoritmo de Dijkstra. No obstante, aún podemos seguir investigando, para lo cual en la próxima sección vamos a ver una posible mejora potencial para la obtención del número de Dios para cubos grandes.

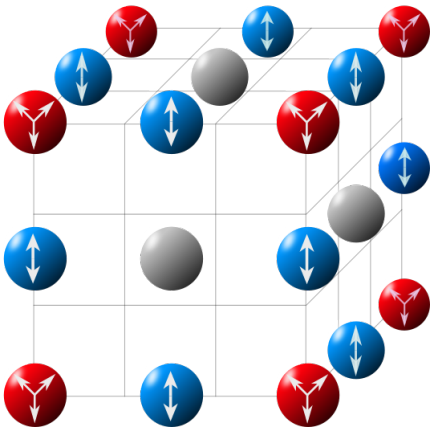

Figura 6: Posible realización del cubo de Rubik cuántico como un sistema de partículas distinguibles de uno, dos y tres niveles.

5.3. El cubo de Rubik cuántico

Ahora estamos interesados en una realización física del cubo de Rubik a nivel cuántico para tratar el problema de la minimización con un algoritmo cuántico. En concreto vamos a promocionar cada una de las permutaciones a un cierto estado cuántico:

$$\begin{aligned} e &\longrightarrow |1\rangle\,, \\ \mathrm{F} &\longrightarrow |2\rangle\,, \\ \mathrm{F}' &\longrightarrow |3\rangle\,, \\ &\vdots \end{aligned}$$

Estos estados serían autoestados de un cierto operador de permutación. Entonces, el estado global vendría dado por

$$|\Psi\rangle = \sum_{j=1}^{|\mathbb{G}|} p_j\,|j\rangle. \tag{12}$$

Estos coeficientes deben elegirse sabiamente para que el estado $|\Psi\rangle$ satisfaga nuestros propósitos. Por ejemplo, si escogemos los coeficientes como el autovector de la matriz de adyacencias dada por (8), el sistema estará en equilibrio; En la práctica no es necesario introducir estos valores manualmente, pues en virtud de (9), sabemos que el sistema va a alcanzar el equilibrio tras un número suficiente de pasos. Notemos que como $|\mathbb{G}|$ es un número muy grande, en la práctica deberíamos aproximar (12) populando el estado con los autoestados más probables, posiblemente por el método de Montecarlo, o reemplazando j por una variable continua α:

$$|\Psi\rangle \longrightarrow \int_0^1 p(\alpha)\,|\alpha\rangle.$$

Una realización concreta de este estado cuántico consistiría en 6 partículas de un único nivel (que serían fijas pero se pueden incluir para garantizar la estabilidad de la estructura), 12 partículas de dos niveles y 8 de tres niveles, sometidas a un cierto potencial que las confine en una región cubica con las restricciones del cubo de Rubik (fig. 6). Estos niveles pueden ser espines que apunten a una cierta dirección z.

- Ejercicio para el lector:

  a) Discutir si esta realización del cubo cuántico es posible. En concreto, la permutación de partículas debe ser siempre par y el espín total en la dirección z debe seguir las restricciones impuestas por las orientaciones posibles de las piezas del cubo: si una partícula cambia de espín, otra debe cambiar en consecuencia. En ese caso las partículas deberían estar entrelazadas, lo cual podría perjudicar el valor computacional de este modelo.

  b) En caso afirmativo, discutir si este estado cuántico puede emplearse para resolver eficientemente con un algoritmo cuántico el problema de la minimización u optimización de la resolución del cubo clásico (posiblemente como un oráculo). ¿Sería de clase BPQ?

Recordemos que en última instancia es obtener el número de Dios para cubos de gran tamaño, por lo que deberíamos poder hacer uso de las coherencias cuánticas para resolver varios cubos simultáneamente y así reducir notablemente el tiempo de ejecución.

Agradecimientos

Quería dar las gracias a todas las personas que me han apoyado y han dedicado parte de su tiempo a revisar e intentar ampliar el presente texto. Especialmente estoy agradecido a Alfredo Luis Aina y a Gerardo García Moreno por organizar los seminarios del Club de óptica cuántica y hacer que esto sea posible.

Lecturas adicionales

- http://birdtracks.eu/courses/PHYS-7143-16/groups.pdf
- https://www.scottaaronson.com/papers/pnp.pdf
- arxiv.org/abs/quant-ph/9912100

Referencias

[1] David Singmaster (1981). *Notes on Rubik's Magic Cube*. New Jersey: Enslow Publishers

[2] D. Bump & D. Auerbach, Unravelling the (miniature) Rubik's Cube through its Cayley Graph

[3] Matsufuru, H., Introduction to lattice QCD Simulations

[4] Francisco J. Ynduráin (2006). *The Theory of Quark and Gluon Interactions*. Springer (4ª edición).

[5] arXiv:1706.06708 [cs.CC]

[6] https://cube20.org/

[7] Nielsen, M., & Chuang, I (2000). *Quantum Computation and Quantum Information*. Cambridge: Cambridge University Press.

[8] A. Galindo, & M. A. Martín-Delgado, Rev. Mod. Phys **74**, 2 (2002)

[9] arXiv:quant-ph/0401091v2

[10] arXiv:quant-ph/0606127v1