Universidade do Estado do Rio de Janeiro
Centro de Tecnologia e Ciências
Instituto de Matemática e Estatística

Jocemar Esteves da Silva Júnior

Teoria de Grupo e o Cubo Mágico

Rio de Janeiro
2016

Jocemar Esteves da Silva Júnior

Teoria de Grupo e o Cubo Mágico

Dissertação apresentada, como requisito parcial para obtenção do título de Mestre, ao Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT, da Universidade do Estado do Rio de Janeiro.

Orientadora: Prof.ª Dra. Patrícia Nunes da Silva

Coorientador: Prof. Dr. Helvécio Rubens Crippa

Rio de Janeiro

2016

CATALOGAÇÃO NA FONTE

UERJ / REDE SIRIUS / BIBLIOTECA CTC-A

S586 Silva Júnior, Jocemar Esteves da.
Teoria de grupo e o cubo mágico/ Jocemar Esteves da Silva Júnior – 2016.
98f. : il.

Orientadora: Patrícia Nunes da Silva
Dissertação (Mestrado Profissional em Matemática em Rede Nacional - PROFMAT) - Universidade do Estado do Rio de Janeiro, Instituto de Matemática e Estatística

1. Cubo mágico - Teses. 2. Teoria dos grupos - Teses. I. Silva, Patrícia Nunes da . II. Universidade do Estado do Rio de Janeiro. Instituto de Matemática e Estatística. III. Título.

CDU 51-8

Autorizo apenas para fins acadêmicos e científicos, a reprodução total ou parcial desta dissertação, desde que citada a fonte.

______________________________ ______________________________
Assinatura Data

Jocemar Esteves da Silva Júnior

Teoria de Grupo e o Cubo Mágico

Dissertação apresentada, como requisito parcial para obtenção do título de Mestre, ao Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT, da Universidade do Estado do Rio de Janeiro.

.

Aprovada em 31 de agosto de 2016.

Banca Examinadora:

Prof.ª Dra. Patrícia Nunes da Silva – Orientadora

Instituto de Matemática e Estatística - UERJ

Prof. Dr. Helvécio Rubens Crippa - Coorientador

Instituto de Matemática e Estatística - UERJ

Prof. Dr. Roberto Alfonso Olivares Jara

Instituto de Matemática e Estatística - UERJ

Prof. Dr. Gladson Octaviano Antunes

Universidade Federal do Estado do Rio de Janeiro

Rio de Janeiro

2016

DEDICATÓRIA

Dedico essa dissertação a todos que pensam, vivem, apreciam, curtem e querem saber sobre Matemática e o Cubo Mágico.

AGRADECIMENTOS

Agradeço a oportunidade de poder contribuir para o ensino da Matemática. Espero que esta dissertação cumpra seu papel de servir como base de estudo para aqueles que percebem a beleza dessa disciplina, a qual rege o universo.

Quero agradecer a Professora Patrícia pela sua dedicação e perseverança em fazer a pessoa acreditar que algo desse porte possa ser feito com segurança e certeza. Com a sua luz as coisas fluem e dão andamento a um bonito trabalho de reconstrução e satisfação.

Agradeço também ao Professor Helvécio pela sua atenção e contribuição.

RESUMO

SILVA JUNIOR, Jocemar Esteves da. *Teoria de Grupo e o Cubo Mágico.* 2016. 98 f. Dissertação (Mestrado em Matemática) - Instituto de Matemática e Estatística, Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2016.

A resolução do Cubo Mágico intriga muitas pessoas até os dias de hoje. Mostraremos como conceitos matemáticos podem nos ajudar a resolver o cubo. Falaremos de Funções e da Teoria dos Grupos e usaremos esses assuntos para embrenharmos no mundo particular do Cubo Mágico com suas partes, nomenclaturas, movimentos e visões. Movimentos básicos serão interpretados como elementos de um grupo. Movimentos mais complexos serão obtidos como combinação desses movimentos através da operação de composição. A prática dos movimentos levará às habilidades necessárias para resolvermos o cubo. Interpretaremos métodos clássicos de resolução a partir da teoria desenvolvida. O cubo é um jogo bastante popular e pode servir como ferramenta de introdução e ensino de conceitos da álgebra abstrata. Detalhamos os resultados apresentados por Chen (2004). Alguns de seus exercícios propostos foram resolvidos e incorporados no corpo do texto. Desse modo, criamos maior unidade e proporcionamos uma leitura mais suave e direta do texto original.

Palavras-chave: Grupos. Cubo Mágico. Método das Camadas.

ABSTRACT

SILVA JUNIOR, Jocemar Esteves da. *Group Theory and the Rubik's Cube*. 2016. 98 f. Dissertação (Mestrado em Matemática) - Instituto de Matemática e Estatística, Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2016.

Solving the Rubik's cube puzzles many people to this day. We show how mathematical concepts can help us to solve the cube. We use Group Theory to enter the private world of the Rubik's cube. Basic moves allow us to make the set of moves of the Rubik's cube into a group. Any move of the Rubik's cube is a combination of the basic moves and inverses of them by means of the group operation. Practicing the moves will lead to the skills needed to solve the cube. We interpret classical methods of resolution from the developed theory. The cube is a very popular game and can serve as a tool for introducing and teaching abstract algebra concepts. We detail the results presented by Chen (2004). Some exercises have been solved and incorporated into the body of the text. In this way, we create greater unity and provide a smoother and more direct reading of the original text.

Keywords: Group Theory. Rubik's cube. Layer Method

LISTA DE ILUSTRAÇÕES

LISTA DE SÍMBOLOS

$\mathbb{Z}$ -	conjunto dos inteiros. . . , -3, -2, -1, 0, 1, 2, 3,. . .
$\mathbb{N}$ -	conjunto dos inteiros positivos 1, 2, 3,. . .
$\mathbb{Q}$ -	conjunto dos números racionais
$\mathbb{R}$ -	conjunto dos números reais
$\mathbb{R}_+$ -	conjunto dos números reais não negativos
$\mathbb{Z}_n$ -	grupo aditivo dos inteiros módulo n , $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$, onde $\bar{x} = \{y \in \mathbb{Z},\ \ y \equiv x \text{ mod}_n\}$.
$\mathbb{Z}_n^\times$ -	grupo de unidades do anel de inteiros módulo n, grupo multiplicativo dos inteiros invertíveis módulo n, $\mathbb{Z}_n^\times = \{\bar{x} \in \mathbb{Z}_n,\ \ \text{mdc}(x, n) = 1\}$.

SUMÁRIO

INTRODUÇÃO

Esta dissertação tem como objetivo traçar um caminho para resolução do Cubo Mágico. Mostraremos como podemos formar conceitos para trabalharmos com o cubo baseando-nos na Teoria dos Grupos. A referência central desse trabalho são as notas *Group Theory and the Rubik's Cube* escritas por Janet Chen (2004) com o objetivo de dar uma introdução à teoria de grupo a partir do Cubo Mágico. Desse modo, é possível permitir que os alunos vejam a álgebra não somente como adição, multiplicação, resolução de equações quadráticas, e assim por diante e oferecer a eles a oportunidade na matemática de encontrar outros objetos, que não números, sendo estudados.

O cerne do nosso trabalho está em trazer perspectivas de resolução do Cubo Mágico e praticá-las para termos habilidades com o manuseio do cubo. Nossos conceitos sobre o cubo serão explicitados com a preocupação de torna-los de fácil compreensão. Não teremos, como muitos esperam, uma equação matemática que possa resolver o cubo, nem uma cartola que possa descobrir a resolução como uma mágica. Trilharemos um caminho baseado em conceitos matemáticos que nos permitirá, a partir de quaisquer posições em que o cubo se encontra, chegarmos a sua configuração inicial, ou seja, com cada uma de suas faces com uma só cor.

Nos seis primeiros capítulos fazemos a tradução e o detalhamento das seis seções iniciais das notas *Group Theory and the Rubik's Cube*. Ao longo desses capítulos, o conjunto de movimentos do cubo é interpretado como um grupo. No sétimo capítulo, utilizamos essa linguagem para discutir as quatro primeiras etapas do Método das Camadas para resolução do Cubo de Mágico. Como contribuição adicional são apresentadas resoluções de alguns dos exercícios propostos no texto original. Foram resolvidos prioritariamente os exercícios citados em demonstrações ou exemplos. Os exercícios resolvidos foram incorporados no texto para manter a continuidade da leitura.

1 FUNÇÕES

Para entender o Cubo Mágico, primeiro precisamos relembrar algumas propriedades de funções.

Definição 1.1. *Uma função ou aplicação f de um domínio D em um intervalo R (representada por $f: D \to R$) é uma relação que atribui a cada elemento $x \in D$ um único elemento $y \in R$. Nós denotamos $f(x) = y$. Dizemos que y é a imagem de x e que x é uma pré-imagem de y. Note que cada elemento em D tem exatamente uma imagem, mas um elemento de R pode ter nenhuma, uma ou mais do que uma pré-imagem.*

Exemplo 1.2. Considere $f: \mathbb{R} \to \mathbb{R}$ dada por $f(x) = x^2$. Se x é um número real qualquer, a sua imagem é o número real x^2. Por outro lado, se y é um número real positivo, há duas pré-imagens, $\sqrt{y}$ e $-\sqrt{y}$. O número real 0 tem uma única pré-imagem, 0; números negativos não têm pré-imagens.

Mais adiante, construiremos exemplos importantes de grupos com funções; nós também usaremos as funções para "traduzirem" informações de um grupo para outro.

Definição 1.3. *Uma função $f: D \to R$ é chamada injetora se $x_1 \neq x_2$ implica $f(x_1) \neq f(x_2)$ para $x_1, x_2 \in D$. Isto é, cada elemento de R tem no máximo uma pré-imagem.*

Exemplo 1.4. Considere a função $f: \mathbb{Z} \to \mathbb{R}$ definida por $f(x) = x + 1$. Esta função é injetora, uma vez que, se $x_1 \neq x_2$, então $x_1 + 1 \neq x_2 + 1$. Se $y \in \mathbb{R}$ é um número inteiro, então ele tem uma única pré-imagem $x = y - 1$. Se $y \in \mathbb{R}$ não é um número inteiro, então ele não tem pré-imagem.

A função $f: \mathbb{Z} \to \mathbb{Z}$ definida por $f(x) = x^2$ não é injetora, uma vez que $f(1) = f(-1)$, mas $1 \neq -1$. Aqui, 1 tem duas pré-imagens, 1 e -1.

Definição 1.5. *Uma função $f: D \to R$ é chamada sobrejetora se, para cada $y \in R$, existe $x \in D$ tal que $f(x) = y$. Equivalentemente, cada elemento de R tem, pelo menos, uma pré-imagem.*

Exemplo 1.6. A função $f: \mathbb{Z} \to \mathbb{R}$ definida por $f(x) = x + 1$ não é sobrejetora, uma vez que, números não inteiros não têm pré-imagens. Por outro lado, a função $f: \mathbb{Z} \to \mathbb{Z}$ definida por $f(x) = x + 1$ é sobrejetora.

A função $f: \mathbb{Z} \to \mathbb{Z}$ definida por $f(x) = x^2$ não é sobrejetora pois não há $x \in \mathbb{Z}$ tal que $f(x) = 2$.

Exemplo 1.7.

(a) Considere função $f: \mathbb{Z} \to \mathbb{Z}$ definida por $f(x) = x^2$. Note que ela não é injetiva, pois temos $f(x) = 4$, para $x = \pm 2$; não é sobrejetora, pois não existe $x \in \mathbb{Z}$ tal que $f(x) = 5$.

(b) Considere a função $f: \mathbb{Z} \to \mathbb{R}$ definida por $f(x) = x + 3$. Ela é injetora, pois para todo número real y pertencente ao conjunto imagem de f, existe um único $x \in \mathbb{Z}$, tal que, $y = f(x)$. Ela não é sobrejetora, pois não existe $x \in \mathbb{Z}$ tal que $f(x) = {}^{1}\!/_{2}$.

(c) Considere a função $f(x): \mathbb{R} \to \mathbb{R}_+$ definida por $f(x) = x^4$. Ela é sobrejetora, pois para todo $y \in \mathbb{R}_+$, existe um $x \in \mathbb{R}$, tal que $y = f(x)$. Ela não é injetora, pois para $x = \pm\sqrt[4]{2}$ temos $f(x) = 2$.

(d) Considere a função $f(x): \mathbb{Z} \to \mathbb{Z}$ definida por $f(x) = x - 1$. Ela é injetora, pois para todo inteiro y pertencente à imagem de f, existe um e somente um $x \in \mathbb{Z}$, tal que $y = f(x)$, a saber $x = y + 1$. Ela é sobrejetora, pois para todo $y \in \mathbb{Z}$, existe um $x \in \mathbb{Z}$, tal que $y = f(x)$.

(e) Considere a função $f: \mathbb{N} \to \mathbb{N}$ definida por $f(x) = x^2 + 1$. A função f não é sobrejetora, pois 4 não pertence à imagem da função, visto que, $x^2 + 1 = 4$ não possui solução em $\mathbb{N}$. É injetiva, pois para $y \in \mathbb{N}$, quando existe $x \in \mathbb{Z}$, tal que $y = f(x)$, ele é único.

(f) Considere a função $f: \mathbb{Z} \to \mathbb{Z}$ definida por $f(x) = 3x + 1$. A função f não é sobrejetora, pois não há $x \in \mathbb{Z}$ tal que $f(x) = 2$. É injetiva, pois para $y \in \mathbb{Z}$, quando existe $x \in \mathbb{Z}$, tal que $y = f(x)$, ele é único.

Definição 1.8. *Uma função $f: D \to R$ é chamada bijetora se ela é injetora e sobrejetora. Equivalentemente, cada elemento de R tem exatamente uma pré-imagem.*

Exemplo 1.9. A função $f\colon \mathbb{Z} \to \mathbb{Z}$ definida por $f(x) = x + 1$ é uma bijeção.

Exemplo 1.10.

(a) Se S é um conjunto qualquer, então podemos definir uma função $f\colon S \to S$ por $f(x) = x$, para todos $x \in S$. Esta função é chamada de identidade e é uma bijeção.

(b) Considere a função $f\colon \mathbb{R} \to \mathbb{R}$ definida por $f(x) = 3x + 1$. A função f é bijetora, pois para $y \in \mathbb{R}$, existe um único $x \in \mathbb{R}$, tal que $y = f(x)$. Lembrando que para f ser bijetora, ela deve ser injetora e sobrejetora.

Definição 1.11. *Se $f\colon S_1 \to S_2$ e $g\colon S_2 \to S_3$, então podemos definir uma nova função $f \circ g\colon S_1 \to S_3$ por $(f \circ g)(x) = g(f(x))$. A operação é chamada de composição.*

Observação 1.12. Usualmente, escrevemos $(f \circ g)(x)$ para representar $f\big(g(x)\big)$ ao invés de $g\big(f(x)\big)$. No entanto, será mais conveniente aqui convencionarmos $(f \circ g)(x) = g(f(x))$. Nós estamos usando esta convenção porque corresponde à convenção normalmente utilizada para o Cubo Mágico.

Proposição 1.13. *Suponha $f_1\colon S_1 \to S_2$ e $f_2\colon S_2 \to S_3$ são injetivas. Então $f_1 \circ f_2$ é injetiva.*

Prova. Observe que $f_1 \circ f_2 : S_1 \to S_3$. Para provar que $f_1 \circ f_2$ é injetiva, basta tomarmos dois elementos distintos de seu domínio e mostrarmos que suas imagens pela $f_1 \circ f_2$ também são distintas. Sendo $x_1 \neq x_2 \in S_1$ e f_1 injetiva, temos $f_1(x_1) \neq f_1(x_2)$. Como $f_1(x_1) \neq f_1(x_2) \in S_2$ e f_2 é injetiva, temos $f_2(f_1(x_1)) \neq f_2(f_1(x_2))$. Logo, se $x_1 \neq x_2 \in S_1$, então $(f_1 \circ f_2)(x_1) \neq (f_1 \circ f_2)(x_2)$.

Observe que na Proposição 1.13, provamos que a composição de duas funções injetivas ainda é injetiva. Isto é, a operação de composição preserva a injetividade.

Proposição 1.14. *Suponha $f_1\colon S_1 \to S_2$ e $f_2\colon S_2 \to S_3$ são sobrejetoras. Então $f_1 \circ f_2$ é sobrejetora.*

Prova. Observe que $f_1 \circ f_2 : S_1 \to S_3$. Para provar que $f_1 \circ f_2$ é sobrejetora, basta tomarmos $y \in S_3$ e provar que existe $x \in S_1$ tal que $y = f_2(f_1(x))$. Dado $y \in S_3$, como f_2 é sobrejetora, existe $w \in S_2$, tal que $y = f_2(w)$. Do mesmo modo, como f_1 é sobrejetora, existe $x \in S_1$, tal que $w = f_1(x)$. Logo, para todo $y \in S_3$, existe um $x \in S_1$, tal que $y = f_2(f_1(x))$.

Proposição 1.15. *Sejam* $f_1: S_1 \to S_2$, $f_2: S_2 \to S_3$ *e* $f_3: S_3 \to S_4$. *Então* $f_1 \circ (f_2 \circ f_3) = (f_1 \circ f_2) \circ f_3$.

Prova. Note que $f_1 \circ (f_2 \circ f_3): S_1 \to S_4$ e $(f_1 \circ f_2) \circ f_3: S_1 \to S_4$. Seja $x \in S_1$. Como $(f_2 \circ f_3)(y) = f_3(f_2(y))$, temos

$$\big(f_1 \circ (f_2 \circ f_3)\big)(x) = (f_2 \circ f_3)\big(f_1(x)\big) = f_3\left(f_2\big(f_1(x)\big)\right).$$

Por outro lado, como $(f_1 \circ f_2)(z) = f_2(f_1(z))$, temos

$$\big((f_1 \circ f_2) \circ f_3\big)(x) = f_3\big((f_1 \circ f_2)(x)\big) = f_3\left(f_2\big(f_1(x)\big)\right).$$

Isto é as funções $f_1 \circ (f_2 \circ f_3)$ e $(f_1 \circ f_2) \circ f_3$ coincidem para todo elemento de S_1. Portanto, são iguais.

2 GRUPOS

Para se ter uma ideia melhor sobre grupos, vamos começar por dois conjuntos familiares. Para os conceitos e resultados da Teoria de Grupo, foram utilizadas, além de Chen (2004), as referências Simis (1977) e Martinez et al. (2013).

Exemplo 2.1. Primeiro, considere os números inteiros módulo 4. Lembre-se que $\mathbb{Z}_4$ é um conjunto com 4 elementos: 0, 1, 2 e 3. Uma das primeiras coisas que você aprendeu na aritmética modular foi como adicionar números módulo n. Vamos escrever uma tabela de adição para $\mathbb{Z}_4$.

