V Bienal da SBM
Sociedade Brasileira de Matemática
UFPB - Universidade Federal da Paraíba
18 a 22 de outubro de 2010

SIMETRIAS, PERMUTAÇÕES E GRUPOS NO CUBO DE RUBIK

KARLA POLYANA SILVA FALCÃO * & WANDERSON ALEKSANDER DA SILVA OLIVEIRA †

1 Gênios e Cubologistas

O que a Arquitetura tem a ver com a Matemática...? Acho que a resposta típica de um estudante de matemática, fosse: "No máximo, estão relacionadas através da geometria!" Pois bem... O arquiteto Húngaro, Ernö Rubik, foi além e ilustrou fantasticamente conceitos puramente algébricos, como a teoria dos grupos, através de um jogo de lógica espacial, que apesar do contraste entre a sua aparência inocente e à dificuldade escondida de sua solução - O Cubo Mágico ou Cubo de Rubik - oferece um sério desafio para todos os fãs de quebra-cabeça, mas especialmente para nós, estudantes de matemática, que estamos profissionalmente preocupados com a dedução lógica.

A aplicação mais interessante da teoria dos grupos é o estudo de simetrias, e na verdade os grupos são a tradução matemática da idéia de simetria. Os grupos de simetria são fundamentais em geometria, em cristalografia e áreas afins. Com grupos podemos entender e resolver O Cubo Mágico : o mais fascinante quebra-cabeça de todos os tempos.

2 No mundo do Cubo Mágico

2.1 Faces, Facetas e cubículos

Nós trabalharemos com o cubo 3x3x3, isto é, ele é constituído de **27 cubículos** de mesmo comprimento de aresta, e cada um tem **seis facetas**.

Um cubículo fica no centro, sendo portanto virtual, e no resto dos cubículos apenas as facetas externas são visíveis. Existem **oito cubículos** que ficam nas pontas e ligam três faces tendo apenas **três facetas** visíveis, portanto definimos como sendo os **cubículos de vértice**. Existem doze cubículos que ficam nas bordas e ligam duas faces tendo apenas duas facetas visíveis, definimos como sendo os **cubículos de aresta**. E por fim, existem seis cubículos que ficam nos meios, entre os cubículos de aresta e os de vértice tendo apenas uma faceta visível, estes são os **cubículos centrais**, dando, portanto um total de **54 facetas**.

Para facilitar a descrição do movimento das faces e dos cubículos introduzimos abreviaturas simples para as seis faces, os doze cubículos de aresta, os oito cubículos de vértice e os seis cubículos centrais do cubo. Então a partir de agora, nós assumimos sempre que tivermos o cubo na nossa frente, tem se uma referência de todos os lados, isto é, de tal forma que a parte da frente, de trás, direita, esquerda, de cima e de baixo poderão ser claramente identificados. Utilizando as demais iniciais minúsculas dos nomes das posições (em inglês, por questão de universalidade!) ficamos com a seguinte notação para as seis faces (ver figura 1) : **f = face frontal (front), b = face de trás (back), l = face esquerda (left), r = face direita (right), u = face de cima (upper), d = face de baixo (down)**.

*Universidade Federal de Pernambuco, UFPE, PE, Brasil, karlatahan@gmail.com.br
†Universidade Federal de Pernambuco, UFPE, PE, Brasil, w.aleksander@bol.com.br

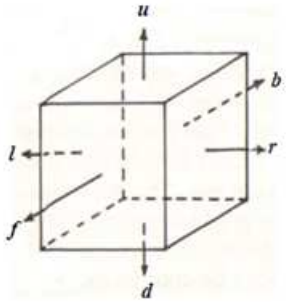
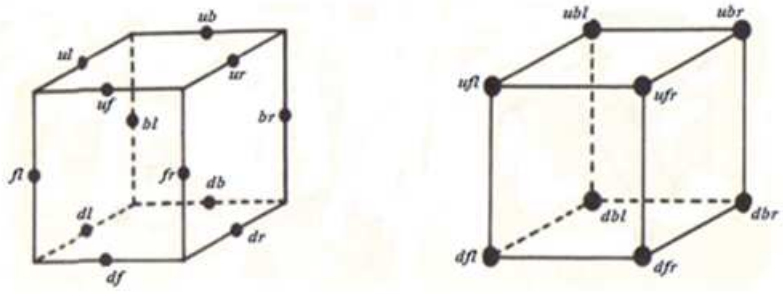


