Cubo Mágico: uma aplicação da teoria de grupos

Arthur Tonietto Lovato
Orientador: Fagner Bernardini Rodrigues
Universidade Federal do Rio Grande do Sul

Resumo

O cubo de Rubik, também conhecido como cubo mágico, é um quebra-cabeça tridimensional, inventado pelo húngaro Ernő Rubik em 1974. O próprio inventor demorou um mês para resolver o cubo pela primeira vez. O cubo de Rubik tornou-se um ícone da década de 1980. O cubo de Rubik possui várias versões, sendo a 3x3x3 a mais comum, composta por 6 faces de 6 cores diferentes. Outras versões menos conhecidas são a 2x2x2, 4x4x4 e a 5x5x5.
Ao indexar cada elemento do cubo por um número, podemos pensar nos movimentos como uma permutação destes números, e expressá-los como uma matriz de permutação, composta por zeros e uns. É possível mostrar que uma sequência de movimentos é dada pela multiplicação dessas matrizes. O conjunto de todas as sequências de possíveis movimentos forma um grupo não-comutativo finito. Com isso em mente, pretendemos explorar propriedades importantes dos grupos finitos para o grupo gerado pelos movimentos do cubo mágico, como existência de subgrupos de certas ordens (Teorema de sylow) entre outras.

Teoria de Grupos

Dado um conjunto G não vazio, e uma operação $\star : G \times G \to G$. Dizemos que o par G e $\star$ é um grupo se são válidas as três propriedades seguintes:

1. Associatividade;
2. Existencia de um elemento neutro;
3. Existencia de um elemento inverso.

Exemplo 1. Consideramos $\mathbb{Z}$ e a operação de adição usual, temos que $(\mathbb{Z}, +)$ é um grupo abeliano (visto que a operação é comutativa) e infinito.
Exemplo 2. O conjunto $\mathbb{Z}_5$ composto da operação de adição, também forma um grupo abeliano, mas nesse caso o grupo é finito, visto que contém apenas 5 elementos.

Definição 1. Seja $(G, \star)$ um grupo e H um conjunto contido em G. Dizemos que H é um subgrupo de G, se $(H, \star)$ for um grupo. Ou seja, se H, com a mesma operação de G, for um grupo.

Proposição 1. Seja G um grupo e H um subconjunto de G. As seguinte afirmações são equivalentes:

1. H é um subgrupo de G;
2(a) H contém o elemento neutro;
(b) $\forall a, b \in H$, tem-se $ab \in H$;
(c) $\forall a \in H$, tem-se $a^{-1} \in H$;
3. $H \neq \{\}$ e $\forall a, b \in H$, tem-se $ab^{-1} \in H$.

Definição 2. Dados dois grupos $(G, \star)$ e $(H, \circ)$, um homomorfismo de grupos é uma função φ tal que para todo $g, h \in G$, vale:

$$\varphi(g \star h) = \varphi(g) \circ \varphi(h)$$

A aplicação identidade é um homomorfismo. Outro exmplo de homomorfismo pode ser obtido do seguinte modo: para $g \in G$, definimos ψ_g por:

$$\psi_g : G \to G$$

$$x \rightsquigarrow \psi_g(x) = x^g = g^{-1}xg$$

Então temos que ψ_g é um homomorfismo $\forall g \in G$.
Dado um subgrupo H de G, consideramos

$$\psi_g(H) = \{\psi_g(h) : h \in H\} = \{h^g = g^{-1}hg : h \in H\}$$

E denotamos por H^g ou $g^{-1}Hg$. É fácil ver que H^g também é um subgrupo de G.

Definição 3. Dizemos que um subgrupo $H \leq G$ é **normal** em G se $\psi_g(H) = H^g \subseteq H, \forall g \in G$.
Definição 4. Seja G um grupo e N um subgrupo normal em G. Definimos o conjunto quociente por $G/N = \{\bar{g} : g \in G\}$, onde $\bar{g} = Ng = \{ng : n \in N\}$.
Definição 5. Dado um homomorfismo $\varphi : G \to H$, definimos o núcleo do homomorfismo como:

$$\ker(\varphi) = \{g \in G : \varphi(g) = 1_H\}$$

Onde 1_H é a identidade em H.
Proposição 2. Dados dois grupos $(G, \star)$ e $(H, \circ)$, onde $1_G, 1_H$ são as identidades em G e H, respectivamente e $\varphi : G \to H$ um homomorfismo. Então:

1. Im $\varphi = \varphi(G) = \{\varphi(g) : g \in G\}$ é um subgrupo de H;

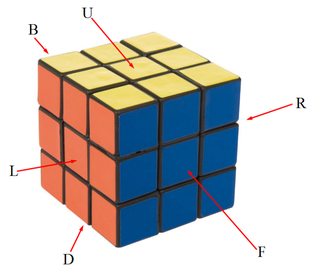
2. $\ker(\varphi) = \{g \in G : \varphi(g) = 1_H\}$ é um subgrupo normal de G e mais,

$$\varphi \text{ é injetiva} \iff \ker(\varphi) = 1_G$$

3. $G/\ker(\varphi) \simeq$ Im φ.

O Cubo

Para começar a análise do cubo, nomeamos cada uma de suas faces.



Dessa maneira, cada movimento no sentido horário recebe o nome da letra da face movimentada. Por exemplo, se movimentarmos a parte superior no sentido horário, estamos realizando o movimento "U". Da mesma maneira, quando fazemos o movimento no sentido anti-horário, estamos realizando o movimento U^{-1}. Além dos movimentos simples de apenas uma das faces, existem as macros, que são sequências de movimentos combinados.
Agora que conhecemos os movimentos do cubo, introduzimos o grupo de Rubik $(\mathcal{R})$, que é gerado pelos 6 movimentos básicos $(\mathcal{R} = (F, B, U, D, L, R))$. Podemos notar que alguns movimentos são comutativos, como os que envolvem duas faces opostas, mas temos muitos outros que não são, o que caracteriza o o cubo mágico como um quebra-cabeça, e, além disso, faz com que tenhamos um grupo não-comutativo.