Quadro 1 – Adição em $\mathbb{Z}_4$

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Fonte: CHEN, 2004

Agora, vamos reescrever a tabela de adição de uma forma que pode parecer bastante inútil; nós, apenas, usaremos o símbolo $*$ ao invés de $+$ para adição, e escreveremos $e = 0$, $a = 1$, $b = 2$ e $c = 3$. Então, a nossa tabela de adição reescrita resulta em

Quadro 2 – Adição em $\mathbb{Z}_4$

$*$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

Fonte: CHEN, 2004

Vamos fazer a mesma coisa para $\mathbb{Z}_5^\times$, o conjunto de unidades módulo 5. As unidades módulo 5 são 1, 2, 3 e 4. Se você adicionar duas unidades, você não necessariamente obtém outra unidade; por exemplo, 1 + 4 = 0, e 0 não é uma unidade. No entanto, se você multiplicar duas unidades, você sempre obterá uma unidade. Assim, podemos escrever uma tabela de multiplicação para $\mathbb{Z}_5^\times$. Aqui está:

Quadro 3 – Multiplicação em $\mathbb{Z}_5^\times$

	1	2	4	3
1	1	2	4	3
2	2	4	3	1
4	4	3	1	2
3	3	1	2	4

Fonte: CHEN, 2004

Novamente, vamos reescrevê-la usando novos símbolos. Denote por $*$ a operação de multiplicação e considere $e = 1$, $a = 2$, $b = 4$ e $c = 3$. Então, a tabela de multiplicação para $\mathbb{Z}_5^\times$ pode ser reescrita como

Quadro 4 – Multiplicação em $\mathbb{Z}_5^\times$

$*$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

Fonte: CHEN, 2004

Observe que esta é exatamente a mesma tabela para adição em $\mathbb{Z}_4$!

O que aprendemos com o fato de termos as mesmas tabelas nestas duas situações tão diferentes? Bem, isso nos permite traduzir as sentenças algébricas sobre adição de elementos de $\mathbb{Z}_4$ em sentenças sobre a multiplicação de elementos de $\mathbb{Z}_5^\times$. Por exemplo, a equação $x + x = 0$ em $\mathbb{Z}_4$ tem duas soluções, $x = 0$ e $x = 2$. Com a nossa notação alternativa, isto é o mesmo que dizer que a equação $x * x = e$ tem as soluções $x = e$ ou $x = b$. Se traduzirmos isso para $\mathbb{Z}_5^\times$, vemos que as soluções de $x \cdot x = 1$, em $\mathbb{Z}_5^\times$, são $x = 1$ ou $x = 4$. Isto é, 1 e 4 são as raízes quadradas de 1 em $\mathbb{Z}_5^\times$, que é exatamente o que acontece!

Em linguagem matemática, dizemos que $\mathbb{Z}_4$ com a adição e $\mathbb{Z}_5^\times$ com a multiplicação são “grupos isomórficos”. Em linhas gerais, apalavra “isomórfico” significa que eles têm a mesma estrutura algébrica. Por ora, vejamos o que é um “grupo”.

Definição 2.2. *Um grupo $(G,*)$ é constituído por um conjunto G e uma operação $*$ que satisfazem às condições:*

1. *G é fechado sob $*$. Isto é, se $a, b \in G$, então, $a * b \in G$.*
2. *A operação $*$ é associativa. Isto é, para quaisquer $a, b, c \in G$,*
$$a * (b * c) = (a * b) * c$$
3. *Existe um elemento $e \in G$ tal que $g = e * g = g * e$ para todo $g \in G$. (o elemento e é chamado de identidade ou elemento neutro)*
4. *Para todo $g \in G$, existe um elemento $h \in G$, tal que $g * h = h * g = e$. (h é chamado de inverso de g).*

Exemplo 2.3.

(a) $\mathbb{Z}_4$ é fechado sob a adição; afinal de contas, nós exibimos toda a tabela de adição, que nos diz como adicionar quaisquer dois elementos de $\mathbb{Z}_4$ e obter outro elemento de $\mathbb{Z}_4$. Analogamente, $\mathbb{Z}_5^\times$ é fechado sob a multiplicação.

(b) $\mathbb{Z}$ é fechado sob a adição: se $a, b \in \mathbb{Z}$, então $a + b \in \mathbb{Z}$. Da mesma forma, $\mathbb{Z}$ também é fechado sob a subtração.

(c) $\mathbb{R}$ é fechado sob multiplicação: se multiplicarmos dois números reais, obtemos um número real.

(d) O conjunto de números negativos não é fechado sob a multiplicação: se multiplicarmos dois números negativos, temos um número positivo.

(e) Adição e multiplicação são associativas. Subtração não é associativa porque $a - (b - c) \neq (a - b) - c$.

(f) Em $(\mathbb{Z}_4, +)$, 0 é um elemento identidade porque $g = 0 + g = g + 0$ para qualquer $g \in \mathbb{Z}_4$. Em $(\mathbb{Z}_5^\times, \cdot)$, 1 é um elemento identidade, porque $g = 1 \cdot g = g \cdot 1$ para qualquer $g \in \mathbb{Z}_5^\times$.

(g) Em $(\mathbb{Z}, +)$, 0 é um elemento identidade, porque $g = 0 + g = g + 0$ para qualquer $g \in \mathbb{Z}$.

(h) Em $(\mathbb{R}, \cdot)$, 1 é um elemento identidade, porque $g = 1 \cdot g = g \cdot 1$ para qualquer $g \in \mathbb{R}$.

(i) Usando a tabela de adição para $\mathbb{Z}_4$, podemos encontrar inversos de todos os elementos de $\mathbb{Z}_4$. Por exemplo, podemos ver na tabela que $1 + 3 = 3 + 1 = 0$, então 3 é um inverso de 1. De modo análogo, uma vez que a tabela para $\mathbb{Z}_5^\times$ é idêntica, todos os elementos de $\mathbb{Z}_5^\times$ têm inversos.

(j) Em $(\mathbb{Z}, +)$, um inverso de $n \in \mathbb{Z}$ é $-n$ porque $n + (-n) = (-n) + n = 0$.

(k) Em $(\mathbb{R}, \cdot)$, nem todo elemento tem um inverso, por exemplo, 0 não tem um inverso. No entanto, se $x \neq 0$, então $\frac{1}{x}$ é um inverso de x porque $x \cdot \frac{1}{x} = \frac{1}{x} \cdot x = 1$.

Exemplo 2.4.

(a) $(\mathbb{Z}_4, +)$ e $(\mathbb{Z}_5^\times, \cdot)$ são grupos. Na verdade, como dissemos anteriormente, estes podem ser vistos como o “mesmo” grupo.

(b) $(\mathbb{Z},+)$ é um grupo. No entanto, $(\mathbb{Z},-)$ não é um grupo, porque subtração não é associativa.

(c) $(\mathbb{R},\ \cdot)$ não é um grupo, uma vez que, 0 não tem um inverso sob a multiplicação. No entanto, $(\mathbb{R}-\{0\},\cdot)$ é um grupo.

(d) O conjunto de números negativos não é fechado sob multiplicação, então, o conjunto de números negativos com a multiplicação não é um grupo.

(e) Podemos construir um grupo $(G,*)$, onde G é um conjunto com apenas um elemento. Como G deve possuir um elemento identidade, chamaremos este único elemento de e. Para definir a operação $*$ do grupo, só precisamos definir o que é $e*e$. Há apenas uma escolha, já que G tem apenas um elemento: $e\ *\ e$ deve ser e. Isto define um grupo que é chamado *grupo trivial*. Como você pode imaginar, o grupo trivial não é muito interessante.

(f) Em $(\{\pm\ 1\},\ \cdot)$, temos as seguintes multiplicações possíveis entre dois elementos nesse conjunto: $1\cdot 1=1$, $1\cdot(-1)=-1$, $(-1)\cdot(-1)=1$ e $(-1)\cdot 1=-1$. Todas elas resultam em 1 ou -1, que estão no conjunto. Isto é, se operarmos os elementos do conjunto, teremos elementos do próprio conjunto. Logo ele é fechado;

Vamos verificar a associatividade. Como sabemos que todas as multiplicações citadas acima dão 1 ou -1 e esgotam as possibilidades de pares multiplicativos dos elementos do conjunto, podemos dizer que as associações feitas darão 1 ou -1. Observe que

- $-1\cdot[(-1)\cdot(-1)]=-1=[(-1)\cdot(-1)]\cdot(-1)$
- $1\cdot[(-1)\cdot(-1)]=1=[1\cdot(-1)]\cdot(-1)$
- $-1\cdot[1\cdot(-1)]=1=(-1\cdot 1)\cdot(-1)$
- $-1\cdot(-1\cdot 1)=1=[(-1)\cdot(-1)]\cdot 1$
- $1\cdot(1\cdot 1)=1=(\ 1\cdot 1)\cdot 1$
- $-1\cdot(1\cdot 1)=-1=(-1\cdot 1)\cdot 1$
- $[1\cdot(-1)]\cdot 1=-1=1\cdot(-1\cdot 1)$
- $1\cdot[1\cdot(-1)]=-1=(1\cdot 1)\cdot(-1)$

Logo a associatividade se verifica;

Seja $e=1$. Note que quando e é multiplicado por qualquer elemento do conjunto, não o altera:

$1\cdot e=1$ e $(-1)\cdot e=-1$. Logo, $e=1$ é o elemento identidade;

Note que se $a\in\{\pm\ 1\}$, então $a\cdot a=1=e$. Logo, cada elemento de $\{\pm\ 1\}$ é seu próprio inverso. Logo, $(\{\pm\ 1\},\ \cdot)$ é um grupo.

(g) Seja $(S, +)$, onde S é o conjunto dos inteiros não negativos $\{0, 1, 2, 3, \dots\}$. É fácil ver, que se $(S, +)$ fosse um grupo, 0 seria o elemento neutro. Não há inversos para todos os elementos de S, por exemplo, não existe $d \in S$ tal que $1 + d = 0$, pois a única solução seria $d = -1$ que não pertence a S. Vemos, nesse caso, $(S, +)$ não é um grupo.

(h) Considere $(2\mathbb{Z}, +)$, onde $2\mathbb{Z}$ é o conjunto dos inteiros pares. Inicialmente, observe que um inteiro é par se, e somente se, pode ser escrito como $2a$, para algum $a \in \mathbb{Z}$. Agora, veremos se a soma de pares é par:

$2a + 2a = 4a = 2 \cdot 2 \cdot a = 2 \cdot (2a)$. De fato, a soma dos elementos do conjunto dará um par. Logo, o conjunto é fechado para a soma.

Vejamos se a associatividade vale para o conjunto:

$2a + (2b + 2c) = 2 \cdot (a + b + c) = (2a + 2b) + 2c$. Verificamos que sim.

Buscaremos o elemento neutro:

$2a + e = 2a$. Como a operação é a soma, o elemento neutro é o 0. Sendo o 0 um inteiro e par $(0 = 2 \cdot 0)$, temos $e = 0$ no conjunto.

Encontraremos, agora, os inversos dos elementos do conjunto.

Dado o inteiro par $2a$, queremos determinar um inteiro par d, tal que $2a + d = e$. Como $e = 0$, temos $2a + d = 0$, que implica $d = -2a = 2 \cdot (-a)$. Assim, temos os inversos de cada elemento do conjunto. Portanto, $(2\mathbb{Z}, +)$ é um grupo.

Em breve, veremos como considerar os movimentos de um Cubo Mágico como elementos de um grupo!

Muitos dos exemplos de grupos que vimos até agora têm uma propriedade especial: para cada $g, h \in G$, $g * h = h * g$; isto é, $*$ é uma operação comutativa. Isso não é verdade para todos os grupos. Sempre que é verdade para um grupo $(G,*)$, dizemos que $(G,*)$ é *abeliano*. Logo veremos exemplos de grupos não abelianos.

Agora, provaremos duas propriedades importantes de grupos.

Lema 2.4. *Um grupo tem exatamente um elemento identidade.*

Prova. Seja $(G,*)$ um grupo, e suponha que e e e' são elementos identidade de G (sabemos que G tem, pelo menos, um elemento de identidade pela definição de grupo). Então, $e * e' = e$ uma vez que e' é um elemento identidade. Por outro lado, $e * e' = e'$, já que e é um elemento identidade. Portanto, $e = e'$.

Lema 2.5. *Se $(G,*)$ é um grupo, então, cada $g \in G$ tem exatamente um inverso.*

Prova. Seja $g \in G$. Como G é um grupo, sabemos que existe um inverso de g. Suponha que g_1 e g_2 são inversos de g. Logo, $g_1 * g = e$ e $g * g_2 = e$. Por associatividade, $(g_1 * g) * g_2 = g_1 * (g * g_2)$. Uma vez que, g_1 é um inverso de g, $(g_1 * g) * g_2 = e * g_2 = g_2$. Da mesma forma, g_2 é um inverso de g, $g_1 * (g * g_2) = g_1 * e = g_1$. Portanto, $g_2 = g_1$.

Em geral, escrevemos o único inverso de g como g^{-1}. No entanto, se sabemos que a operação do grupo é a adição, então escrevemos o inverso de g como $-g$.

Exemplo 2.6. Seja $(G, \circ)$, onde G é o conjunto das bijeções de algum conjunto S sobre si mesmo e $\circ$ denota a composição de funções. Queremos verificar que $(G, \circ)$ é um grupo. Se g e h pertencem a G, a composição $g \circ h$ está bem definida. Vimos nas Proposições 1.13 e 1.14 que a composição preserva a injetividade e a sobrejetividade. Portanto, G é fechado sob a operação de composição.

Vejamos a associatividade. Sendo $g, h, f \in G$, temos:

$[g \circ (h \circ f)](x) = (h \circ \text{f})\big(g(x)\big) = f[h\big(g(x)\big)]$, primeiro caso.

$[(g \circ h) \circ f](x) = f((g \circ h)(x)) = f[h(g(x)\ )]$, segundo caso.

Reparamos que os dois casos são iguais, logo há a associatividade no conjunto.

Para encontrarmos o elemento neutro, imaginemos uma função que nada faz com o elemento do domínio. Isto é, considere $e: S \to S$ dada por $e(x) = x$. Então, dada $f \in G$, temos $(f \circ e)(x) = f(x) = (e \circ f)(x)$. Logo a função e é o elemento neutro.

Os inversos no conjunto são as funções inversas: $f \circ f^{-1} = e = f^{-1} \circ f$. Logo há inversos para todos os elementos de G. Concluímos que $(G, \circ)$ é um grupo.

Exemplo 2.7. Sejam G um grupo e $g, h \in G$. Podemos usar o Lema 2.5 para escrever $(gh)^{-1}$ em termos de g^{-1} e h^{-1}. Sabemos que o inverso é único e $(gh)^{-1}$ é o inverso de gh. Note que $(gh)(h^{-1}g^{-1}) = g(hh^{-1})g^{-1} = gg^{-1} = e$. Logo, $(gh)^{-1} = h^{-1}g^{-1}$.

Lema 2.8. *Seja $(G,*)$ um grupo e $a, b, c \in G$. Então*

a) Se $a * b = a * c$, então, $b = c$.

b) Se $b * a = c * a$, então, $b = c$.

Prova.

a) Considere o inverso a^{-1} de a. Pela associativa temos

$$b = (a^{-1} * a) * b = a^{-1} * (a * b) = a^{-1} * (a * c) = (a^{-1} * a) * c = c$$

b) Considere o inverso a^{-1} de a. Pela associativa temos

$$b = b * (a * a^{-1}) = (b * a) * a^{-1} = (c * a) * a^{-1} = c * (a * a^{-1}) = c$$

O Lema 2.8 nos mostra que podemos cancelar em grupos.

Lema 2.9. *Se $(G,*)$ é um grupo e $g \in G$, então $(g^{-1})^{-1} = g$.*

Prova. Temos $(g^{-1})^{-1} * g^{-1} = e = g * g^{-1}$. Pelo Lema 2.8, $(g^{-1})^{-1} = g$.

Lema 2.10. *Se $(G,*)$ é um grupo e $g, h \in G$ são tais que, $g * h = e$, então $h * g = e$.*

Prova. Partindo de $g * h = e$, pela associatividade, temos:

$$g^{-1} * \big(g * (h * g)\big) = g^{-1} * \big((g * h) * g\big) = g^{-1} * (e * g) = e$$

Por outro lado,

$$g^{-1} * \big(g * (h * g)\big) = (g^{-1} * g) * (h * g) = h * g$$

Logo, $h * g = e$.

Lema 2.11. *Se $(G,*)$ é um grupo e $g, h \in G$ são tais que, $g * h = e$, então h* é *o inverso de g e g é o inverso de h.*

Prova. Consequência direta dos Lemas 2.5 e 2.10.

Lema 2.12. *Se $(G,*)$ é um grupo e $g, h \in G$ tais que $g * h = h$, então g é o elemento de identidade de G.*

Se $g * h = h$, temos $g * h = e * h$. Pelo Lema 2.8, $g = e$.

Se $(G,*)$ é um grupo e G tem um número finito de elementos, dizemos que G é finito. Denotamos por g^n o produto $g * g * \cdots * g$ com n cópias de g.

Lema 2.13. *Seja $(G,*)$ um grupo finito. Então existe um número inteiro positivo n tal que $g^n = e$.*

Prova. Se $g = e$, então $g^n = e$ com $n = 1$. Com $g \neq e$:

Suponha que G tenha m elementos. Considere os $m + 1$ elementos de G:

$$g, g^2, \dots, g^{m+1}.$$

Pelo princípio da casa dos pombos, existem $1 \leq k < r \leq m + 1$, tais que

$g^k = g^r = g^k * g^{r-k}$. Isto é, $g^k * e = g^k * g^{r-k}$.

Pelo Lema 2.12, $g^{r-k} = e$.

O menor inteiro n tal que $g^n = e$ é chamado *ordem* de g.

Lema 2.14. *Seja G um conjunto e $*$ uma operação em G, tal que, as quatro propriedades:*

a) G é fechado sob $*$.

b) $*$ é associativa.

c) *Existe* $e \in G$, *tal que* $g * e = g$ *para todo* $g \in G$. *(Chamamos* e *de uma "identidade à direita").*

d) *Para cada* $g \in G$, *existe* $h \in G$, *tal que,* $g * h = e$. *(Chamamos* h *de um "inverso à direita" de* g*).*

são satisfeitas. Então $(G,*)$ *é um grupo.*

Prova. Para provar que $(G,*)$ é um grupo, basta observar que pelos Lemas 2.10 e 2.11, temos:

- Se existe $e \in G$, tal que $g * e = g$ para todo $g \in G$, então $g * e = e * g = g$ para todo $g \in G$
- Se para cada $g \in G$, existe $h \in G$, tal que, $g * h = e$, então para cada $g \in G$, existe $h \in G$, tal que, $g * h = h * g = e$

3 O CUBO MÁGICO E SUBGRUPOS

3.1 Notação para o Cubo

O Cubo Mágico é composto por vinte e sete pequenos cubos que serão chamados de "cubinhos". Vinte e seis desses cubinhos são visíveis (se você pegar seu cubo, descobrirá que o 27º cubinho, na verdade, não existe).

Ao trabalhar com o Cubo Mágico, é útil ter uma maneira sistemática de referir-se aos cubinhos individuais. Apesar de parecer natural usar as cores no cubinho, na verdade, é mais útil ter nomes que descrevam as localizações dos cubinhos. Os cubinhos dos cantos são chamados, apropriadamente, "cubinhos canto". Cada cubinho canto tem três faces visíveis, e há oito cubinhos canto. Os cubinhos com duas faces visíveis são chamados "cubinhos borda"; há doze cubinhos borda. Finalmente, os cubinhos com uma única face visível são chamados "cubinhos centro", e há seis cubinhos centro.