Figura 1: Faces do cubo

Para a notação dos cubículos de aresta e vértice, usamos as iniciais em qualquer ordem das faces que cada cubículo conecta, logo para as arestas temos duas iniciais, e para os vértices temos três. Por exemplo, **ru** (ou **ur**) indica a borda superior direita, **ubr** (ou **bru**, **bur**, etc) indica o canto superior de trás à direita, e **fdl** (ou **dlf**, **lfd**, etc) indica o canto inferior da frente à esquerda", a figura 3 ilustra bem as demais e únicas posições dos cubículos.



2.2 Manipulações no Cubo

A fim de descrever como qualquer posição possível no cubo pode ser devolvida a uma posição inicial, precisamos de uma simples, mas suficiente notação geral para todas as manipulações permitidas no cubo.

As manipulações elementares são os movimentos! *Os* ***movimentos do cubo****, são (um pouco mais tarde eles serão generalizados) os giros de 90° ou 180° de qualquer face do cubo como um corpo rígido em torno do eixo de ligação do centro da mesma face.*

Caracterizar os movimentos por meio de cores parece impraticável, e a razão óbvia seria por causa da diferente coloração dos cubos disponíveis hoje. Em vez disso vamos supor que o cubo está diante de nós, de tal forma como dito antes. Em seguida, *as correspondentes iniciais :* $\boldsymbol{F}$*,* $\boldsymbol{R}$*,* $\boldsymbol{B}$*,* $\boldsymbol{L}$*,* $\boldsymbol{U}$*,* $\boldsymbol{D}$*, denotam o giro de 90° no sentido horário. Se em vez disso o giro de 90° é no sentido contrário (anti-horário) podemos mudar os símbolos para :* $\boldsymbol{F}^{-1}, \boldsymbol{R}^{-1}, \boldsymbol{B}^{-1}, \boldsymbol{L}^{-1}, \boldsymbol{U}^{-1}, \boldsymbol{D}^{-1}$ *também podem ser chamados de movimentos inversos* (ver figura 4). No caso de 180° basta colocar o movimento elevado a dois, o que equivale a fazer o mesmo giro de 90° duas vezes, logo: $\mathbf{F}^2, \mathbf{R}^2, \mathbf{B}^2, \mathbf{L}^2, \mathbf{U}^2, \mathbf{D}^2$. Obviamente que, se for elevado a três será o mesmo que aplicar o inverso, e quatro voltará para a posição inicial a qual chamamos de **I** (identidade). Se seguirmos assim com vários movimentos consecutivos da mesma face, estes podem sempre ser condensados em um movimento simples é conhecido, no caso de F múltiplas vezes cairemos sempre sobre I, F, F^2 ou F^{-1}, isto também se aplica a vários movimentos consecutivos do cubo em torno do mesmo eixo, como por exemplo, $FRR^{-1}D$ tem o mesmo efeito de FD.

Geralmente, é claro, iremos executar toda uma seqüência de movimentos. Tais seqüências são chamadas de **Manobras**, uma manobra pode ser constituída de outras manobras e manobras-movimentos, e é muito importante

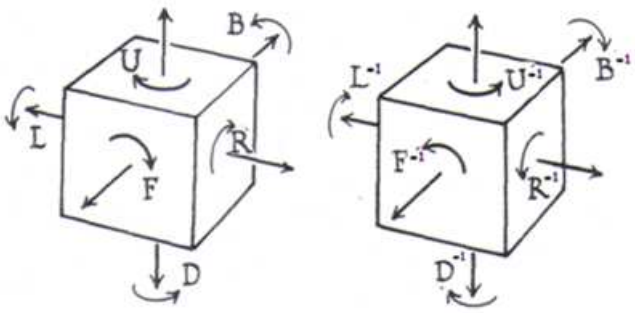


Figura 2: Movimentos

ter isto em mente. Uma manobra é constituída de movimentos escritos sempre da esquerda para a direita na ordem em que eles devem ser realizados. Por exemplo, S = FLU, significa que devemos aplicar F seguido de L e logo depois U. No final de uma manobra estará (entre parênteses) o número de movimentos necessários para efetuá-la, que em geral indica a sua **duração**, assim: S = FLU (3). Mas cuidado, pois a ordem dos movimentos é importante! Por exemplo, o movimento UR, traz o cubículo de aresta **ur** para **uf** e RU traz o mesmo cubículo de aresta **ur** para **br** (verifique!). Esse tipo de fenômeno é descrito como não-comutatividade, isto é, a ordem dos fatores altera o produto.