Visto que existe apenas um número finito de facetas, é possível mostrar que voltaremos para a configuração inicial dada qualquer sequência de movimentos, aplicada um número finito de vezes. Esse número de vezes com que repetimos a sequência é chamado de **ordem**. Por exemplo, se repetirmos o movimento F quatro vezes, iremos voltar à configuração original do cubo, ou seja:

$$F^4 = I$$

Portanto temos que $\mathcal{O}(F) = 4$

Os próximos pensamentos que ocorrem ao estudarmos o cubo mágico são:
- Quais são os movimentos possíveis?
- Quantas combinações são possíveis atingir?
É claro que alguns embaralhamentos serão impossíveis, por exemplo, não há maneira de trocar uma aresta (peça com 2 cores) por um canto (peça com 3 cores), mas alguns outros movimentos não são tão óbvios. Para isso temos que pensar nos movimentos do cubo como permutações de seus elementos, de modo que é possível mostrar que os movimentos do cubo são gerados apenas por permutações pares.
Para calcular o número de arranjos que o cubo pode atingir, podemos pensar na cardinalidade de $\mathcal{R}$. Fazemos a conta de todos os arranjos possíveis, desconsiderando as restrições, e em seguida as aplicamos, chegando ao resultado de quantas combinações o cubo atinge.
Quando embaralhamos o cubo mágico, estamos aplicando uma macro aleatória S. Assim, quando queremos resolver o cubo, após o embaralhamento S, temos que aplicar uma macro T, de modo que:

$$ST = I$$

Tomando como permutações os movimentos dos pequenos cubos que compõem o cubo mágico, vemos que todos os movimentos elementares são permutações pares, portanto qualquer movimento será uma permutação par. Esse fato explica por que não podemos trocar apenas um par de cantos, pois, para isso, precisaríamos de uma permutação ímpar. Assim, é possível estudarmos a cardinalidade de $\mathcal{R}$. Primeiramente, consideraremos que todos os movimentos são possíveis, assim existem 8 posições para cada cubinho de canto e 12 posições para cada cubinho de aresta, ou seja, $8! * 12!$ combinações. Além disso, existem 3 rotações em que cada cubinho de canto pode estar, logo 3^8 possibilidades. Os cubinhos de aresta podem estar girados ou não, o que resulta em mais 2^12 possibilidades. Até aqui temos então $8! * 12! * 3^8 * 2^12$ arranjos. Agora começaremos a considerar as limitações. Apenas $1/3$ terá a orientação correta dos cantos, apenas $1/2$ terá a orientação correta das arestas e somente metade terá a paridade correta. Portanto o tamanho de $\mathcal{R}$ será:

$$\frac{8! * 12! * 3^8 * 2^12}{3 * 2 * 2} = 43252003247489856000$$

Para iniciar o estudo da resolução do cubo utilizando teoria de grupos, veremos agora alguns exemplos de homomorfismos no cubo mágico.
Exemplo 3. $\varphi : \mathbb{Z}_6 \to \mathcal{R}$ definida por $\varphi(\bar{n}) = (FFLL)^n$ é um homomorfismo injetor de grupos. Sua imagem é o subgrupo $\mathcal{H} = \langle F^2L^2 \rangle$, logo $\mathcal{H} \simeq \mathbb{Z}_6$.
Exemplo 4. $\psi : \mathbb{Z}_4 \to \mathcal{R}$ definida por $\psi(k) = U^k$ é um isomorfismo entre $\mathbb{Z}_4$ e o subgrupo $\langle U \rangle \subseteq \mathcal{R}$.

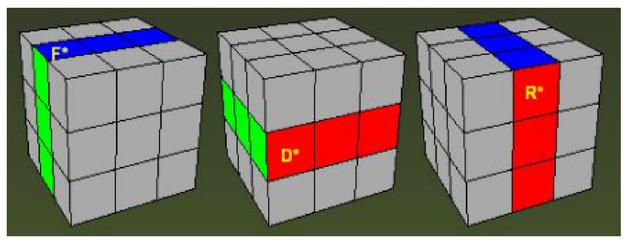
Resolvendo o Cubo com teoria de grupos

Para resolver o cubo utilizando a teoria de grupos devemos definir o subgrupo $\mathcal{F}$ de $\mathcal{R}$. Esse subgrupo é composto por três movimentos: $\langle F^*, D^*, R^* \rangle$, que podemos escrever como:

$$F^* = BF^{-1} = F^{-1}B$$

$$D^* = UD^{-1} = D^{-1}U$$

$$R^* = LR^{-1} = R^{-1}L$$



Agora utilizando um embaralhamento do cubo apenas com elementos de $\mathcal{F}$ é possivel mostrar que através de um homomorfismo $\phi : \mathcal{F} \to S_4 \times \mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_4$ conseguimos resolver o cubo levando os elementos para o núcleo do homomorfismo, que nesse caso corresponde a resolver um sistema linear.
O objetivo desse trabalho é apresentar uma aplicação interessante da teoria de grupos, e não resolver realmente o cubo mágico utilizando essa teoria, por isso não entraremos em detalhes das contas que são feitas nessa etapa.

Referências

[1] "Álgebra Linear - Um Segundo Curso"
Hamilton Prado Bueno
[2] "Introdução à Álgebra"
Adilson Gonçalves