Agora, vamos nomear as seis faces do Cubo Mágico. Seguindo a notação desenvolvida por David Singmaster (veja FREY e SINGMASTER (1982)), nós as chamaremos direita (r), esquerda (l), superior (u), inferior (d), frontal (f) e posterior (b). A vantagem desta nomenclatura é que cada face pode ser referida por uma única letra.

Para citar um cubinho canto, nós, simplesmente, listaremos suas faces visíveis no sentido horário. Por exemplo, o cubinho do canto superior direito frontal será representado por urf. Claramente, nós também podemos nos referir a este cubinho como rfu ou fur. Às vezes, será relevante qual face está listada em primeiro lugar; nestes casos, consideraremos "cubinhos orientados". Isto é, os cubinhos orientados urf, rfu e fur são diferentes. Em outras situações, não nos importaremos com qual face está listada em primeiro lugar; nesses casos, consideramos "cubinhos não orientados". Isto é, os cubinhos não orientados urf, rfu e fur são o mesmo.

Da mesma forma, para cubinhos borda e centro, apenas listaremos as faces visíveis dos cubinhos. Por exemplo, o cubinho no centro da face frontal é simplesmente chamado de f, porque a sua única face visível encontra-se na parte da frente do cubo. Já para o cubinho borda dr, sua localização está nas faces inferior e direita.

Observe que estas nomenclaturas nos permitem agilizar a visualização do cubinho com que queremos trabalhar. Note também, que o Cubo Mágico, uma vez posto em sua posição inicial, terá suas configurações estabelecidas a partir desse momento, ou seja, todas as nomenclaturas citadas acima para os cubinhos serão dadas a partir da posição inicial considerada. Não podemos tirar o cubo dessa posição. Claro que os cubinhos podem sair de suas posições, conforme as faces sejam rotacionadas, no entanto, esses cubinhos não perdem suas nomenclaturas, apenas vão para outras posições conforme conveniência de quem os manuseia.

Figura 1 – Posição Inicial

Fonte: o Autor, 2016

Nós, também, frequentemente, mencionaremos os “cubículos”. Eles são rotulados da mesma maneira como os cubinhos, mas eles descrevem o espaço em que o cubinho reside. Assim, se o Cubo Mágico está na configuração de partida (isto é, o Cubo Mágico está resolvido), então cada cubinho reside no cubículo de mesmo nome (o cubinho urf encontra-se no cubículo urf, o cubinho f, no cubículo f, e assim por diante). Se você girar uma face do Cubo Mágico, os cubículos não se movem, mas os cubinhos se movem. Observe, porém, que quando você gira uma face do Cubo Mágico, todos cubinhos centros permanecem em seus cubículos.

Antes das convenções aqui apresentadas, sabíamos que o cubo estava resolvido quando todos os nove quadradinhos de cada uma das seis faces fossem todos da mesma cor. Se o cubo não estiver resolvido, como decidir qual a cor correta de uma face? Respondemos a esse questionamento olhando os cubinhos centros. Sabemos que eles não saem do lugar conforme as faces são rotacionadas, portanto, eles se tornam referências para todos os cubinhos de mesmas cores, como se eles polarizassem os cubinhos com cores afins às suas. (Lembre-se que as faces podem ser giradas e não existe a possibilidade de girarmos duas camadas de nove cubinhos, por isso a estabilidade dos cubinhos centros. Girar duas camadas, o que não é possível, é o mesmo que girar a terceira camada que, aí sim, é girar uma face).

Finalmente, queremos nomear alguns movimentos realizados no Cubo Mágico. O movimento mais básico que pode ser feito é girar uma única face. Indicaremos por R uma rotação no sentido horário da face direita (olhando para a face direita, vire-a $90°$ no sentido horário). Da mesma forma, usaremos as letras maiúsculas L, U, D, F e B para denotar rotações no sentido horário das faces correspondentes. Em geral, chamaremos qualquer sequência destes seis movimentos de face de um "movimento" do Cubo Mágico. Por exemplo, girando a face da direita no sentido anti-horário é um movimento que coincide com fazer R três vezes. Mais adiante, iremos apresentar uma notação para esses movimentos mais complexos.

Alguns fatos são evidentes. Em primeiro lugar, já observamos que os seis movimentos básicos mantêm os cubinhos centrais em seus cubículos. Note que qualquer movimento é uma sequência desses seis movimentos básicos. Isso significa que qualquer movimento do Cubo Mágico mantém os cubinhos centro em seus correspondentes cubículos (para uma prova formal, veja o exemplo logo após a Proposição 4.9). Também, qualquer movimento do Cubo Mágico coloca cubinhos canto em cubículos canto e cubinhos borda em cubículos borda; é impossível para um cubinho canto ocupar um cubículo borda ou para um cubinho borda ocupar um cubículo canto. Usando esses dois fatos, podemos começar a determinar quantas configurações possíveis o Cubo Mágico tem. Consideremos, por exemplo, no cubículo urf. Teoricamente, qualquer um dos 8 cubinhos canto poderia ocupar esse cubículo. Restariam, 7 possíveis cubinhos canto para ocupar o cubículo urb, 6 para o próximo cubículo canto, e assim por diante. Portanto, há $8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$ possíveis posicionamentos dos cubinhos canto. Observe que um cubinho canto pode encaixar-se em seu cubículo de 3 maneiras diferentes. Por exemplo, se um cubinho vermelho, branco e azul se encontra no cubículo urf, a face vermelha, branca, ou azul poderia estar na face u do cubículo (e observe que isto determina onde as outras duas faces estão). Uma vez que há 8 cubinhos canto e cada um pode se posicionar em seu cubículo em três maneiras diferentes, existem 3^8maneiras diferentes dos cubinhos canto poderem ser orientados. Portanto, existem $3^8 \cdot 8!$ possíveis configurações dos cubinhos canto. Da mesma forma, como há 12 cubinhos borda, existem 12! Posições que podem ser assumidas pelos cubinhos borda; cada cubinho borda tem duas orientações possíveis, dando 2^{12}orientações possíveis. Assim, existem $2^{12} \cdot 12!$ possíveis configurações dos cubinhos borda, dando um total de $2^{12} \cdot 3^8 \cdot 8! \cdot 12!$ configurações possíveis do Cubo Mágico. (Este número é aproximadamente igual a $5{,}19 \cdot 10^{20}$, ou 519 quintilhões).

Embora essas configurações sejam teoricamente possíveis, isso não significa que podem realmente ocorrer. Diremos que uma configuração do Cubo Mágico é válida se ela pode ser alcançada por uma série de movimentos a partir da configuração inicial. Verifica-se que algumas das configurações teoricamente possíveis que contamos não são realmente válidas. É natural, portanto, que tentemos:

1. Demonstrar que algumas configurações não são válidas.
2. Encontrar um conjunto de movimentos que podem nos levar, a partir de qualquer configuração válida de volta para a configuração inicial.

No presente trabalho, discutiremos apenas o aspecto de resolução do cubo.

3.2 **Interpretando o Cubo Mágico como um Grupo**

Nós podemos considerar o conjunto de movimentos do Cubo Mágico como elementos de um grupo, o qual denotaremos por $(\mathbb{G},*)$. Os elementos de $\mathbb{G}$ serão todos os movimentos possíveis do Cubo Mágico (por exemplo, um movimento possível é uma rotação no sentido horário de face superior seguida por uma rotação no sentido anti-horário da face direita). Dois movimentos serão considerados o mesmo se resultarem na mesma configuração do Cubo (por exemplo, girando uma face no sentido horário por $180°$ é o mesmo que girar a mesma face no sentido anti-horário em $180°$). A operação $*$ do grupo será definida da seguinte maneira: se M_1 e M_2 são dois movimentos, então $M_1 * M_2$ é o movimento em que você primeiro faz M_1 e depois faz M_2.

$(\mathbb{G},*)$ é um grupo? Para responder a esta pergunta, basta verificarmos as quatros propriedades indicadas no Lema 2.14.

- $\mathbb{G}$ é, certamente, fechado sob $*$ uma vez que, se M_1 e M_2 são movimentos, $M_1 * M_2$ também é um movimento.
- Se definimos e como o movimento "vazio" (isto é, um movimento que não altera a configuração do Cubo Mágico), então $M * e$ significa "primeiro faça M, então faça nada". Isto é certamente o mesmo que fazer apenas M, então $M * e = M$. Então, $(\mathbb{G},*)$ tem uma identidade à direita.
- Se M é um movimento, podemos inverter os passos do movimento e definir um movimento M'. Então, o movimento $M * M'$ significa "primeiro faça M, em seguida, inverta todos os passos de M". Isto é o mesmo que não fazer nada, então $M * M' = e$, assim M' é o inverso de M. Portanto, todos os elementos de $\mathbb{G}$ têm um inverso à direita.
- Finalmente, devemos mostrar que $*$ é associativa. Recorde que um movimento pode ser definido pela mudança que provoca na configuração. Em particular, um

movimento é determinado pela posição e orientação em que ele coloca cada cubinho.

Se C é um cubinho orientado, escreveremos $M(C)$ para o cubículo orientado que C ocupa depois de aplicarmos o movimento M, com as faces de $M(C)$ escritas na mesma ordem que as faces de C. Isto é, a primeira face de C coincidirá com a primeira face de $M(C)$, e assim por diante. Por exemplo, o movimento D coloca o cubinho ur no cubículo br, com a face u do cubinho coincidindo com a face b do cubículo e face r do cubinho, com a face r do cubículo. Assim, escrevemos $D(ur) = br$.

Primeiro, vamos investigar o quê uma sequência de dois movimentos faz com um cubinho. Se M_1 e M_2 são dois movimentos, então $M_1 * M_2$ é o movimento em que primeiro fazemos M_1 e depois fazemos M_2. O movimento M_1 move C ao cubículo $M_1(C)$; o movimento M_2 então, move-o para $M_2(M_1(C))$. Portanto, $(M_1 * M_2)(C) = M_2(M_1(C))$.

Para mostrar que $*$ é associativa, precisamos mostrar que $(M_1 * M_2) * M_3 = M_1 * (M_2 * M_3)$, para quaisquer movimentosM_1,M_2 e M_3. Isto é o mesmo que mostrar que$(M_1 * M_2) * M_3$ e $M_1 * (M_2 * M_3)$ fazem a mesma coisa para cada cubinho. Isto é, queremos mostrar que

$$[(M_1 * M_2) * M_3](C) = [M_1 * (M_2 * M_3)](C)$$

para qualquer cubinho C. Vimos acima que

$$[(M_1 * M_2) * M_3](C) = M_3\big((M_1 * M_2)(C)\big) = M_3\left(M_2\big(M_1(C)\big)\right)$$

Por outro lado,

$$[M_1 * (M_2 * M_3)](C) = (M_2 * M_3)\big(M_1(C)\big) = M_3\left(M_2\big(M_1(C)\big)\right).$$

Então,

$$(M_1 * M_2) * M_3 = M_1 * (M_2 * M_3).$$

Assim, $*$ é associativa.

Portanto, $(\mathbb{G},*)$ é de fato um grupo.

3.3. Subgrupos

Calculamos que há cerca de 519 quintilhões de possíveis configurações do Cubo Mágico (embora nem todas elas sejam válidas). Tentar entender um número tão grande de configurações, não é tarefa fácil! Será útil particularizar o problema; por exemplo, em vez de olhar para todos os movimentos possíveis do Cubo Mágico, poderíamos começar por olhar para os movimentos que apenas envolvem rotações das faces inferior e da direita.

Esta é uma filosofia geral na teoria de grupo: para compreender um grupo G, devemos tentar entender pequenas partes dele.

Definição 3.1. *Um subconjunto não vazio H de um grupo $(G,*)$ é chamado um subgrupo de G se $(H,*)$ é um grupo.*

A vantagem de estudar subgrupos é que eles podem ser muito menores e, consequentemente, mais simples; no entanto, eles ainda têm estrutura algébrica.

Exemplo 3.2. Um grupo é sempre um subgrupo de si mesmo. Além disso, o grupo trivial é um subgrupo de qualquer grupo. No entanto, estes subgrupos não são muito interessantes!

Exemplo 3.3. O conjunto dos inteiros pares é um subgrupo de $(\mathbb{Z}, +)$: afinal, os inteiros pares são certamente um subconjunto de $\mathbb{Z}$, e sabemos que a partir do Exemplo 2.4(h) que $(2\mathbb{Z}, +)$ é um grupo.

O próximo lema facilita verificar se um subconjunto é na verdade um subgrupo.

Lema 3.4. *Seja $(G,*)$ um grupo. Um subconjunto não vazio H de G é um subgrupo de $(G,*)$ se, e somente se, para todo $a, b \in H$, $a * b^{-1} \in H$.*

Prova. Em primeiro lugar, suponhamos que H é um subgrupo. Se $b \in H$, então $b^{-1} \in H$, uma vez que $(H,*)$ é um grupo. Assim, se sabemos também que $a \in H$, então $a * b^{-1} \in H$.

Reciprocamente, suponhamos que, para todo $a, b \in H$, tenhamos $a * b^{-1} \in H$.

- Seja $a \in H$. Então, $e = a * a^{-1}$, assim $e \in H$.
- Seja $b \in H$. Então, $b^{-1} = e * b^{-1} \in H$, assim existem inversos em H.
- Sejam $a, b \in H$. Pela etapa anterior, $b^{-1} \in H$, assim $a * b = a * (b^{-1})^{-1} \in H$. Assim, H é fechado sob $*$.
- Observe que $*$ é associativa, uma vez que, $(G,*)$ é um grupo.

Portanto, $(H,*)$ é um grupo, o que significa que H é um subgrupo de G.

Lema 3.5. *Seja G um grupo e S um subconjunto de G. Seja H o conjunto de todos os elementos de G que podem ser escritos como um produto finito de elementos de S e seus inversos. Então, H é um subgrupo de G.*

Prova. Note que H consiste em todos os elementos da forma $s_1 \cdots s_n$ (essa notação indica que temos um produto com vários elementos do conjunto) onde cada s_i ou é um elemento de S ou o inverso de um elemento de S. Observe que podemos estender por indução o resultado do Exemplo 2.7 para um produto com mais de dois fatores. Isto é, $(s_1 \cdots s_n)^{-1} = s_n^{-1} \cdots s_1^{-1}$.

Sejam $s_1 \cdots s_n$, $u_1 \cdots u_m \in H$. Conforme o Lema 3.4, basta mostrarmos que $(s_1 \cdots s_n) \cdot (u_1 \cdots u_m)^{-1} \in H$. Note que $(u_1 \cdots u_m)^{-1} = u_m^{-1} \cdots u_1^{-1}$. Portanto, $(s_1 \cdots s_n) \cdot (u_1 \cdots u_m)^{-1} = w_1 \cdots w_{m+n}$, onde cada w_i ou é um elemento de S ou o inverso de um elemento de S. Consequentemente, $(s_1 \cdots s_n) \cdot (u_1 \cdots u_m)^{-1} \in H$. Portanto, H é um subgrupo de G.

Chamamos H de *subgrupo de G gerado por S* e escrevemos $H = \langle S \rangle$. Ele é o menor subgrupo de G contendo S (você vê o porquê?).

3.4. Notação de Grupo Simplificada

É prática comum escrever as operações do grupo como uma multiplicação; isto é, escrevemos gh ao invés de $g * h$, e chamamos isso de "produto" de g e h. Com a afirmação "seja G um grupo" indicaremos que G é um grupo sob alguma operação que será escrita como multiplicação. Nós, também, muitas vezes, escreveremos o elemento de identidade de G como 1, em vez de e. Finalmente, usaremos a notação padrão para potências, assim g^2 representa gg, g^3 denota ggg, e assim por diante.

Em particular, faremos isso com ($\mathbb{G}$,$*$). Ou seja, a partir de agora, apenas chamaremos este grupo de $\mathbb{G}$, e escreveremos a operação $*$ como uma multiplicação. Por exemplo, DR representa o movimento D seguido pelo movimento R. O movimento que gira a face direita 90° no sentido anti-horário é o mesmo que um movimento de rotação de 90° no sentido horário da face direita três vezes, assim podemos escrever este movimento como R^3.

4 GERADORES

Seja G um grupo e S um subconjunto de G. No Lema 3.5, caracterizamos o subgrupo $\langle S\rangle$. Agora, apresentaremos algumas propriedades de $\langle S\rangle$. Primeiro, vamos olhar para o caso especial quando $\langle S\rangle$ é o próprio G.

Definição 4.1. *Seja G um grupo e S um subconjunto de G. Dizemos que S gera G ou que S é um conjunto de geradores de G se $G = \langle S\rangle$; isto é, cada elemento de G é escrito como um produto finito (sob a operação do grupo) envolvendo elementos de S ou inversos de elementos de S.*

Exemplo 4.2. Cada elemento de $\mathbb{Z}$ é escrito como uma soma finita de $1'$s ou $-1'$s, assim $\mathbb{Z}$ é gerado por $\{1\}$. Isto é, $\mathbb{Z} = \langle 1\rangle$. Nesse exemplo, G=$(\mathbb{Z}, +)$ e $S = \{1\}$. Observe, por exemplo, que -3 pode ser gerado por elementos de S ou seus inversos: $-3 = (-1) + (-1) + (-1)$. Pela mesma razão, $\mathbb{Z} = \langle -1\rangle$. Nesse caso, $G = (\mathbb{Z}, +)$ e $S = \{-1\}$. Claramente, também é verdade que $\mathbb{Z} = \langle 1,2\rangle$. Observe que -3 pode ser gerado por elementos de $S = \{1,2\}$ ou seus inversos, por exemplo: $(-1) + (-2) = -3$. Em geral, há muitos conjuntos de geradores possíveis de um grupo. Será que $\mathbb{Z} = \langle 2\rangle$? Nesse caso, $S = \{2\}$ não é um gerador de $G = (\mathbb{Z}, +)$. Isso fica evidenciado quando, por exemplo, considerarmos os inteiros ímpares que não podem ser expressos como somas de $2's$ ou $-2's$.

Exemplo 4.3. Cada elemento do $\mathbb{Z}_4$ é escrito como uma soma finita de $1'$s, assim $\mathbb{Z}_4 = \langle 1\rangle$.

Usualmente, se temos $a = b$ e $c = b$, concluímos que $a = c$. Note que o conjunto $S = \{1\}$ tanto gera $\mathbb{Z}$ quanto $\mathbb{Z}_4$, isto é, $\mathbb{Z} = \langle 1\rangle$ e $\mathbb{Z}_4 = \langle 1\rangle$, mas esses dois conjuntos não são iguais! Relembrando que $\mathbb{Z}_4$ é o conjunto das classes de equivalência dos restos da divisão de um número inteiro x por 4, ou seja, são os inteiros módulo 4. Já, $\mathbb{Z}$ é o conjunto dos números inteiros. Observe que $\langle S\rangle$ só faz sentido no contexto de um dado grupo.