Da mesma forma que ao girarmos as faces certo número de vezes (no caso quatro), caímos sobre a posição inicial I, acontece analogamente para as manobras, se repetirmos uma manobra certo número de vezes ela cairá sobre o que tínhamos no início, ou seja, a posição I, formando assim um ciclo. Vimos que o menor número de múltiplos movimentos F para se chegar a I foi quatro, portanto denotamos por **Ordem de** F = **O(**F) tal número, assim trivialmente O(R) = O(L) = O(U) = O(D) = O(B) = O(F) = 4. Da mesma forma usaremos para as manobras, podemos verificar que a ordem das manobras S = L^2F^2 e T = LF são respectivamente, O(S) = 6 e a macro O(T) = 105. Mais tarde veremos como calcular ordens de manobras quaisquer.

Outra grande questão "chave"para a resolução do cubo é: Como podemos reverter uma manobra que acaba de ser realizada? Afinal, resolver o cubo mágico não seria como reverter uma operação bagunçada, num cubo que estava ordenado...? Isto certamente não representa qualquer problema para um único movimento: a **manobra inversa** de R é R^{-1}, de R^{-1} é R e R^2 é sua própria inversa, da mesma forma para os outros movimentos. Mas como a manobra RU pode ser revertida? Como reverter uma manobra muito grande? Posso garantir que a manobra inversa para RU não é $R^{-1}U^{-1}$, mas $U^{-1}R^{-1}$! Logo mais poderemos mostrar que em geral : *a manobra inversa* M^{-1} *de uma manobra qualquer M é obtida pela leitura dos movimentos em M de trás para frente, invertendo cada movimento único.* Depois de mais um exemplo simples, $(R^2D^{-1}R^2D)^{-1} = D^{-1}R^2DR^2$ poderemos verificar o entendimento calculando a inversa das manobras abaixo (e verificá-las no cubo).

1. $F^2ULRF^2RLUF^2$ (12) =
2. $R^{-1}DRFD^{-1}U^{-1}FD^{-1}F^{-1}R^{-1}D^{-1}RU$ (14) =
3. $LF^{-1}UL^{-1}FB^{-1}UR^{-1}FU^{-1}RF^{-1}BU^{-1}$ (14) =

Acima de tudo resolver o cubo significa tirá-lo do estado de caos, retornando assim ao estado de ordem pré-estabelecida, geralmente pelas cores. Fazendo uma comparação conveniente, seria como aplicar uma operação definida sobre os elementos de um conjunto, para se obter um determinado resultado, que deverá estar sempre presente neste conjunto. Mas, é importante observar que *nem sempre existirá uma única maneira de tirá-lo do caos*, e ao longo do caminho iremos entender o porquê, e se é possível ter *o mais eficiente dos resultados, que no caso seria a quantidade mínima de movimentos*, por mais caótica e desconhecida que seja a configuração do cubo.

Por quê é possível que um experiente cubologista geralmente só precise de um olhar rápido em uma pequena área do cubo, para a manobra acordar automaticamente de uma parte sonâmbula de sua mente e de repente sentar-se na ponta dos dedos, como uma sonata tocada por um talentoso pianista?

3 Métodos de Resolução

Prático : Decorar e praticar um conjunto de manobras já preparadas para um fim específico!

Matemático : Usando teorias algébricas e combinatórias, calculamos manobras específicas ou aprimoramos outras para resolver o cubo de maneira criativa e autentica, sendo necessários conhecimentos de simbologias e teorias matemáticas. Este será o nosso método, por isso arregace as mangas e equipe-se, pois o nosso cubo não será mais um simples cubo mágico, mas sim, um cubo matemágico!