Exemplo 4.4. Cada elemento de $\mathbb{G}$ é escrito como uma sequência finita de voltas do Cubo Mágico, de modo que $\mathbb{G} = \langle D, U, L, R, F, B\rangle$. Vejamos alguns exemplos: relembremos que D é uma rotação da face inferior no sentido horário, U é uma rotação da face superior no sentido horário, assim como L, R, F e B são rotações das faces esquerda, direita, frontal e posterior, respectivamente, no sentido horário. Também temos, por exemplo, D^3 sendo três rotações da face inferior no sentido horário, o que seria o mesmo que D^{-1}, que por sua vez é uma rotação da mesma face no sentido anti-horário.

Você pode pensar em geradores como sendo o "cerne", a "essência" do grupo; uma vez que cada elemento do grupo é escrito em termos dos geradores, o conhecimento sobre os geradores pode, muitas vezes, ser traduzido para o conhecimento sobre todo o grupo. Faremos isto, mais precisamente, em breve.

Definição 4.5. *Um grupo G é cíclico se existe $g \in G$ tal que $G = \langle g \rangle$.*

Em outras palavras, um grupo G é cíclico quando todos os seus elementos são gerados por um único elemento $g \in G$ sob a operação do grupo, através de um número finito dessa operação com g ou seu inverso. Isto não quer dizer que G é, necessariamente, finito, pelo fato de ser cíclico.

Exemplo 4.6. $\mathbb{Z}$ e $\mathbb{Z}_4$ são cíclicos pois são gerados por conjuntos unitários. Nesse caso, $\mathbb{Z}$ é infinito e $\mathbb{Z}_4$ é finito.

Para grupos finitos, podemos até relaxar, levemente, a definição de geradores, deixando de fora os inversos de S. Para provar isso, precisamos de um lema.

Lema 4.7. Seja G um grupo finito e $g \in G$. Então, $g^{-1} = g^n$, para algum $n \in \mathbb{N}$.
Prova. Se $g = e$, então, nada há para mostrar pois $e^{-1} = e^1$. Isto é, o lema se verifica para $g = e$ com $n = 1$. Assim, suponha $g \neq e$. Pelo Lema 2.13, existe um inteiro positivo$m$, tal que, $g^m = e$. Uma vez que $g \neq e$, temos $m \neq 1$. Logo, $m > 1$. Seja $n = m - 1 \in \mathbb{N}$. Então, $gg^n = g^m = e$, assim g^n é o inverso do g pelo Lema 2.11.

O Lema 4.7 nos diz que em um grupo finito, para todo elemento g do grupo, seu inverso g^{-1} pode ser escrito como uma potência g, ou seja, $g^{-1} = g^n$, para algum natural n. Consequentemente, ao definirmos um gerador S de um grupo finito G, não será necessário considerar os inversos dos elementos de S. Isto é, qualquer elemento de G poderá ser escrito como um produto finito de elementos de S.

Lema 4.8. Seja G um grupo finito e S um subconjunto de G. Então, $G = \langle S \rangle$ se e somente se cada elemento de G for escrito como um produto finito dos elementos de S.

Prova. Se cada elemento de G é escrito como um produto finito dos elementos de S, então é claro que $G = \langle S \rangle$.

Por outro lado, suponha que $G = \langle S \rangle$. Isto significa que cada elemento de G é escrito como um produto finito $s_1 \cdots s_n$onde cada s_i está em S ou é o inverso de um elemento de S. O ponto de chave da prova é o uso do Lema 4.7 que garante que o inverso de um elemento de S também pode ser escrito como um produto finito de elementos de S. Para ser mais rigoroso, usaremos indução sobre n.

Suponha $n = 1$. Isto é, o elemento $g \in G$ é escrito em termos dos elementos de S como $g = s_1$, onde s_1 pertence a S ou é o inverso de algum de elemento s de S. No primeiro caso, g é escrito como um produto de um único elemento de S. Se s_1 é o inverso de $s,$ então pelo Lema 4.7, temos $s^{-1} = s^n$, para algum $n \in \mathbb{N}$. Logo, $g = s_1 = s^{-1} = s^n$. Isto é, g é escrito como um produto finito de elementos de S.

Agora, suponha que a afirmação é verdadeira para todos os números naturais menores do que n; considere um elemento $g \in G$ que seja escrito como o produto $s_1 \cdots s_n$, onde cada s_i está em S ou é o inverso de um elemento de S. Queremos mostrar que $s_1 \cdots s_n$ pode ser escrito como um produto finito de elementos de S. Pela hipótese de indução, $s_1 \cdots\ s_{n-1}$ e s_n são, ambos, escritos como produtos finitos de elementos de S. Portanto, seu produto $(s_1 \cdots\ s_{n-1})s_n$ certamente também o pode. Consequentemente, $s_1 \cdots s_n = (s_1 \cdots\ s_{n-1})s_n$ pode ser escrito como um produto finito de elementos de S.

Agora, veremos como estender propriedades dos geradores para todo o grupo.

Proposição 4.9. *Seja G um grupo finito e Sum subconjunto de G. Suponha que as duas condições a seguir são satisfeitas.*

1. *Cada elemento de S satisfaz uma propriedade P.*
2. *Se $g \in G$ e $h \in G$, ambos satisfazendo a propriedade P, então gh também satisfaz a propriedade P.*

Então, cada elemento de $\langle S \rangle$ satisfaz P.

Prova. Pelo Lema 4.8, qualquer elemento de $\langle S \rangle$ pode ser escrito como $s_1 \cdots s_n$ para algum $n \in \mathbb{N}$ e cada s_i é um elemento de S. Provaremos a proposição por indução em n.

Suponha $n = 1$. Isto é, tomamos um elemento $g \in G$ que pode ser escrito em termos dos elementos de S como $g = s_1$, onde s_1 pertence a S. Como$s_1 \in S$, $g = s_1$ satisfaz a propriedade P por hipótese.

Suponhamos, indutivamente, que todo elemento de G que pode ser escrito como um produto envolvendo $n-1$ elementos de S satisfaz a propriedade P. Considere agora um elemento g de G que pode ser escrito como um produto de n elementos de S. Isto é, $g = s_1 \cdots s_n$ e cada s_i é um elemento de S. Então, como o produto $(s_1 \cdots s_{n-1})s_n$ é um produto de dois elementos que satisfazem a propriedade P e $g = s_1 \cdots s_n = (s_1 \cdots s_{n-1})s_n$, temos que g também satisfaz a propriedade P.

A proposição anterior nos diz que para que uma propriedade satisfeita por todos os elementos de um subconjunto S de um grupo finito G também seja satisfeita pelo grupo gerado por S é suficiente que o subconjunto dos elementos de G que satisfazem P seja "fechado" com relação à propriedade P.

Antes de provarmos isto, vamos ver como esta propriedade poderia ser usada.

Exemplo 4.10. Seja $S = \{D, U, L, R, F, B\} \subset \mathbb{G}$. Então, cada $M \in S$ satisfaz a propriedade "M mantém todos os cubinhos centro em seus cubículos". Se $M_1, M_2 \in \mathbb{G}$ são, tais que, mantém todos os cubinhos centro em seus cubículos, então, M_1M_2, certamente, mantém todos os cubinhos centro em seus cubículos. Uma vez que $\mathbb{G} = \langle S \rangle$, a proposição diz que todo elemento de $\mathbb{G}$ mantém os cubinhos centro em seus cubículos.

Esta proposição é extremamente útil para o Cubo Mágico, porque isso significa, em linhas gerais, que só precisamos compreender as propriedades dos seis movimentos básicos, ao invés de todos os 5×10^{20} movimentos possíveis.

5 O GRUPO SIMÉTRICO

Quando deduzimos o número de configurações possíveis do Cubo Mágico, utilizamos o fato de que qualquer movimento envia cubinhos canto para cubículos canto para deduzir que há 8! possíveis maneiras de posicionar os cubinhos canto. Neste capítulo, estabeleceremos os fundamentos matemáticos necessários para compreender essas possibilidades.

Ao invés de apenas olhar para as configurações dos oito cubinhos, olharemos para as configurações de quaisquer n objetos. Indicaremos esses objetos por $1, 2, \ldots, n$. Queremos organizar esses objetos colocando-os em n caixinhas. Se numerarmos as caixas de 1 a n, então podemos definir uma função $\sigma\colon \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$, representando por $\sigma\,(i)$ o objeto que foi colocado na caixa i.

Exemplo 5.1. Podemos colocar os objetos $1, 2, 3$, na ordem de 3 1 2. Aqui, 3 está na primeira caixa, 1 está na segunda caixa, e 2 está na terceira caixa. Assim, esta ordenação corresponde à função $\sigma\colon \{1, 2, 3\} \to \{1, 2, 3\}$ definida por $\sigma\,(1) = 3$, $\sigma\,(2) = 1$ e $\sigma\,(3) = 2$.

O que sabemos sobre σ?

Lema 5.2. A função σ é uma bijeção.

Prova. Suponha $x \neq y$. Uma vez que um número não está em mais do que uma caixa, se $x \neq y$, as caixas x e y devem conter números diferentes, Isto é, $\sigma\,(x) \neq \sigma\,(y)$. Portanto, σ é injetora.

Como toda caixa terá que receber um número e cada número só pode estar em uma única caixa, qualquer número $y \in \{1, 2, \ldots, n\}$ deve estar em alguma caixa, digamos que ele esteja na caixa x. Então, $\sigma\,(x) = y$. Assim, σ é sobrejetora.

Por outro lado, se consideramos uma bijeção $\sigma\colon \{1, \ldots, n\} \to \{1, \ldots, n\}$, então σ define uma arrumação de n objetos: por exemplo, coloque o objeto $\sigma(i)$ na caixa i. Assim, o conjunto de todas as possíveis arrumações pode, naturalmente, ser identificado com o conjunto de bijeções $\sigma\colon \{1, \ldots, n\} \to \{1, \ldots, n\}$. Portanto, ao invés de estudar as arrumações possíveis, estudaremos essas bijeções.

Definição 5.3. *O grupo simétrico sobre n letras é o conjunto das bijeções de* $\{1,2,\ldots,n\}$ *em* $\{1,2,\ldots,n\}$*, com a operação de composição. Denotamos este grupo por* S_n*.*

Note que S_n é um grupo pelo Exemplo 2.6.

Vamos fazer um exemplo para melhor compreender este grupo.

Exemplo 5.4. Sejam $\sigma,\tau \in S_3$ definidas por $\sigma(1)=3$, $\sigma(2)=1$, $\sigma(3)=2$, $\tau(1)=1$, $\tau(2)=3$ e $\tau(3)=2$. Então, $(\sigma\tau)(1)=\tau\big(\sigma(1)\big)=\tau\,(3)=2$, $(\sigma\tau)(2)=\tau\,(1)=1$ e $(\sigma\tau)(3)=\tau(2)\ =\ 3$.

Observe que qualquer elemento de S_n pode ser identificado com uma permutação do conjunto $\{1,2,\ldots,n\}$. Os elementos de S_n também são chamados de permutações.

5.1. Decomposição em Ciclos disjuntos

Há uma forma mais compacta de escrever os elementos do grupo simétrico. Usaremos um exemplo para facilitar o entendimento deste processo .

Exemplo 5.5. Considere $\sigma \in S_{12}$ definida por:

$$\begin{array}{cccccc} \sigma(1)=12 & \sigma(2)=4 & \sigma(3)=5 & \sigma(4)=2 & \sigma(5)=6 & \sigma(6)=9 \\ \sigma(7)=7 & \sigma(8)=3 & \sigma(9)=10 & \sigma(10)=1 & \sigma(11)=11 & \sigma(12)=8 \end{array}$$

Escreveremos "$i\ \mapsto\ j$" ("i mapeia para j") para representar $\sigma\,(i)=j$. Então,

$1\mapsto 12, 12\mapsto 8, 8\mapsto 3, 3\mapsto 5, 5\mapsto 6, 6\mapsto 9, 9\mapsto 10, 10\mapsto 1$

$2\mapsto 4, 4\mapsto 2$

$7\mapsto 7$

$11\mapsto 11$

Estes dados nos dizem o que σ faz a cada número, logo definem σ. Abreviadamente, escreveremos:

$\sigma\ =\ (1\ 12\ 8\ 3\ 5\ 6\ 9\ 10)\ (2\ 4)\ (7)\ (11)$.

Aqui, $(1\ 12\ 8\ 3\ 5\ 6\ 9\ 10)$, $(2\ 4)$, (7) e (11) são chamados de ciclos. Ao escrever a decomposição em ciclos disjuntos, omitimos os ciclos com apenas um número, assim a decomposição em ciclos disjuntos de σ é $\sigma=(1\ 12\ 8\ 3\ 5\ 6\ 9\ 10)\ (2\ 4)$.

Agora, vamos, realmente, definir o que é um ciclo.

Definição 5.6. *O ciclo* $(i_1\, i_2 \cdots\, i_k)$ *é o elemento* $\tau \in S_n$ *definido por* $\tau\,(i_1) = i_2, \tau\,(i_2) = i_3, \ldots, \tau(i_{k-1}) = i_k$, $\tau(i_k) = i_1$ *e* $\tau(j) = j$, *se* $j \neq i_r$ *para qualquer* r. *O comprimento desse ciclo é* k, *e o suporte do ciclo é o conjunto* $\{i_1, \ldots, i_k\}$ *dos números que aparecem no ciclo. O suporte é denotado por* supp τ. *Um ciclo de comprimento* k *é também chamado um* k*-ciclo.*

Definição 5.7. *Dois ciclos* σ *e* τ *são disjuntos se eles não têm números em comum, isto é,* supp $\sigma \cap$ supp $\tau = \emptyset$.

Lema 5.8. *Sejam* $\sigma, \tau \in S_n$ *ciclos. Se* σ *e* τ *são disjuntos, então* $\sigma\tau = \tau\sigma$.

Prova. Como supp $\sigma \cap$ supp $\tau = \emptyset$, o conjunto $\{1, \ldots, n\}$ pode ser escrito como a união disjunta de supp σ, supp τ e o complementar da união dos suportes. Isto é

$$\{1, \ldots, n\} = \text{supp}\,\sigma \cup \text{supp}\,\tau \cup \{1, \ldots, n\} \setminus (\text{supp}\,\sigma \cup \text{supp}\,\tau).$$

Note que os elementos de $\{1, \ldots, n\} \setminus (\text{supp}\,\sigma \cup \text{supp}\,\tau)$ são justamente os ciclos com apenas um número. Desse modo, se $i \in \{1, \ldots, n\}$, há apenas duas possibilidades:

- $i \notin$ supp σ e $i \notin$ supp τ. Neste caso, $i \in \{1, \ldots, n\} \setminus (\text{supp}\,\sigma \cup \text{supp}\,\tau)$ e $\sigma(i) = i$ de modo que
$$(\sigma \circ \tau)(i) = \tau\left(\sigma(i)\right) = \tau\,(i) = i \;\text{ e }\; (\tau \circ \sigma)(i) = \sigma(\tau\,(i)) = \sigma(i) = i.$$
- i pertence ao suporte de apenas um dos ciclos σ ou τ. Podemos supor sem perda de generalidade, que $i \notin$ supp σ e $i \in$ supp τ. Então, $\sigma(i) = i$, assim
$$(\sigma \circ \tau)(i) = \tau\,(\sigma(i)) = \tau(i).$$
Por outro lado, $(\tau \circ \sigma)(i) = \sigma(\tau(i))$. Agora, uma vez que $\tau(i) \in$ supp τ e supp $\tau \cap$ supp $\sigma = \emptyset$, $\tau(i) \notin$ supp σ. Portanto, $\sigma\left(\tau(i)\right) = \tau(i)$. Assim, novamente teremos $(\sigma\tau)(i) = (\tau\sigma)(i)$.

Portanto, $(\sigma\tau)(i) = (\tau\sigma)(i) = i$ para todo i, o que mostra que $\sigma\tau = \tau\sigma$.

Em geral, dadas duas bijeções f e g, $f, g\colon A \to A$, não é verdade que $f \circ g = g \circ f$. O Lema 5.8 nos diz que quando os ciclos $\sigma, \tau \in S_n$ são disjuntos, as bijeções σ e τ comutam, isto é, $\sigma \circ \tau = \tau \circ \sigma$.

Qualquer bijeção $\sigma \in S_n$ é escrita como um produto (sob a operação do grupo, que é a composição) de ciclos disjuntos. Este produto é chamado decomposição em ciclos disjuntos de σ. No nosso exemplo, apresentaremos um método para encontrar a decomposição em ciclos disjuntos de uma permutação.

Denotamos a permutação identidade por 1.

Exemplo 5.9. O grupo S_2 tem apenas dois elementos: as permutações 1 e $(1\ 2)$.

Exemplo 5.10. Sejam $\sigma, \tau \in S_6$ definidas por

$\sigma(1) = 3$	$\sigma(2) = 5$	$\sigma(3) = 4$	$\sigma(4) = 1$	$\sigma(5) = 2$	$\sigma(6) = 6$
$\tau(1) = 5$	$\tau(2) = 4$	$\tau(3) = 3$	$\tau(4) = 2$	$\tau(5) = 1$	$\tau(6) = 6$

Em notação de ciclo, $\sigma = (1\ 3\ 4)\ (2\ 5)$ e $\tau = (1\ 5)\ (2\ 4)$. Logo, $\sigma\tau = (1\ 3\ 2)\ (4\ 5)$ e $\tau\sigma = (1\ 2)(3\ 4\ 5)$. Podemos também facilmente calcular $\sigma^2 = (1\ 4\ 3)$ e $\tau^2 = 1$.

Lembramos que a representação $\tau^2 = 1$ nos diz que a composição de τ com ela mesma resulta na permutação identidade. Isto é, $\tau^2(i) = i$ para todo $i = 1, \dots, 6$.

Exemplo 5.11.

(a) Sejam $\sigma, \tau \in S_5$ definidas da seguinte forma.

$$\sigma(1) = 3 \quad \sigma(2) = 4 \quad \sigma(3) = 5 \quad \sigma(4) = 2 \quad \sigma(5) = 1$$
$$\tau(1) = 5 \quad \tau(2) = 3 \quad \tau(3) = 2 \quad \tau(4) = 4 \quad \tau(5) = 1$$

Em notação de ciclo,

$$\sigma = (1\ 3\ 5)(2\ 4) \qquad \tau = (1\ 5)(2\ 3)$$
$$\sigma^2 = (1\ 5\ 3) \qquad \tau^2\sigma = (1\ 3\ 5)(2\ 4)$$

(b) Seja $\sigma = (1\ 12\ 8\ 10\ 4)(2\ 13)(5\ 11\ 7)(6\ 9)$.

Em notação de ciclo,

$\sigma^2 = (1\ 8\ 4\ 12\ 10)(2\ 13)(5\ 7\ 11)$.

$\sigma^3 = (1\ 10\ 12\ 4\ 8)(2\ 13)\ (6\ 9)$.

Lema 5.12. *Se σ é uma permutação com o tipo de ciclo de $n_1, \dots, n_r$, então a ordem*[1] *de σ é n_r.*

Prova. Para determinar a ordem de uma permutação, vamos expressar a ação de sucessivas aplicações de σ sobre um de seus ciclos de comprimento m. Seja $(k_1 k_2 \cdots k_m)$ um dos ciclos na decomposição de σ, queremos mostrar que $\sigma^j(k_i) = k_{i+j \bmod m}$, para $1 \leq j \leq m$ e convencionamos que $k_0 = k_m$. Observe que teremos a identidade quando $\sigma^j(k_i) = k_{i+j \bmod m} = k_i$. Isto é quando $i = i + j \bmod m$. O menor valor de j que torna essa identidade verdadeira coincide com o comprimento do ciclo. Se $j = 1$, temos $\sigma(k_i) = k_{i+1 \bmod m}$. Suponha que $\sigma^j(k_i) = k_{i+j \bmod m}$, para $1 \leq j < m$. Temos $\sigma^{j+1}(k_i) = \sigma\left(\sigma^j(k_i)\right) = \sigma\left(k_{i+j \bmod m}\right) = k_{i+j+1 \bmod m}$. Sabemos que $1 \leq n_1 \leq n_2 \leq \cdots \leq n_r$. Portanto, a ordem de uma permutação com tipo de ciclo de $n_1, \dots, n_r$ é igual a n_r.

Definição 5.12. Seja $\sigma \in S_n$. A lista de inteiros $1 \leq n_1 \leq \cdots \leq n_r$ formada pelos comprimentos dos ciclos de uma decomposição (incluindo seus 1-ciclos) em ciclos disjuntos de σ é chamada de tipo de ciclo de σ.

5.2. Cubo Mágico

Podemos escrever cada movimento do Cubo Mágico usando uma notação ciclo ligeiramente modificada. Queremos descrever o que acontece com cada cubinho orientado; ou seja, queremos descrever para onde cada cubinho se move e para onde cada face do cubinho se move. Por exemplo, se "desdobrássemos" o cubo e desenhássemos a face voltada para baixo, obteríamos

Figura 2 – Face inferior

	f	f	f	
l	d	d	d	r
l	d	d	d	r
l	d	d	d	r
	b	b	b	

Fonte: CHEN, 2004

Se rodarmos esta face no sentido horário em 90° (isto é, aplicarmos o movimento D), então, a face voltada para baixo mostrará

[1] Para definição de ordem, veja Lema 2.13.

Figura 3 – Face inferior rotacionada

	l	l	l	
b	d	d	d	f
b	d	d	d	f
b	d	d	d	f
	r	r	r	

Fonte: CHEN, 2004

Logo, $D(dlf) = dfr$ pois o cubinho dlf agora reside no cubículo dfr (com a face d do cubinho residindo na face d do cubículo, a face l do cubinho residindo na face f do cubículo, e a face f do cubinho residindo na face r do cubículo). Da mesma forma, $D(dfr) = drb$, $D(drb) = dbl$ e $D(dbl) = dlf$. Se fizermos a mesma coisa para os cubinhos borda, encontramos $D = (dlf\ dfr\ drb\ dbl)\ (df\ dr\ db\ dl)$. Note que essa decomposição em dois ciclos traduz as afirmações feitas anteriormente sobre os movimentos do cubo. O primeiro ciclo nos mostra que cubinhos canto movem-se para cubículos canto e os borda movem-se para cubículos borda.

Exemplo 5.13. Verifique que a decomposição ciclos disjuntos de R é $(rfu\ rub\ rbd\ rdf)\ (ru\ rb\ rd\ rf)$.

Figura 4 – Face direita

	b	b	b	
u	r	r	r	d
u	r	r	r	d
u	r	r	r	d
	f	f	f	

(a)

	u	u	u	
f	r	r	r	b
f	r	r	r	b
f	r	r	r	b
	d	d	d	

(b)

Legenda: (a) – Face direita desdobrada; (b) – Face direita girada
Fonte: o Autor, 2016

Vale citar a regra da mão direita!!!

Podemos nos valer de uma visão prática para orientarmos o sentido horário no cubo. Basta usarmos a mão direita como instrumento para essa orientação.

Com os quatro dedos unidos e levemente curvados, mostramos o giro no sentido horário. Já, com o polegar perpendicular aos quatro dedos, apontamos o mesmo para o cubo. Assim, definimos a rotação no sentido horário para quaisquer faces ou para quaisquer orientações nos cubinhos.

Figura 5 – Regra da mão direita

Fonte: O Autor, 2015

.

6 CONFIGURAÇÕES DO CUBO MÁGICO

Como já dissemos, a configuração do Cubo Mágico é determinada por quatro parâmetros:

- as posições dos cubinhos canto
- as posições dos cubinhos borda
- as orientações dos cubinhos canto
- as orientações dos cubinhos borda

O primeiro é descrito por um elemento σ de S_8 (isto é, o elemento de S_8 que move os cubinhos canto para as novas posições). O segundo é descrito por um elemento τ de S_{12}. Agora, veremos como entender o terceiro e o quarto parâmetros. A ideia básica é fixar uma "orientação de partida" e uma forma sistemática de escrever como uma determinada orientação difere desta orientação inicial. Isto é, na maioria das vezes, apenas uma questão de notação.

Começaremos com os cubinhos canto. Cada cubinho canto tem três possíveis orientações, e numeraremos estas orientações com 0, 1 e 2. Vamos explicar o que esses números significam. Imagine que o seu Cubo Mágico esteja na configuração inicial. Escrevamos um número sobre uma face de cada cubículo canto, como se segue.

1 na face u do cubículo ufl

2 na face u do cubículo urf

3 na face u do cubículo ubr

4 na face u do cubículo ulb

5 na face d do cubículo dbl

6 na face d do cubículo dlf

7 na face d do cubículo dfr

8 na face d do cubículo drb

Assim, cada cubículo canto agora tem exatamente uma face numerada. Cada cubinho canto, portanto, tem uma face que se encontra em uma face numerada do cubículo. Rotule essa face do cubinho com 0. Siga no cubinho no sentindo horário, rotule a próxima face com 1 e, em seguida, rotule a face final com 2. Em nossas ilustrações, consideramos na configuração inicial do cubo a seguinte convenção: a face direita (r) é a branca; a esquerda (l), amarela; a superior (u), vermelha; a inferior (d), laranja; a frontal (f), azul e a posterior (b), verde.

Figura 6 – Numeração dos cubinhos

(a)

(b)

Legenda: (a) faces frontal, superior e direita; (b) faces esquerda, superior e frontal.
Fonte: o Autor, 2016

Exemplo 6.1. Se olharmos diretamente para a face inferior e "desdobrarmos" o cubo, veremos as faces dos cubinhos dispostas da seguinte maneira.

Figura 7 – Face inferior

	f	f	f	
l	d	d	d	r
l	d	d	d	r
l	d	d	d	r
	b	b	b	

(a)

	6		7	
	5		8	

(b)

	2		1	
1	0		0	2
2	0		0	1
	1		2	

(c)

Legenda: (a) – Face inferior desdobrada; (b) – numeração dos cubículos; (c) – rótulos dos cubinhos
Fonte: o Autor, 2016

Agora, cada face de cada cubinho canto tem um número nela. Se o Cubo Mágico está em qualquer configuração, descreveremos as orientações dos cubinhos canto da seguinte maneira: para qualquer i tomado no conjunto $\{1,2,\dots,8\}$, encontramos a face do cubículo rotulada por i; seja x_i o número da face do cubinho situada nessa face do cubículo. Escrevemos x para a 8-upla $(x_1,\dots,x_8)$. Observe que podemos pensar em cada $x_i$como a quantidadede voltas no sentido horário que afastam o cubinho de sua posição original. Isto é a quantidade de voltas que afastaram a face 0 do cubinho da face numerada do cubículo. Note que um cubinho que dê 3 voltas terá a mesma orientação que um cubinho que não saiu de sua posição original, isto é, que não tenha dado nenhuma volta. Assim, devemos pensar em x_i como um elemento de $\mathbb{Z}_3$. Então, x é uma 8-upla de elementos de $\mathbb{Z}_3$; escrevemos $x \in (\mathbb{Z}_3)^8$.

Exemplo 6.2. Se o Cubo Mágico está na configuração inicial, cada x_i é 0. Também escrevemos $x = 0$ para indicar que cada $x_i = 0$.

Exemplo 6.3. Vejamos como ficam os x_i depois que aplicamos o movimento R para um cubo na configuração inicial. Na configuração de inicial, a face direita está organizada da seguinte maneira:

Figura 8 – Face direita

	u	u	u	
f	r	r	r	b
f	r	r	r	b
f	r	r	r	b
	d	d	d	

(a)

	2		3	
	7		8	

(b)

	0		0	
2	1		2	1
1	2		1	2
	0		0	

(c)

Legenda: (a) – Face direita desdobrada; (b) – numeração dos cubículos; (c) – rótulos dos cubinhos
Fonte: o Autor, 2016

Após um giro de 90° da face direita do cubo, a face fica assim organizada:

Figura 9 – Face direita rotacionada

	f	f	f	
d	r	r	r	u
d	r	r	r	u
d	r	r	r	u
	b	b	b	

(a)

	1		2	
0	2		1	0
0	1		2	0
	2		1	

(b)

Legenda: (a) – Face direita desdobrada; (b) – rótulos dos cubinhos
Fonte: o Autor, 2016

Os cubinhos na face esquerda não são afetados por R, assim $x_1 = 0$, $x_4 = 0$, $x_5 = 0$ e $x_6 = 0$. Por outro lado, temos $x_2 = 1$, $x_3 = 2$, $x_7 = 2$ e $x_8 = 1$. Assim, $x = (0, 1, 2, 0, 0, 0, 2, 1)$.

Podemos fazer a mesma coisa para os cubinhos borda. Primeiro, rotulamos os cubículos borda como se segue. Escreva:

1 na face u do cubículo ub

2 na face u do cubículo ur

3 na face u do cubículo uf

4 na face u do cubículo ul

5 na face b do cubículo lb

6 na face b do cubículo rb

7 na face f do cubículo rf

8 na face f do cubículo lf

9 na face d do cubículo db

10 na face d do cubículo dr

11 na face d do cubículo df

12 na face d do cubículo dl

Cada cubinho borda, agora, tem uma face situada em uma face numerada do cubículo; rotule essa face do cubinho com 0 e rotule a outra face do cubinho com 1. Em seguida, seja y_i o número da face do cubinho na face numerada i do cubículo. Isto define $y \in (\mathbb{Z}_2)^{12}$.

Assim, qualquer configuração do Cubo Mágico pode ser descrita por $\sigma \in S_8$, $\tau \in S_{12}$, $x \in (\mathbb{Z}_3)^8$ e $y \in (\mathbb{Z}_2)^{12}$. Então, escreveremos configurações do Cubo Mágico como 4-uplas (σ, τ, x, y).

Vamos ilustrar essa notação para cubo. Usaremos dois cubos, um com as numerações e o outro com as letras correspondentes de cada face. Seguiremos esse padrão para as nossas representações posteriores, ou seja, essa será nossa configuração inicial para o cubo.

Figura 10 – Numeração dos cubinhos

(a) (b)

(c)

(d)

(e)

(f)

Legenda: (a) – direita; (b) – esquerda; (c) – superior; (d) – inferior; (e) – frontal; (f) – posterior.
Fonte: o Autor, 2016

Sempre que quisermos localizar os cubículos, nos remeteremos a essa configuração inicial.

Exemplo 6.4. A configuração inicial é $(1, 1, 0, 0)$.

Exemplo 6.5. Assuma que seu cubo está na configuração inicial. Seja (σ, τ, x, y) a configuração do cubo depois de fazermos o movimento $[D, R]$, que é definido por $DRD^{-1}R^{-1}$. Vamos identificar σ, τ, x e y para essa situação.

Mostramos, anteriormente, que

$$D = (dlf\ dfr\ drb\ dbl)(df dr\ db\ dl) \quad \text{e} \quad R = (rfu\ rub\ rbd\ rdf)(ru\ rb\ rd\ rf).$$

Portanto,

$$D^{-1} = (dbl\ drb\ dfr\ dlf)(dl\ db\ dr\ df) \quad \text{e} \quad R^{-1} = (rdf\ rbd\ rub\ rfu)(rf\ rd\ rb\ ru).$$

Assim,

$$[D, R] = (dlf\ dfr\ lfd\ frd\ fdl\ rdf)(drb\ bru\ bdr\ ubr\ rbd\ rub)\ (df dr\ br) \qquad (6.1)$$

De fato, para facilitar a compreensão, vamos representar os cubículos das faces inferior e direita usando negrito:

Figura 11 – Cubículos das faces inferior e direita

	$\boldsymbol{f}$	$\boldsymbol{f}$	$\boldsymbol{f}$	
$\boldsymbol{l}$	$\boldsymbol{d}$	$\boldsymbol{d}$	$\boldsymbol{d}$	$\boldsymbol{r}$
$\boldsymbol{l}$	$\boldsymbol{d}$	$\boldsymbol{d}$	$\boldsymbol{d}$	$\boldsymbol{r}$
$\boldsymbol{l}$	$\boldsymbol{d}$	$\boldsymbol{d}$	$\boldsymbol{d}$	$\boldsymbol{r}$
	$\boldsymbol{b}$	$\boldsymbol{b}$	$\boldsymbol{b}$	

	$\boldsymbol{u}$	$\boldsymbol{u}$	$\boldsymbol{u}$	
$\boldsymbol{f}$	$\boldsymbol{r}$	$\boldsymbol{r}$	$\boldsymbol{r}$	$\boldsymbol{b}$
$\boldsymbol{f}$	$\boldsymbol{r}$	$\boldsymbol{r}$	$\boldsymbol{r}$	$\boldsymbol{b}$
$\boldsymbol{f}$	$\boldsymbol{r}$	$\boldsymbol{r}$	$\boldsymbol{r}$	$\boldsymbol{b}$
	$\boldsymbol{d}$	$\boldsymbol{d}$	$\boldsymbol{d}$	

Fonte: o Autor, 2016

Disposição dos cubinhos das faces inferior e direita após aplicação de D:

Figura 12 – Cubinhos das faces inferior e direita

	l	l	l	
b	d	d	d	f
b	d	d	d	f
b	d	d	d	f
	r	r	r	

	u	u	u	
f	r	r	r	b
f	r	r	r	b
l	f	f	f	r
	d	d	d	

Fonte: o Autor, 2016

Ilustraremos todas as passagens desse exemplo. Para chegarmos até $DRD^{-1}R^{-1}$, que é $[D,R] = (dlf\ dfr\ lfd\ frd\ fdl\ rdf)(drb\ bru\ bdr\ ubr\ rbd\ rub)\ (dfdr\ br)$, seguiremos os passos a seguir:

- Faremos o movimento D.

  Figura 13 – Movimento D

movimento D front left

movimento D back right

(a) (b)

(c)

(d)

Legenda: (a) – faces frontal e esquerda; (b) – faces posterior e direita; (c) – face superior; (d) – face inferior.
Fonte: o Autor, 2016

- Em seguida faremos o movimento R, obtendo o movimento DR.

Figura 14 – Movimento DR

(a)

(b)

(c)

(d)

Legenda: (a) – faces frontal e esquerda; (b) – faces posterior e direita; (c) – face superior; (d) – face inferior.
Fonte: o Autor, 2016

- Agora, passemos para a terceira etapa e façamos o movimento D^{-1}. Assim teremos o movimento DRD^{-1}.

Figura 15 – Movimento DRD^{-1}

movimento D R D^{-1} front left

(a)

movimento D R D^{-1} right back

(b)

movimento D R D^{-1} up

(c)

movimento D R D^{-1} down

(d)

Legenda: (a) – faces frontal e esquerda; (b) – faces posterior e direita; (c) – face superior; (d) – face inferior.
Fonte: o Autor, 2016

- E por fim, concluímos com o movimento R^{-1}. Chegando assim, ao movimento $DRD^{-1}R^{-1}$.

Figura 16 – Movimento $DRD^{-1}R^{-1}$

movimento D R D^{-1} R^{-1} front left

(a)

movimento D R D^{-1} R^{-1} back right

(b)

movimento D R D^{-1} R^{-1} up

(c)

movimento D R D^{-1} R^{-1} down

(d)

Legenda: (a) – faces frontal e esquerda; (b) – faces posterior e direita; (c) – face superior; (d) – face inferior.
Fonte: o Autor, 2016

Comparando as configurações da Figura 16 com a configuração inicial (Figura 17), concluímos que no movimento $[D, R]$, temos $\sigma = (drb\; bru)(dfl\; dfr)$ e $\tau = (df\; dr\; br)$.

Figura 17 – Configuração Inicial

Fonte: o Autor, 2016

De fato, lembre que τ é um elemento de S_{12}; é uma bijeção do conjunto de 12 cubinhos borda não orientados para o conjunto de 12 cubículos borda. Ela é definida da seguinte maneira: se C é um cubinho borda não orientado na configuração inicial, então $\tau(C)$

é o cubículo borda não orientado em que C se encontra após a realização dos movimentos. Como qualquer elemento de S_{12}, τ é escrito em notação ciclos disjuntos.

Neste exemplo em particular, $[D, R]$ move cubinho df para cubículo dr, cubinho dr para cubículo br e cubinho br para cubículo df. Portanto, $\tau = (df\ dr\ br)$.

Da mesma forma, pensamos em σ como um bijeção do conjunto de 8 cubinhos canto não orientados para o conjunto de 8 cubículos canto não orientados. Para encontrar σ, devemos descobrir qual o efeito de $[D, R]$ sobre as posições dos cubinhos canto. Observe que $[D, R]$ muda as posições dos cubinhos dfl e dfr, e ele também muda as posições de drb e bru. Portanto, $\sigma = (drb\ bru)(dfl\ dfr)$.

Definimos x_i como o número da face do cubinho na face i do cubículo. Na posição inicial, todas as faces numeradas dos cubículos têm faces dos cubinhos numeradas com 0. Uma vez que o movimento $[D, R]$ não afeta cubinhos ufl, urf, ulb ou dbl, x_1, x_2, x_4 e x_5 devem ser 0. Para encontrar x_3, queremos ver qual face do cubinho está na face u do cubículo urb. Podemos ver a partir das Figuras 16 e 17 que $[D, R]$ coloca a face b do cubinho drb lá; pelo nosso esquema de numeração, a face b do cubinho drb é numerada com 2; Portanto, $x_3 = 2$. Do mesmo modo, $x_6 = 2$, $x_7 = 0$ e $x_8 = 2$. Assim, a 8-upla x é $(0, 0, 2, 0, 0, 2, 0, 2)$.