Algumas perguntas devem ser respondidas por aqueles que pretender aprender o método matemático:

- Quantas e quais as posições que podemos alcançar a partir da posição inicial, girando as faces?
- Como estamos restritos se apenas uma parte de todos os movimentos é permitido?
- Existe alguma operação não trivial para o qual não faz diferença se realizarmos antes ou depois de outra operação?

4 Preparo matemático

4.1 Grupos

Um grupo é constituído de dois ingredientes básicos: um conjunto e uma operação definida neste conjunto. Vamos chamar o conjunto de G *e a operação de* $*$. Por operação estamos entendendo uma regra que a cada dois elementos $a, b \in G$ associa um terceiro elemento $a * b$ que também está em G. Entretanto nem toda associação "conjunto e operação" constitui um grupo. Para termos um grupo é necessário que a operação satisfaça algumas condições.

Um conjunto G onde está definida uma operação $*$ é um grupo se a operação satisfaz as seguintes condições :

(A) Associatividade : $a * (b * c) = (a * b) * c$ *para cada* a,b *e* $c \in G$;

(E) Elemento neutro : *Existe um único elemento* $e \in G$, *tal que para cada* $a \in G$ *então* $a * e = e * a = a$;

(I) Elemento inverso : *Dado um elemento* $a \in G$ *qualquer, existe um único elemento* $a' \in G$ *(o inverso de a) tal que,* $a * a' = a' * a = e$.

A seguinte regra pode ser válida em alguns casos. Com ela temos outro tipo de grupo, o *Grupo Comutativo ou Abeliano* (devido ao matemático norueguês N. H. Abel, 1802-1829):

(C) Comutatividade : $a * b = b * a$ *para todo* $a, b \in G$.

O número de elementos de um grupo G é a sua **ordem**, denotada por $|G|$. Um grupo finito fácil de descrever é $\{-1, 1\}$ com a operação de produto de inteiros, neste caso a ordem é 2 ($|\{-1, 1\}| = 2$) . Veremos exemplos mais concretos de grupos finitos.

Um subconjunto não vazio A de um grupo G, é dito um ***subgrupo*** *de G, se A é um grupo com a operação definida em G. Temos ainda que, qualquer que seja um subgrupo A de G, então ordem de A divide a ordem de G.*

4.2 Permutações

*Uma **permutação** nada mais é, do que o **rearranjo** de um conjunto finito de elementos quaisquer.* Por exemplo, $(b\ a\ c)$ é uma permutação do conjunto $\{a, b, c\}$, (2 1 3) é uma permutação do conjunto $\{1, 2, 3\}$. Ambas as permutações são essencialmente iguais, pois trocam o 1° e o 2° elementos do conjunto. O número de permutações em um dado conjunto é $n!$ (trivial). Mostraremos a maior utilidade de permutações, e principalmente com a notação simplificada.

Se o conjunto a ser permutado é $\{1, 2, ..., n\}$, uma permutação nesse conjunto pode ser descrita por :

$$\begin{pmatrix} 1 & 2 & \dots & n \\ 2 & 1 & \dots & n \end{pmatrix}.$$

Essa matriz dá uma descrição precisa da permutação que troca o primeiro elemento com o segundo, denotamos também, $1 \to 2 \to 1$ ou (1 2), que é a **notação cíclica** de permutações.

Na notação cíclica, os n elementos entre parênteses formam um $n - ciclo$, usualmente o menor elemento tem que começar o ciclo e os elementos que ficam parados (i.e. não permutam) não aparecem. Temos também que toda permutação é escrita de forma única como produto de $k - ciclos$ disjuntos com $k \leq n$.

Por exemplo, considere as permutações:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix},\ \rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 5 & 6 & 4 \end{pmatrix}$$

Podemos representá-las na notação cíclica das seguintes formas: $\sigma = (1\ 3\ 4)$ e $\rho = (1\ 2) \circ (4\ 5\ 6)$

Podemos agora definir: O grupo simétrico S_n é o grupo de todas as permutações do conjunto $\{1, 2, ..., n\}$, com a operação de composição $\circ$, que, no nosso caso, será aplicar a primeira permutação depois aplicar a segunda.

Exemplo: $\mu = (1\ 3\ 4\ 6)$ e $\tau = (1\ 4\ 5\ 3\ 2)$.