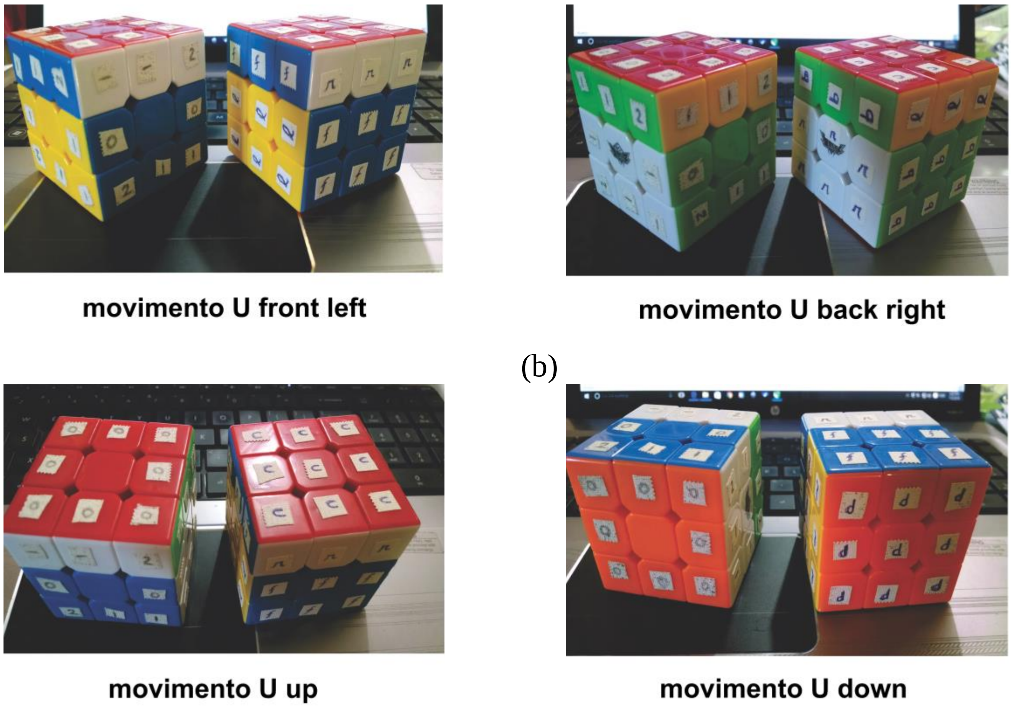
Da mesma forma, para definir y, lembramos que ele é a 12-upla $(y_1, \dots, y_{12})$, onde y_i é o número da face que se encontra no cubículo borda i. Uma vez que$[D, R]$ afeta apenas os cubinhos borda df, dr e br, sabemos imediatamente que y_{11}, y_{10} e y_6 são os únicos y_i que são diferentes de zero. Uma vez que $[D, R]$ coloca a face b do cubículo br na face d do cubículo df, $y_{11} = 0$. .Do mesmo modo, y_{10} e y_6 são ambos nulos. Assim, $y = (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$.

Você poderia se perguntar por que nos preocupamos em definir configurações do Cubo Mágico desta forma, uma vez que parece muito mais fácil obter as informações diretamente a partir de (6.1). A principal razão é que escrever σ, τ, x e y, separadamente, nos permite reconhecer padrões mais facilmente (e prová-los!).

Exemplo 6.6. Vamos mostrar como fica o movimento $[U, R]$.

- Começamos pelo movimento U.

Figura 18 – Movimento U

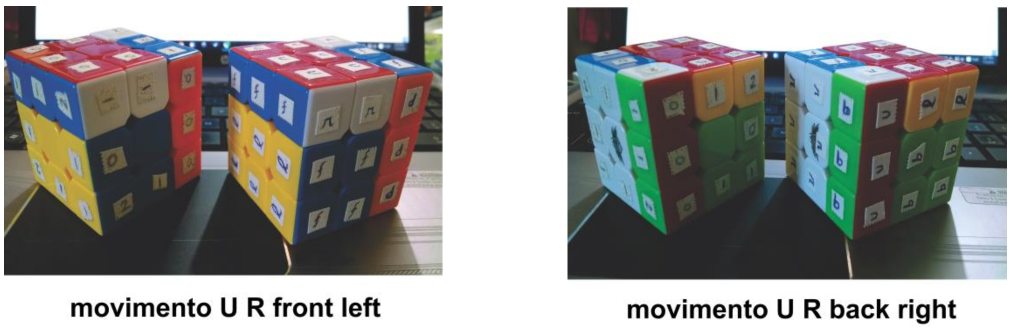


(a) (b) (c) (d)

Legenda: (a) – faces frontal e esquerda; (b) – faces posterior e direita; (c) – face superior; (d) – face inferior.
Fonte: o Autor, 2016

- Em seguida faremos o movimento R, obtendo o movimento UR.

Figura 19 – Movimento UR



(a) (b)

movimento U R up

(c)

movimento U R down

(d)

Legenda: (a) – faces frontal e esquerda; (b) – faces posterior e direita; (c) – face superior; (d) – face inferior.
Fonte: o Autor, 2016

- Agora, passemos para a terceira etapa e façamos o movimento U^{-1}. Assim teremos o movimento URU^{-1}.

Figura 20 – Movimento URU^{-1}

movimento U R U^{-1} front left

(a)

movimento U R U^{-1} back right

(b)

movimento U R U-1 up

(c)

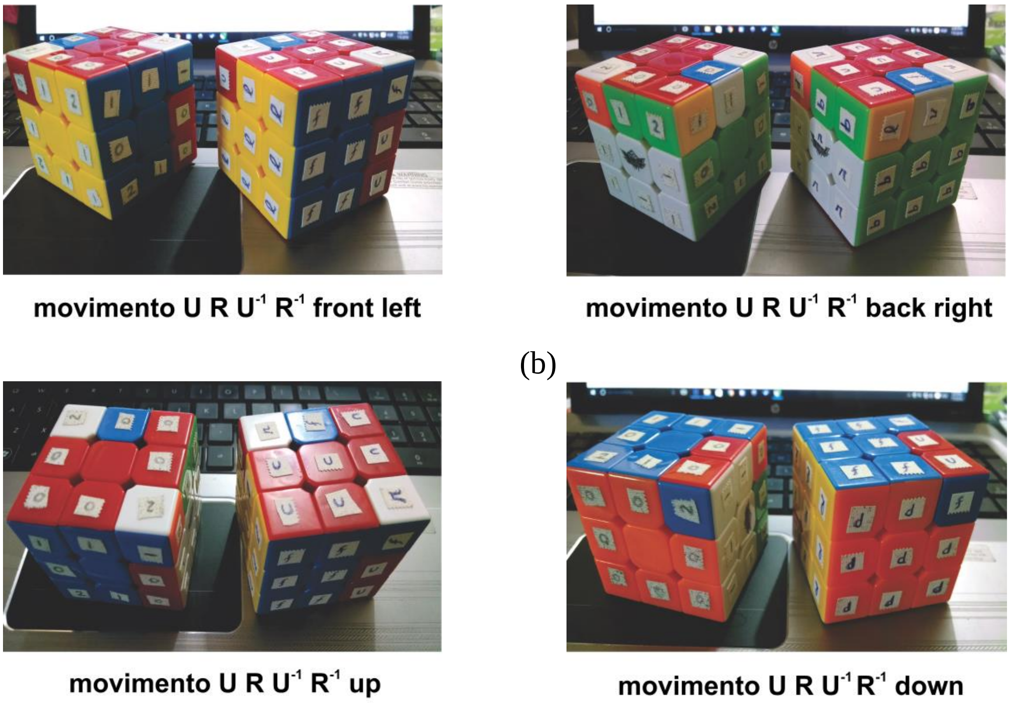
movimento U R U^{-1} down

(d)

Legenda: (a) – faces frontal e esquerda; (b) – faces posterior e direita; (c) – face superior; (d) – face inferior.
Fonte: o Autor, 2016

- E por fim, concluímos com o movimento R^{-1}. Chegando assim, ao movimento $URU^{-1}R^{-1}$.

Figura 21 – Movimento U$RU^{-1}R^{-1}$



(a) (b) (c) (d)

Legenda: (a) – faces frontal e esquerda; (b) – faces posterior e direita; (c) – face superior; (d) – face inferior.
Fonte: o Autor, 2016

Comparando as configurações da Figura 21 com a configuração inicial (Figura 17), concluímos que $[U,R] = (frd\ fur\ dfr\ rfu\ rdf\ urf)\ (rub\ ulb\ ubr\ lbu\ bru\ bul)\ (ub\ ur\ fr)$. Isso nos faz observar que dois pares de cubinhos canto permutam entre si, são eles frd e fur e o outro par é o rub e ulb. Assim como, também, temos a permutação dos cubinhos bordas ub, ur e fr entre si. Então, conforme o exercício anterior, podemos dizer que o movimento $[U,R]$ pode ser caracterizado como $\sigma = (rub\ ulb)(frd\ fur)$ e $\tau = (ub\ ur\ fr)$.

7 ANÁLISE DE UM MÉTODO DE RESOLUÇÃO DO CUBO MÁGICO

Muitas estratégias de resolução do Cubo Mágico foram desenvolvidas por praticantes e entusiastas desse passatempo. Em linhas gerais, elas podem ser classificadas em quatro grandes grupos de acordo o tipo de subproblema que é resolvido inicialmente em cada uma delas. Há estratégias que iniciam recolocando todos os cubinhos canto nas posições corretas, outras começam pelos cubinhos borda, outras trabalham por blocos $2 \times 2 \times 3$ e há as que resolvem o cubo por camadas. O tempo de resolução e a eficiência dos algoritmos de resolução podem ser melhorados através de novas sequências de movimentos e de modificações e ampliações do método básico (RUBIK *et al.,* 1987). Neste capítulo, descreveremos o método por camadas. Na prática, os movimentos básicos R, L, U, D, F e B não são realizados com as faces fixadas inicialmente. O cubo é girado e a cada momento os movimentos são realizados com as faces correspondentes. Para manter a coerência de notação, vamos apresentar o método das camadas mantendo a correspondência entre os movimentos básicos $R,\ L,\ U, D,\ F$ e Be as faces esquerda (l), inferior (d), superior (u), direita (r), frontal (f) e posterior (b). Partindo do cubo montando, convencionamos que a face vermelha é a face superior e que a face azul é a frontal.

7.1 Análise dos movimentos utilizados no método das camadas

Antes de descrever o método, vamos identificar quais alterações na configuração do cubo os movimentos utilizados no método promovem. Para cada um deles, vamos identificar as 4-uplas (σ, τ, x, y) correspondentes aos movimentos propostos e analisar quais foram as modificações no cubo a partir da configuração inicial do cubo resolvido.

Para determinar , vamos usar a configuração inicial (Figura 22) como referência.

Figura 22 – Configuração Inicial

Fonte: o Autor, 2016

1. $\boldsymbol{U^{-1}R}$

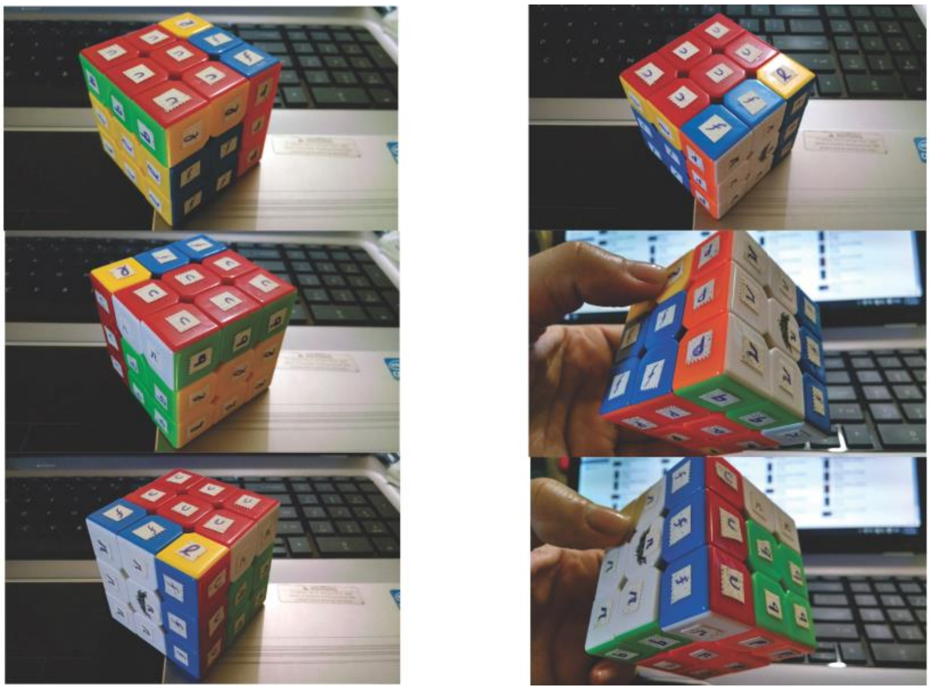
Nesse caso,

$$\sigma = (ulb\ ufl\ bru)(urf\ bdr\ dfr), \qquad \tau = (ur\ ub\ ul\ uf\ br\ dr\ fr),$$

$$x = (0\ 1\ 2\ 0\ 0\ 0\ 2\ 1), \quad y = (0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0).$$

Para entender a decomposição de σ, repare que há uma visão triangular em cada face movimentada com os cubinhos canto deslocados entre si. Na face superior temos os cubinhos canto ulb, ufl e bru que formam um triângulo e na face direita temos os cubinhos canto urf, bdr e dfr que também formam um triângulo. Na figura abaixo temos essa ilustração.

Figura 23 – Movimento $U^{-1}R$: σ



(a) (b)

Legenda: (a) – primeiro ciclo; (b) – segundo ciclo;
Fonte: o Autor, 2016

Na Figura 23(a), vemos que ao final do movimento,

- o cubinho canto ulb ocupa o cubículo ufl
- o cubinho canto bru ocupa o cubículo ulb
- o cubinho canto ufl ocupa o cubículo bru

caracterizando assim o ciclo $(ulb\, ufl\, bru)$ na decomposição de σ.

Na Figura 23(b), vemos que ao final do movimento,

- o cubinho canto dfr ocupa o cubículo urf
- o cubinho canto bdr ocupa o cubículo dfr
- o cubinho canto urf ocupa o cubículo dfr

caracterizando assim o ciclo $(urf\, bdr\, dfr)$ na decomposição de σ. Os demais cubinhos canto permaneceram em seus cubículos.

Agora, para τ temos $\tau = (ur\, ub\, ul\, uf\; br\, dr\, fr)$. Repare que todos os cubinhos borda das faces envolvidas mudaram de posições entre si formando um caminho com aspecto de “oito”.

Figura 24 – Movimento $U^{-1}R$: τ

Fonte: o Autor, 2016

Na Figura 24, vemos que ao final do movimento,

- o cubinho borda ur ocupa o cubículo ub
- o cubinho borda ub ocupa o cubículo ul
- o cubinho borda ul ocupa o cubículo uf
- o cubinho borda uf ocupa o cubículo br
- o cubinho borda br ocupa o cubículo dr
- o cubinho borda dr ocupa o cubículo fr
- o cubinho borda fr ocupa o cubículo ur

caracterizando assim o ciclo $(ur\ ub\ ul\ uf\ br\ dr\ fr)$ na decomposição de τ.

Temos $x = (0\ 1\ 2\ 0\ 0\ 0\ 2\ 1)$. De fato, na Figura 25, vemos que nas faces u e d somente houve alteração em x_2, x_3, x_7 e x_8. Agora a face numerada dos cubinhos que coincide com as faces numeradas dos cubículos são $x_2 = 1, x_3 = 2, x_7 = 2$ e $x_8 = 1$.

Figura 25 – Movimento $U^{-1}R$: x

Fonte: o Autor, 2016

Por fim, $y = (0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0)$. A Figura 26 nos mostra que nas faces u, f, b e d, as faces dos cubinhos borda que coincidem com as faces numeradas dos cubículos são todas numeradas com zero.

Figura 26 – Movimento $U^{-1}R$: y

Fonte: o Autor, 2016

2. RUF^{-1}

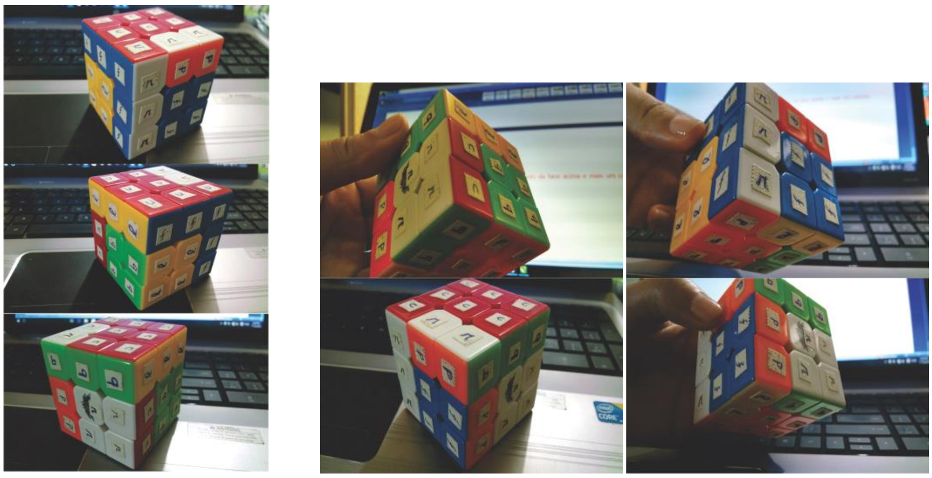
Nesse caso,

$$\sigma = (urf\ ufl\ ulb\ ubr\ bdr)(frd\ lfd), \qquad \tau = (uf\ ul\ ub\ ur\ br\ dr)(fd\ fr\ lf),$$

$$x = (0\ 1\ 0\ 0\ 0\ 0\ 1\ 1), \qquad y = (0\ 0\ 1\ 0\ 0\ 0\ 1\ 1\ 0\ 0\ 1\ 0).$$

Podemos notar que os cubinhos canto da face superior e mais um cubinho canto rbd trocam de posições entre si. Notamos também que os cubinhos frd e lfd trocam de posições entre si.

Figura 27 – Movimento RUF^{-1}: σ



(a) (b)

Legenda: (a) – primeiro ciclo; (b) – segundo ciclo;

Fonte: o Autor, 2016

Na Figura 27(a), vemos que ao final do movimento,

- o cubinho canto urf ocupa o cubículo ufl
- o cubinho canto ufl ocupa o cubículo ulb
- o cubinho canto ulb ocupa o cubículo ubr
- o cubinho canto ubr ocupa o cubículo bdr
- o cubinho canto bdr ocupa o cubículo urf

caracterizando assim o ciclo $(urf\ ufl\ ulb\ ubr\ bdr)$ na decomposição de σ.

Na Figura 27(b), vemos que ao final do movimento,

- o cubinho canto frd ocupa o cubículo lfd
- o cubinho canto lfd ocupa o cubículo frd

caracterizando assim o ciclo $(frd\ lfd)$ na decomposição de σ.

Agora, para τ temos $\tau = (uf\ ul\ ub\ ur\ br\ dr)(fd\ fr\ lf)$. Podemos observar que três cubinhos bordas da face superior trocam de posições entre si e o quarto ur vai para face direita, empurrando um cubinho da face direita para a face superior. Vemos também que três cubinhos bordas da face frontal trocam de posições entre si e o quarto fu, que havia trocado de posição na troca dos cubinhos bordas da face superior, abre espaço para o cubinho que veio da face direita na troca citada anteriormente.

Figura 28 – Movimento RUF^{-1}: τ

(a) (b)

Legenda: (a) – primeiro ciclo; (b) – segundo ciclo;

Fonte: o Autor, 2016

Na Figura 28(a), vemos que ao final do movimento,

- o cubinho borda dr ocupa o cubículo uf
- o cubinho borda uf ocupa o cubículo ul

- o cubinho borda ul ocupa o cubículo ub
- o cubinho borda ub ocupa o cubículo ur
- o cubinho borda ur ocupa o cubículo br
- o cubinho borda br ocupa o cubículo dr

caracterizando assim o ciclo $(uf\ ul\ ub\ ur\ br\ dr)$ na decomposição de τ.

Na Figura 28(b), vemos que ao final do movimento,

- o cubinho borda fd ocupa o cubículo fr
- o cubinho borda fr ocupa o cubículo lf
- o cubinho borda lf ocupa o cubículo fd

caracterizando assim o ciclo $(fd\ fr\ lf)$ na decomposição de τ.

Temos $x = (0\ 1\ 0\ 0\ 0\ 0\ 1\ 1)$. De fato, na Figura 29, vemos que nas faces u e d somente houve alteração em x_2, x_7 e x_8. Agora a face numerada dos cubinhos que coincide com as faces numeradas dos cubículos são $x_2 = 1$, $x_7 = 1$ e $x_8 = 1$.

Figura 29 – Movimento RUF^{-1}: x

Fonte: o Autor, 2016

Por fim, $y = (0\ 0\ 1\ 0\ 0\ 0\ 1\ 1\ 0\ 0\ 1\ 0)$. Na Figura 30, vemos que nas faces u, b, f e d, somente houve alteração em y_3, y_7, y_8 e y_{11}. Agora a face numerada dos cubinhos que coincide com as faces numeradas dos cubículos são $y_3 = 1$, $y_7 = 1, y_8 = 1$ e $y_{11} = 1$.

Figura 30 – Movimento RUF^{-1}: y

Fonte: o Autor, 2016

3. $\boldsymbol{L^{-1}U^{-1}L}$

Nesse caso,

$$\sigma = (rub\ ufl\ lfd\ fur), \qquad \tau = (uf\ ur\ ub\ fl),$$

$$x = (2\ 2\ 0\ 0\ 0\ 2\ 0\ 0), \qquad y = (0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0).$$

Repare que temos um aspecto triangular na face superior e um aspecto triangular na face frontal, com dois cubinhos canto em comum, ou seja, os dois cubinhos canto que estão nas duas faces em questão.

Figura 31 – Movimento $L^{-1}U^{-1}L$: σ

Fonte: o Autor, 2016

Na Figura 31, vemos que ao final do movimento,

- o cubinho canto rub ocupa o cubículo ufl
- o cubinho canto ufl ocupa o cubículo lfd
- o cubinho canto lfd ocupa o cubículo fur
- o cubinho canto fur ocupa o cubículo rub

caracterizando assim o ciclo $(rub\, ufl\, lfd\, fur)$ na decomposição de σ. Os demais cubinhos canto permaneceram em seus cubículos.

Agora, para τ temos $\tau = (uf\ ur\ ub\ fl)$. Temos três cubinhos borda da face superior trocando de posições com um cubinho borda da face esquerda com a face frontal.

Figura 32 – Movimento $L^{-1}U^{-1}L$: τ

Fonte: o Autor, 2016

Na Figura 32, vemos que ao final do movimento,

- o cubinho borda uf ocupa o cubículo ur
- o cubinho borda ur ocupa o cubículo ub
- o cubinho borda ub ocupa o cubículo fl

- o cubinho borda fl ocupa o cubículo uf

caracterizando assim o ciclo $(uf\ ur\ ub\ fl)$ na decomposição de τ. Os demais cubinhos borda permanecem em seus cubículos.

Temos $x = (2\ 2\ 0\ 0\ 0\ 2\ 0\ 0)$. De fato, na Figura 33, vemos que nas faces u e d somente houve alteração em x_1, x_2 e x_6. Agora a face numerada dos cubinhos que coincide com as faces numeradas dos cubículos são $x_1 = 2, x_2 = 2$ e $x_6 = 2$.

Figura 33 – Movimento $L^{-1}U^{-1}L$: x

Fonte: o Autor, 2016

Por fim, $y = (0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0)$. A Figura 34 nos mostra que nas faces u, f, b e d, as faces dos cubinhos borda que coincidem com as faces numeradas dos cubículos são todas numeradas com zero.

Figura 34 – Movimento $L^{-1}U^{-1}L$: y

Fonte: o Autor, 2016

4. $\boldsymbol{RUR^{-1}}$

Nesse caso,

$$\sigma = (frd\ ufl\ ulb\ fur), \qquad \tau = (fr\ uf\ ul\ ub),$$

$$x = (1\ 1\ 0\ 0\ 0\ 0\ 1\ 0), \qquad y = (0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0).$$

Nesse caso, $\sigma = (frd\ ufl\ ulb\ fur)$. Repare que há trocas de posições de três cubinhos canto da face superior, formando um aspecto triangular, com um cubinho canto que se localiza na face inferior com a face direita com a face frontal, formado outro aspecto triangular na face frontal.

Figura 35 – Movimento RUR^{-1}: σ

Fonte: o Autor, 2016

Na Figura 35, vemos que ao final do movimento,

- o cubinho canto frd ocupa o cubículo ufl
- o cubinho canto ufl ocupa o cubículo ulb
- o cubinho canto ulb ocupa o cubículo fur
- o cubinho canto fur ocupa o cubículo frd

caracterizando assim o ciclo $(frd\,ufl\,ulb\,fur)$ na decomposição de σ. Os demais cubinhos canto permaneceram em seus cubículos.

Agora, para τ temos, $\tau = (fr\ uf\ ul\ ub)$, notamos que há trocas de posições entre três cubinhos borda da face superior com um cubinho borda da face frete com a face direita.

Figura 36 – Movimento RUR^{-1}: τ

Fonte: o Autor, 2016

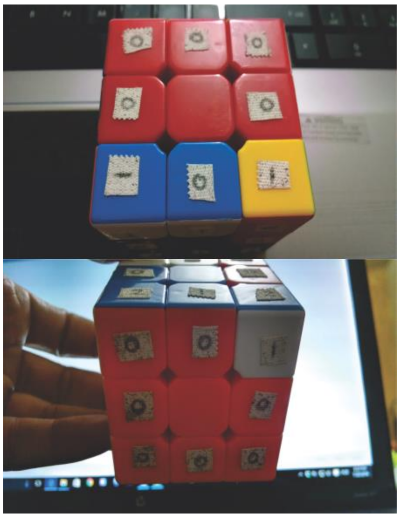
Na Figura 36, vemos que ao final do movimento,

- o cubinho borda fr ocupa o cubículo uf
- o cubinho borda uf ocupa o cubículo ul
- o cubinho borda ul ocupa o cubículo ub
- o cubinho borda ub ocupa o cubículo fr

caracterizando assim o ciclo $(fr\ uf\ ul\ ub)$ na decomposição de τ.

Temos $x = (1\ 1\ 0\ 0\ 0\ 0\ 1\ 0)$. De fato, na Figura 37, vemos que nas faces u e d somente houve alteração em x_1, x_2 e x_7. Agora a face numerada dos cubinhos que coincide com as faces numeradas dos cubículos são $x_1 = 1, x_2 = 1$ e $x_7 = 1$.

Figura 37 – Movimento RUR^{-1}: x



Fonte: o Autor, 2016

Por fim, $y = (0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0)$. A Figura 38 nos mostra que nas faces u, f, b e d, as faces dos cubinhos borda que coincidem com as faces numeradas dos cubículos são todas numeradas com zero.

Figura 38 – Movimento RUR^{-1}: y

Fonte: o Autor, 2016

5. $\boldsymbol{RU^2R^{-1}U^{-1}}$

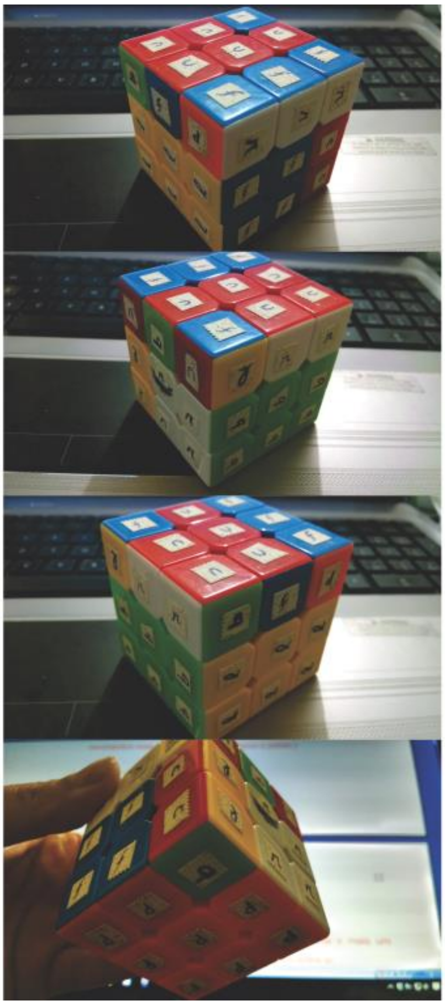
Nesse caso,

$$\sigma = (frd\ ufl\ rub\ bul), \qquad \tau = (fr\ uf\ ul)(ub\ ur),$$

$$x = (1\ 2\ 1\ 0\ 0\ 0\ 2\ 0), \qquad y = (0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0).$$

Nesse caso, $\sigma = (frd\ ufl\ rub\ bul)$. Repare que teremos três cubinhos canto da face superior e mais um cubinho canto da face inferior trocando de posições entre si.

Figura 39 – Movimento $RU^2R^{-1}U^{-1}$: σ



Fonte: o Autor, 2016

Na Figura 39 vemos que ao final do movimento,

- o cubinho canto frd ocupa o cubículo ufl
- o cubinho canto ufl ocupa o cubículo rub
- o cubinho canto rub ocupa o cubículo bul
- o cubinho canto bul ocupa o cubículo frd

caracterizando assim o ciclo $(frd\ ufl\ rub\ bul)$ na decomposição de σ. Os demais cubinhos canto permaneceram em seus cubículos.

Agora, para τ temos $\tau = (fr\ uf\ ul)(ub\ ur)$. Dois cubinhos borda da face superior e um cubinho borda das faces frontal e direita traçando de posições entre si. Temos, também, dois cubinhos borda da face superior trocando de posições entre si

Figura 40 – Movimento $RU^2R^{-1}U^{-1}$: τ

(a) (b)

Legenda: (a) – primeiro ciclo; (b) – segundo ciclo;

Fonte: o Autor, 2016

Na Figura 40(a), vemos que ao final do movimento,

- o cubinho borda fr ocupa o cubículo uf
- o cubinho borda uf ocupa o cubículo ul
- o cubinho borda ul ocupa o cubículo fr

caracterizando assim o ciclo $(fr\ uf\ ul)$ na decomposição de τ.

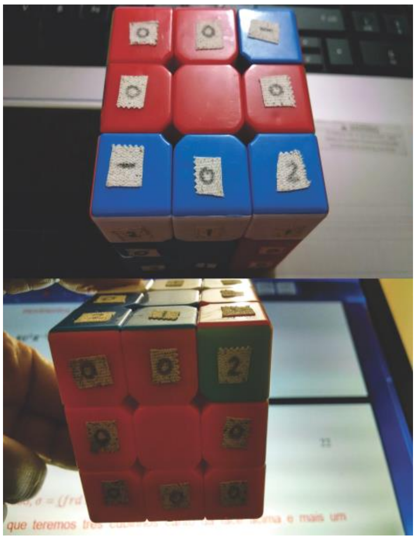
Na Figura 40(b), vemos que ao final do movimento,

- o cubinho borda ub ocupa o cubículo ur
- o cubinho borda ur ocupa o cubículo ub

caracterizando assim o ciclo $(ub\ ur)$ na decomposição de τ. Os demais cubinhos borda permaneceram em seus cubículos.

Temos $x = (1\ 2\ 1\ 0\ 0\ 0\ 2\ 0)$. De fato, na Figura 41, vemos que nas faces u e d somente houve alteração em x_1, x_2, x_3 e x_7. Agora a face numerada dos cubinhos que coincide com as faces numeradas dos cubículos são $x_1 = 1, x_2 = 2, x_2 = 1$ e $x_7 = 2$.

Figura 41 – Movimento $RU^2R^{-1}U^{-1}$: x



Fonte: o Autor, 2016

Por fim, $y = (0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0)$. A Figura 42 nos mostra que nas faces u, f, b e d, as faces dos cubinhos borda que coincidem com as faces numeradas dos cubículos são todas numeradas com zero.

Figura 42 – Movimento $RU^2R^{-1}U^{-1}$: y

Fonte: o Autor, 2016

6. $\boldsymbol{URU^{-1}R^{-1}U^{-1}F^{-1}UF}$

Nesse caso,

$$\sigma = (rub\ ufl\ bul), \quad \tau = (ul\ uf\ rf\ bu\ ru),$$

$$x = (2\ 0\ 0\ 1\ 0\ 0\ 0\ 0), \qquad y = (0\ 0\ 0\ 1\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 0).$$

Nesse caso, $\sigma = (rub\ ufl\ bul)$. Notemos que nesse movimento, três cubinhos canto da face superior trocam de posições entre si.

Figura 43 – Movimento $URU^{-1}R^{-1}U^{-1}F^{-1}UF$: σ

Fonte: o Autor, 2016

Na Figura 43, vemos que ao final do movimento,

- o cubinho canto rub ocupa o cubículo ufl
- o cubinho canto ufl ocupa o cubículo bul
- o cubinho canto bul ocupa o cubículo rub

caracterizando assim o ciclo $(rub\ ufl\ bul)$ na decomposição de σ. Os demais cubinhos canto permaneceram em seus cubículos.

Agora, para τ temos $\tau = (ul\ uf\ rf\ bu\ ru)$. Verificamos que os quatro cubinhos borda da face superior e mais um cubinho borda das faces frontal e direita trocam de posições.

Figura 44 – Movimento $URU^{-1}R^{-1}U^{-1}F^{-1}UF$: τ

Fonte: o Autor, 2016

Na Figura 44, vemos que ao final do movimento,

- o cubinho borda ul ocupa o cubículo uf
- o cubinho borda uf ocupa o cubículo rf
- o cubinho borda rf ocupa o cubículo bu
- o cubinho borda bu ocupa o cubículo ru
- o cubinho borda ru ocupa o cubículo ul

caracterizando assim o ciclo $(ul\ uf\ rf\ bu\ ru)$ na decomposição de τ.

Temos $x = (2\ 0\ 0\ 1\ 0\ 0\ 0\ 0)$. De fato, na Figura 45, vemos que nas faces u e d somente houve alteração em x_2, x_3, x_7 e x_8. Agora a face numerada dos cubinhos que coincide com as faces numeradas dos cubículos são $x_2 = 1, x_3 = 2, x_7 = 2$ e $x_8 = 1$.

Figura 45 – Movimento $URU^{-1}R^{-1}U^{-1}F^{-1}UF$: x

Fonte: o Autor, 2016

Por fim, $y = (0\ 0\ 0\ 1\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 0)$. Na Figura 46, vemos que nas faces u, b, f e d, somente houve alteração em y_4 e y_7. Agora a face numerada dos cubinhos que coincide com as faces numeradas dos cubículos são $y_4 = 1$ e $y_7 = 1$.

Figura 46 – Movimento $URU^{-1}R^{-1}U^{-1}F^{-1}UF$: y

Fonte: o Autor, 2016

7. $\boldsymbol{U^{-1}L^{-1}ULUFU^{-1}F^{-1}}$

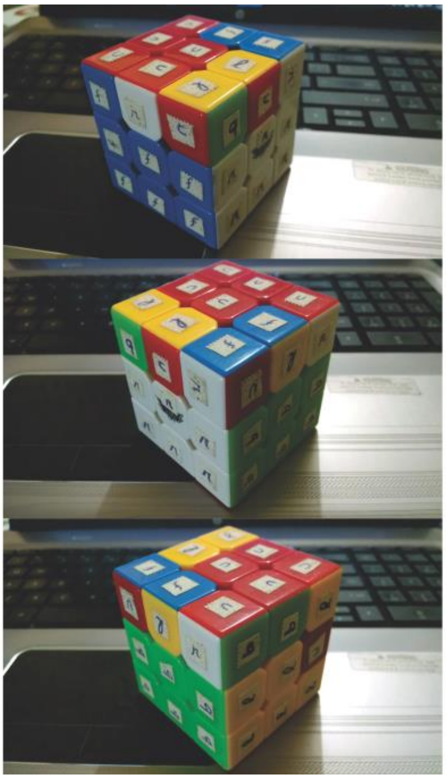
Nesse caso,

$$\sigma = (lbu\ urf\ bru), \quad \tau = (ur\ uf\ lf\ bu\ lu),$$

$$x = (0\ 1\ 2\ 0\ 0\ 0\ 0\ 0), \qquad y = (0\ 1\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0).$$

Nesse caso, $\sigma = (lbu\ urf\ bru)$. Repare que três cubinhos canto da face superior trocam de posições entre si.

Figura 47 – Movimento $U^{-1}L^{-1}ULUFU^{-1}F^{-1}$: σ



Fonte: o Autor, 2016

Na Figura 47, vemos que ao final do movimento,

- o cubinho canto lbu ocupa o cubículo urf
- o cubinho canto urf ocupa o cubículo bru
- o cubinho canto bru ocupa o cubículo lbu

caracterizando assim o ciclo $(lbu\, urf\ bru)$ na decomposição de σ. Os demais cubinhos canto permaneceram em seus cubículos.

Agora, para τ temos $\tau = (ur\ uf\ lf\ bu\ lu)$. Vemos que os quatro cubinhos borda da face superior e mais um cubinho borda das faces frontal e esquerda trocam de posições entre si.

Figura 48 – Movimento $U^{-1}L^{-1}ULUFU^{-1}F^{-1}$: τ

Fonte: o Autor, 2016

Na Figura 48, vemos que ao final do movimento,

- o cubinho borda ur ocupa o cubículo uf
- o cubinho borda uf ocupa o cubículo lf
- o cubinho borda lf ocupa o cubículo bu
- o cubinho borda bu ocupa o cubículo lu
- o cubinho borda lu ocupa o cubículo ur

caracterizando assim o ciclo $(ur\ uf\ lf\ bu\ lu)$ na decomposição de τ.

Temos $x = (0\ 1\ 2\ 0\ 0\ 0\ 0\ 0)$. De fato, na Figura 49, vemos que nas faces u e d somente houve alteração em x_2 e x_3. Agora a face numerada dos cubinhos que coincide com as faces numeradas dos cubículos são $x_2 = 1$ e $x_3 = 2$.

Figura 49 – Movimento $U^{-1}L^{-1}ULUFU^{-1}F^{-1}$: x

Fonte: o Autor, 2016

Por fim, $y = (0\ 1\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0)$. Na Figura 50, vemos que nas faces u, b, f e d, somente houve alteração em y_2 e y_8. Agora a face numerada dos cubinhos que coincide com as faces numeradas dos cubículos são $y_2 = 1$ e $y_8 = 1$.