Exercício: Calcule $\mu\tau$.

Em S_n é importante notar que (1 2)(1 3) ... (1 n) = (1 2 3 ... n).
Portanto todo $k - ciclo$ disjunto se escreve como produto de $2 - ciclos$ chamados também de **transposições**. Mais ainda, o número total de transposições é ímpar se k for par, e o número de transposições é par se k for ímpar.

Sem dificuldades, mostramos que S_n é grupo.

Agora consideremos $\sigma = (1\ 2)(3\ 4\ 5)$, que consiste de um $2 - ciclo$ e um $3 - ciclo$ sem elementos em comum. Por isso a cada aplicação de σ podemos olhar apenas para (1 2) ou apenas para (3 4 5). Após 2 aplicações, o $2 - ciclo$ (1 2) volta à posição intacta. Isso ocorre para σ^2, σ^4, σ^6, ... E após 3 aplicações, o $3 - ciclo$ (1 2 3) também volta à posição intacta, isso ocorre para σ^3, σ^6, σ^9, ... O que acontece se repetirmos σ três vezes? O $3 - ciclo$ desaparece, mas não o $2 - ciclo$, logo $\sigma^3 = (1\ 2)$. Embora σ mova 5 elementos, σ^3 move apenas 2. Logo, a permutação σ volta a posição intacta após 6 aplicações sucessivas dela mesma.

Portanto, *se uma permutação η consiste de k, l, ..., n−ciclos disjuntos então sua ordem é o $MMC(k, l, \dots, n)$.*Por exemplo: Se η consiste de ciclos de tamanhos 2, 3, 6, 7, então sua ordem é $MMC(2, 3, 6, 7) = 42$.

Dizemos que uma permutação é par se ela se escreve como produto par de transposições, caso contrário, dizemos que ela é ímpar. O conjunto de todas as permutações pares é denotado por A_n, e este forma um grupo por si mesmo, chamado grupo alterno. A metade ímpar não é grupo, pois $1 \in A_n$. Logo A_n é um subgrupo de S_n, e temos que, $|A_n| = n!/2$. Para mais detalhes, veja[1].

4.3 Simetrias

Simetria de uma figura geométrica pode ser descrita como uma "transformação" que, quando aplicada à figura, não altera o seu aspecto visual. Iremos apresentar o mínimo de simetrias de figuras finitas no plano, necessário

para o estudo adiante, a partir da qual, é possível generalizar para o espaço. Para mais detalhes sobre simetrias e demonstrações veja [3].

Vamos descrever as simetrias do quadrado, e logo após, a combinação de todas estas simetrias. É importante observar que o conjunto das simetrias do quadrado o é o subconjunto das simetrias do cubo.

Todas as simetrias do quadrado são descritas através de composições entre:

- o elemento neutro e (não fazer nada);
- uma rotação θ;
- e uma reflexão r qualquer de espelho que divide o quadrado ao meio.

O grupo das simetrias do quadrado é chamado D_4, e é definido formalmente como :

$$D_4 = \langle e, r, \theta \mid \theta^{4-k} r = r\theta^k \ \forall \ 0 \leq k \leq 4 \rangle$$

Pode-se mostrar através dos axiomas dos movimentos rígidos finitos no plano (Teorema de Leonardo Da Vinci) que todas as simetrias do quadrado são:

$$D_4 = \langle e,\ \theta,\ \theta^2,\ \theta^3,\ r,\ \theta r,\ \theta^2 r,\ \theta^3 r \rangle \ e \ dim(D_4) = 8$$

Pela tabela de multiplicação :

$\circ$	e	θ	θ^2	θ^3
e	e	θ	θ^2	θ^3
r	r	θr	$\theta^2 r$	$\theta^3 r$

Podemos também denotar cada transformação no quadrado com a notação de permutações dos vértices :

Rotações: $e = 1$, $\theta = (1\ 2\ 3\ 4)$, $\theta^2 = (1\ 3)(2\ 4)$, $\theta^3 = (1\ 4\ 3\ 2)$.

Reflexões: $r = (2\ 4)$, $\theta r = (1\ 4)(2\ 3)$, $\theta^2 r = (1\ 3)$, $\theta^3 r = (1\ 2)(3\ 4)$.

5 Cubologia

5.1 Permutações e simetrias no cubo

Os movimentos do cubo agora podem ser formalizados como permutações das facetas e de cubículos devido a manobras quaisquer. Eles alteram a configuração das facetas dos cubículos, mas preservam a forma geral do cubo, por isso são chamados simetrias do cubo. Nem todas as configurações são possíveis. Por exemplo, cubículos de aresta não podem ser trocados com os de vértice, etc. Há portanto algumas restrições óbvias nas possíveis configurações. Mais adiante, veremos que há outras menos óbvias. Por exemplo, será que é possível trocar apenas dois cubículos de lugar deixando todo o resto como está ?

O que é "resolver"o Cubo?

Embaralhar o Cubo significa aplicar uma seqüência aleatória de movimentos S a um Cubo resolvido (I).

Resolver o Cubo geralmente significa encontrar alguma seqüência de movimentos T tal que ST = I.

Resolver não é só desembaralhar, pois T não precisa ter os mesmos movimentos de S^{-1}. Por exemplo, se $S = (FLU)^{42}$, então tanto $S^{-1} = (U^{-1}L^{-1}F^{-1})^{42}$ quanto $T = FLU^{-1}L^2U^2L^2UF^{-1}U^2L^{-1}UF^2U^2F^2U^{-1}$ resolvem o

Cubo. Só que S^{-1} tem duração 126, enquanto T tem apenas 22. É interessante notar que TS = ITS = S^{-1}STS = S^{-1}IS = I, portanto S = T^{-1}.

Usaremos uma notação básica para as facetas dos cubículos, desta forma operamos com as suas permutações. Basta, com a notação de antes para os cubículos, colocarmos na frente e em maiúsculo a letra da face que queremos indicar como faceta (de acordo com a nossa referência) e adotaremos a seguinte hierarquia para as posições das outras letras : $f, b \nwarrow u, d \nwarrow l, r$. Por exemplo, o cubículo ruf, tem três facetas indicadas por, Rfu, Ufr e Fur.

Então R, L, F, B, U, D permutam o conjunto das facetas. Logo, o movimento F é análogo aos movimentos das outras faces e faz as seguintes permutações de facetas (ver Rubik):

$$F = (Fur\ Fdr\ Fdl\ Ful)(Fr\ Fd\ Fl\ Fu)(Rfu\ Dfr\ Lfd\ Ufl)(Rfd\ Dfl\ Lfu\ Ufr)(Rf\ Df\ Lf\ Uf)$$

Usando os números 1, 2, ..., 48 ao invés dos nomes das facetas, temos:

$$F = (1234)(5678)(9111315)(10121416)(17181920)$$

As facetas centrais giram em torno de si mesmas, por isso não aparecem nos ciclos.

E se os objetos permutados fossem os cubículos do cubo ? Os cubículos das seis faces sempre permanecerão em seus lugares servindo como um sistema de referência fixa, e uma posição pode facilmente ser descrita pela localização dos cubículos de vértice e de aresta, sem se preocupar com as orientações, denotaremos essas permutações com todas as letras minusculas, e seguindo a hierarquia definida anteriormente.

Um tipo de manobra entre faces adjacentes generaliza bastante todos os possíveis movimentos do cubo. Por exemplo, vamos analisar a manobra S = F^2L^2 que move exatamente 13 cubículos. (ver Rubik!) A manobra S faz:

$$S = (fdfu)(dlul)(flfrbl)(fdlfurbul)(bdlbulfdr)$$

Após executá-la três vezes, são trocados apenas dois pares de cubinhos, pois os elementos presentes nos 3-ciclos tem ordem 3 e voltam à posição inicial. No entanto, os elementos dos 2-ciclos foram permutados um número ímpar de vezes, por isso permanecem trocados. Logo,

$$T = S^3 = (fdfu)(dlul)$$

Curiosamente, como $S^6 = T^2 = I$, logo $T^{-1} = T$ e portanto $(F^2L^2)^3 = (L^2F^2)^3$.

Exercicio : *Descreva quais as permutações dos cubículos que as manobra abaixo causa :*

$$Z = F^2ULRF^2RLUF^2(12)$$

5.2 Lei genérica da cubologia

Uma operação é possível, se e somente se as três seguintes condições são satisfeitas :

1. *O número total de ciclos ou permutações de comprimento par (ciclos de aresta e vértice) é par.*

   Portanto, não existe nenhuma combinação de movimentos que consiga trocar apenas **um número ímpar de pares de cubículos**, pois isso só pode ser conseguido com uma permutação ímpar, ou seja um número ímpar de permutações de comprimento par. Então **sempre um número par de cubículos é permutado**. Vimos que $(F^2L^2)^3$ troca 2 pares de cubículos, e a manobra $F^2ULRF^2RLUF^2$ (12) = (Uf Ul Ur) que troca ciclicamente 3 cubículos (são permutações pares).

2. *O número de giros a direita de ciclos de vértice é igual ao número de giros a esquerda de ciclos de vértice modulo 3.*

   Sempre a rotação total dos oito cubículos de vértice deve ser congruente a zero módulo 360, ou seja três giros de ciclos ou permutações e também por conta da ordem da permutação de cada face.

3. *O número de reorientação dos ciclos de aresta é par.*

   Observemos atentamente a configuração dos cubículos de aresta antes e depois do movimento F: para cada cubículo de aresta, exatamente dois pares de cubículo de aresta são girados. **Sempre exatamente um número par de cubículos é girado**. Portanto não é possível girar um único cubículo de aresta deixando os demais como estão.

5.3 O Grupo de Rubik

O conjunto de todas as possíveis permutações das facetas do cubo forma um grupo $\Re$ chamado Grupo de Rubik.

Ele consiste dos movimentos L, R, F, B, U, D e de todas as manobras S, **assumindo que duas manobras que produzem o mesmo resultado são vistas como iguais**, por exemplo, F e F^5 são os elementos equivalentes do grupo $\Re$. O número total de elementos do grupo $\Re$ é exatamente o número de todas as possíveis configurações do Cubo, isso não significa que $\Re$ deva conter todas as permutações das facetas, mas apenas aquelas que podem ser atingidas por meio dos movimentos acima, portanto $\Re$ é um subgrupo do grupo P de todas as permutações.

O grupo P é composto de

1. S_8 e S_{12}, que são os grupos simétricos bem conhecidos pela gente e equivalem as permutações dos cubículos de vértice e aresta no cubo.

2. Os elementos de $C_3^8 = \{0,1,2\}^8$ e $C_2^{12} = \{0,1\}^{12}$ caracterizados pela orientação dos 8 cubículos de vértice e 12 aresta respectivamente. Se cada 0, 1 e 2 correspondem a três cores adjacentes(e diferentes é claro) nos vértices. E cada 0 e 1 corresponde as cores adjacentes de cada aresta.

Aordem do grupo P é:

$$|P| = |S^8 \cup S^{12} \cup C_3^8 \cup C_2^{12}| = |S^8| \cdot |S^{12}| \cdot |C_3^8| \cdot |C_2^{12}| = 8! \cdot 12! \cdot 3^8 \cdot 2^{12}.$$

Agora, podemos calcular a ordem do grupo $\Re$, a partir da ordem de P e da lei genérica da cubologia :

Sabemos que $\Re$ é um subgrupo de P constituído apenas de permutações pares, logo $\frac{|P|}{2}$; E também pela lei genérica da cubologia, *cada orientação arbitrária de 7 cubículos de vértice, determina uma orientação do oitavo cubículo de vértice, e cada orientação arbitrária de 11 cubículos de aresta, determina uma orientação do décimo segundo cubículo de aresta.* Portanto, o número de possíveis posições no cubo é

$$|\Re| = \frac{1}{(2 \cdot 2 \cdot 3)} \cdot 8! \cdot 12! \cdot 3^8 \cdot 2^{12} = 43.252.003.274.489.856.000.$$

6 Referências

[1] BANDELOW, C. - *Inside Rubik's cube and beyond.*, Editora, Lugar, edição, ano.

[2] COUTINHO, S.C. - *Números Inteiros e Criptografia RSA*, Série de Computação e Matemática - IMPA, 2007.

[3] SCHÜTZER W. - *Aprendendo Álgebra com o Cubo Mágico*, V Semana da Matemática da UFU-FAMAT, 2005.

[4] AUTOR - *Winning Ways*, editora , ano.