Figura 50 – Movimento $U^{-1}L^{-1}ULUFU^{-1}F^{-1}$: y

Fonte: o Autor, 2016

7.2 **Método das camadas**

A descrição aqui apresentada do método das camadas foi adaptada da feita por Renan Cerpe[2]. O método está dividido em oito passos. As figuras são apenas exemplos. É importante entender os movimentos e aplicar as fórmulas de acordo com as situações do cubo que será resolvido.

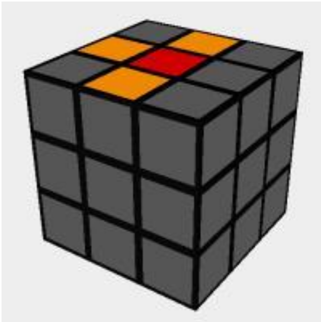
7.1.1 Primeiro passo – Cruz Laranja

No primeiro passo deste método, vamos iniciar com uma cruz com os quatro cubinhos borda laranjas ao redor do centro vermelho, ou seja, ignore os cubinhos canto laranja e os demais cubinhos.

Vamos analisar as possibilidades de colocação do último cubinho da cruz. Tomando como ponto de partida a configuração ilustrada na Figura 51.

[2]http://www.cubovelocidade.com.br/tutoriais/cubo-magico-basico-metodo-camadas-1-passo-cruz-branca.html, acessado em 01 de julho de 2016. As figuras foram geradas com o Rubik'simagegenerator disponível em https://ruwix.com/online-rubiks-cube-solver-program/, acessado em 01 de julho de 2016.

Figura 51 – Cruz Laranja: início

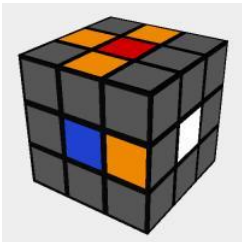


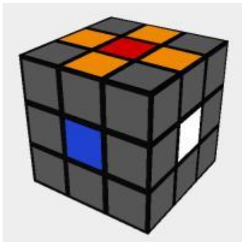
Fonte: o Autor, 2016

Há quatro situações a serem consideradas

1. **Movimento $\boldsymbol{R}$** – Este é o caso mais simples, onde um cubinho borda laranja está na face f do cubo e logo acima existe um "espaço vazio". (Figura 52(a)). Neste caso, realize o movimento R. Caso o cubinho borda laranja esteja na face inferior d, realize o movimento R^2 (Figura 52(b)).

Figura 52 – Cruz Laranja: caso 1





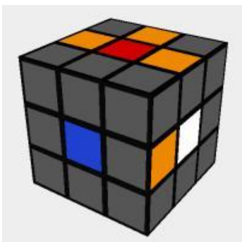
(a) (b)

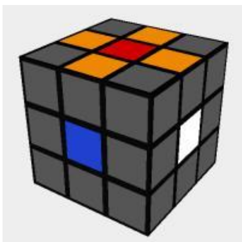
Legenda: (a) – cruz incompleta; (b) – cruz completa.

Fonte: o Autor, 2016

2. **Movimento $\boldsymbol{F^{-1}}$**– Neste caso nós temos um cubinho borda laranja na lateral direita do cubo e um "espaço vazio" logo a sua frente (Figura 53(a)). Basta realizar o movimento F^{-1}. Caso o cubinho borda laranja esteja na base do cubo, realize o movimento F^2 (Figura 53(b)).

Figura 53 – Cruz Laranja: caso 2



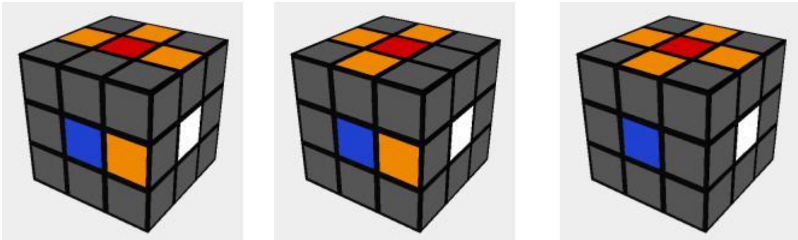


(a) (b)

Legenda: (a) – cruz incompleta; (b) – cruz completa.
Fonte: o Autor, 2016

3. **Movimento $\boldsymbol{U^{-1}R}$** – Agora antes de simplesmente “subir” o cubinho borda laranja que está na frente do cubo para o topo, é preciso alinha um “espaço vazio” na direção deste cubinho borda (Figura 54(a)). Neste exemplo, vamos usar o movimento U^{-1} para alinhar o “espaço vazio” com o cubinho borda laranja (Figura 53(a)). Feito isso, basta fazer o movimento R. (Figura 54(b)).

Figura 54 – Cruz Laranja: caso 3

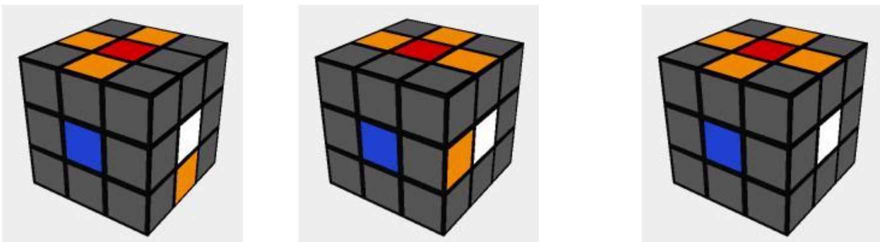


(a) (b)

Legenda: (a) – cruz incompleta; (b) – cruz completa.
Fonte: o Autor, 2016

4. **Movimento $\boldsymbol{RUF^{-1}}$**–No ponto de partida desse último caso, o “espaço vazio da cruz” deve estar em cima do cubinho borda laranja (Figura 55(a)). Execute o movimento R para reposicionar este cubinho borda laranja na lateral do cubo. Realize o movimento U para alinhar o “espaço vazio” com cubinho borda laranja da lateral (Figura 55(a)), e por fim, o movimento F^{-1} para posicionar o cubinho borda laranja no topo do cubo (Figura 55(a)).

Figura 55 – Cruz Laranja: caso 4



(a) (b)

Legenda: (a) – cruz incompleta; (b) – cruz completa.

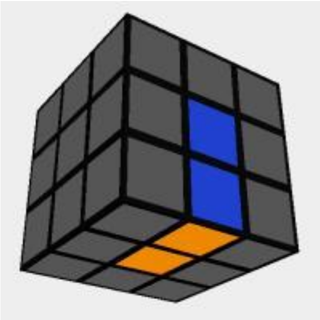
Fonte: o Autor, 2016

7.1.2 Segundo passo – Alinhar a Cruz Laranja

No primeiro passo, a cruz foi solucionada ao redor do centro vermelho e nós levamos em consideração apenas a cor laranja de cada um dos quatro cubinhos borda.

Cada cubinho borda possui duas cores. Neste passo, nós vamos alinhar a segunda cor de cada cubinho borda laranja ao redor do centro laranja (na base do cubo), para obter o seguinte resultado:

Figura 56 – Alinhamento da Cruz Laranja



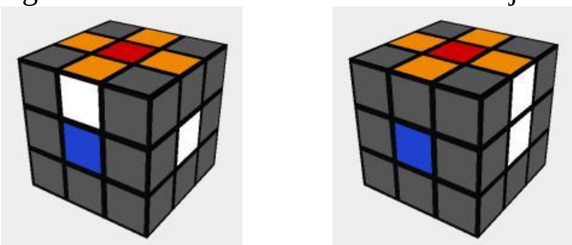
Fonte: o Autor, 2016

Perceba que o cubinho borda laranja/azul está fazendo ligação entre os centros laranja e azul. O mesmo deve acontecer para todos os cubinhos borda.

Este passo está dividido em duas etapas.

1. **Movimento $\boldsymbol{U}$**– Escolha qualquer um dos cubinhos borda laranja para começar e movimente a face vermelha com o movimento U, U^{-1} ou U^2 até que a segunda cor deste cubinho borda escolhido se alinhe com o centro correspondente na lateral do cubo. A figura ilustra a escolha do cubinho borda laranja/branco (Figura 57(a)). Como ele está alinhado com o centro azul, vamos movimentar a face superior do cubo com o movimento U^{-1} para que cubinho borda laranja/branco se alinhe com o centro branco (Figura 57(b)).

Figura 57 – Alinhamento da Cruz Laranja: etapa 1



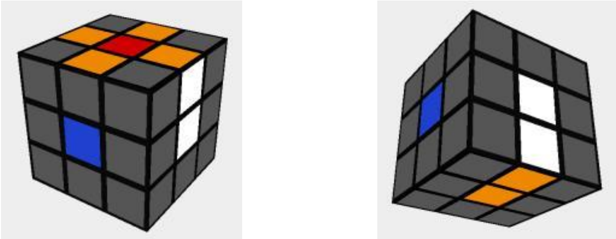
(a) (b)

Legenda: (a) – início; (b) – alinhado.
Fonte: o Autor, 2016

2. **Movimento $\boldsymbol{R^2}$** – o segundo movimento terá como objetivo levar o cubinho borda que você acabou de alinhar na primeira etapa para a base do cubo. No nosso exemplo, basta executar o movimento R^2. Assim, a cor laranja vai sair da face superior (Figura

58(a)) e ir para a base do cubo, e a outra cor deste cubinho borda (branca, nesse caso) continuará alinhada (Figura 58(b)).

Figura 58 – Alinhamento da Cruz Laranja: etapa 2



(a) (b)

Legenda: (a) – início; (b) – alinhado.

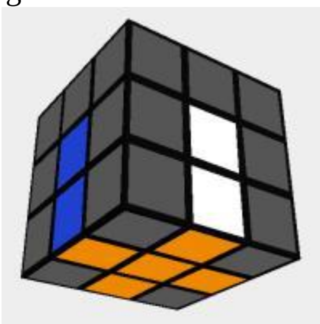
Fonte: o Autor, 2016

Agora basta você executar estas duas etapas para cada um dos quatro cubinhos borda laranja até que todos fiquem corretamente alinhados em relação ao centro laranja na base, e claro, as cores das laterais também devem estar alinhadas com os centros correspondentes.

7.1.3 <u>Terceiro passo – Camada Laranja</u>

Neste passo, nós vamos finalizar a camada laranja. Como a cruz laranja já está completa na base do cubo, as peças que faltam são os cubinhos canto laranjas, conforme pode ser observado na Figura 59.

Figura 59 – Camada Laranja



Fonte: o Autor, 2016

Observe que, ao final deste passo, vamos preencher toda a base do cubo com peças laranjas, e as laterais devem estar completamente corretas em relação à cor dos centros de cada face.

Este passo está dividido em quatro etapas.

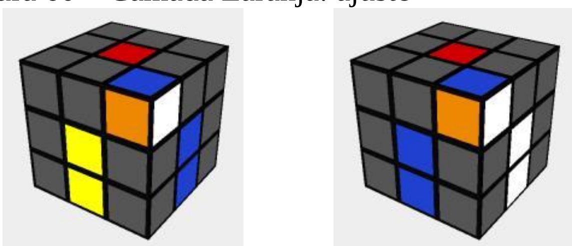
1. mantendo a cruz na base, encontre um cubinho canto laranja que esteja na camada do topo do seu cubo (caso você não encontre, pule as próximas etapas e verifique o caso “cubinho canto laranja na base”).
2. confira as cores do cubinho canto que você encontrou na primeira etapa, e identifique o lugar em que ele deverá ser encaixado com a ajuda dos três centros correspondentes.

3. execute o movimento U, U^{-1} ou U^2, até que cubinho canto laranja fique em cima do lugar em que ele deverá entrar.
4. veja em qual das três situações possíveis o seu cubo ficou e aplique o movimento correspondente.

   Cada situação será ilustrada através de um exemplo.

- **Posicionamento correto do cubinho canto** – Considere o cubinho canto laranja/azul/branco (Figura 60(a)). A posição correta desse cubinho na camada de base é determinada pelos cubinhos centro branco, azul e laranja. Nesse caso, vamos movimentar a face superior até posicionar esse cubinho canto em um cubículo canto associado a cubinhos centro branco e azul. No caso, basta fazer o movimento U^{-1}. Observe que a faceta laranja do cubinho canto está à esquerda da face em que a cor da faceta do cubinho canto coincide com a cor do cubinho centro. No exemplo, a cor branca. Essa configuração será chamada de "Cubinho canto na esquerda" (Figura 60(b)).

Figura 60 – Camada Laranja: ajuste



(a) (b)

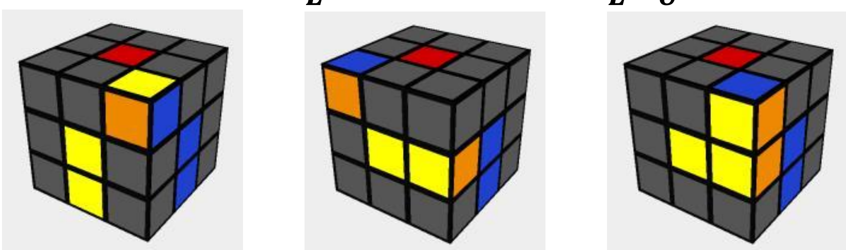
Legenda: (a) – início; (b) – posição correta.
Fonte: o Autor, 2016

Confira os quatro movimentos para as possíveis posições das quinas brancas:

- **Cubinho canto na esquerda ($L^{-1}U^{-1}L$)**

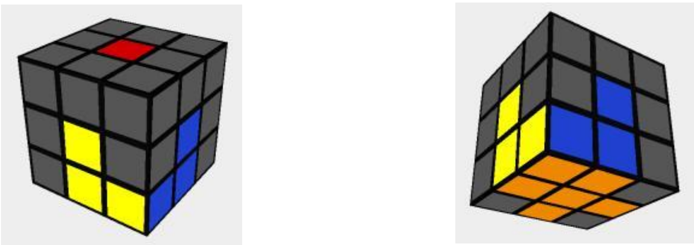
Figura 61 – Camada Laranja: situação 1

$\boldsymbol{L^{-1}}$ $\boldsymbol{L^{-1}U^{-1}}$



(a) (b) (c)

$L^{-1}U^{-1}L$



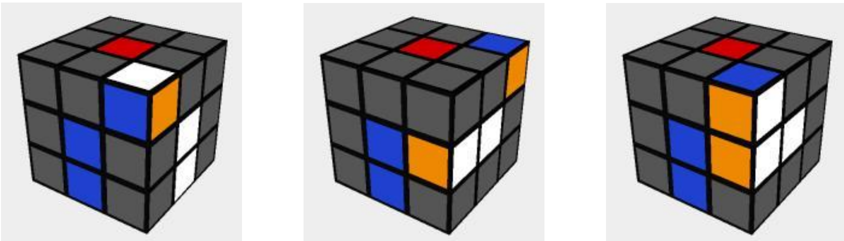
(d) (e)

Legenda: (a) – esquerda; (b), (c) e (d) – movimentação; (e) – movimento completo.
Fonte: o Autor, 2016

- **Cubinho canto na direita (RUR^{-1})**

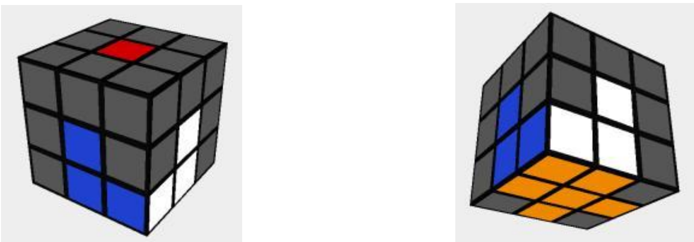
Figura 62 – Camada Laranja: situação 2

R RU



(a) (b) (c)

RUR^{-1}



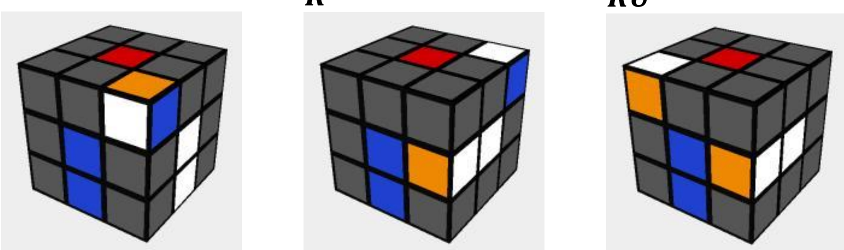
(d) (e)

Legenda: (a) – direita; (b), (c) e (d) – movimentação; (e) – movimento completo.
Fonte: o Autor, 2016

- **Cubinho canto no topo ($RU^2R^{-1}U^{-1}RUR^{-1}$)**

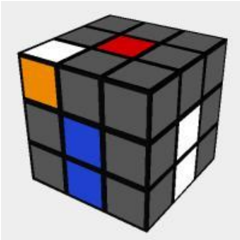
Figura 63 – Camada Laranja: situação 3

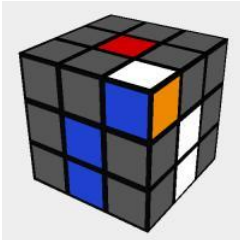
R RU^2



(a) (b) (c)

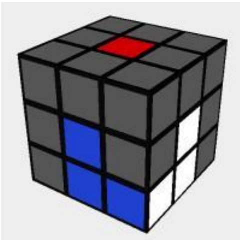
RU^2R^{-1} $RU^2R^{-1}U^{-1}$

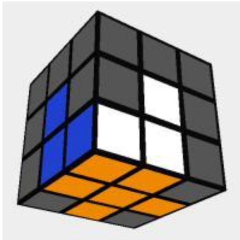




(d) (e)

$RU^2R^{-1}U^{-1}RUR^{-1}$





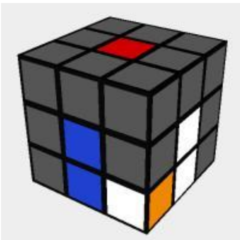
(f) (g)

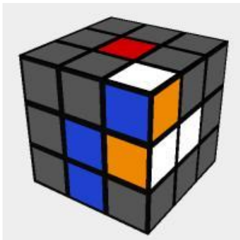
Legenda: (a) – topo; (b) a (f) – movimentação; (g) – movimento completo.
Fonte: o Autor, 2016

- **Cubinho canto na base (RUR^{-1})**

Figura 64 – Camada Laranja: base

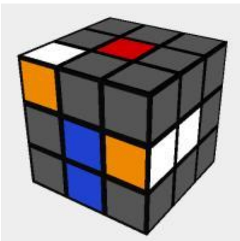
R

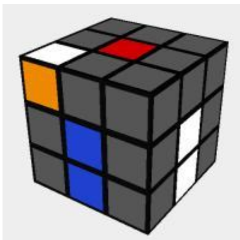




(a) (b)

RU RUR^{-1}





(c) (d)

Legenda: (a) – base; (b) a (d) – movimentação.
Fonte: o Autor, 2016

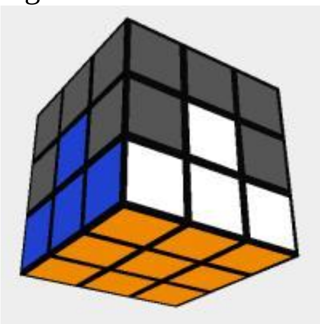
No caso “Cubinho canto na base”, o objetivo do movimento proposto é apenas posicionar o cubinho na camada superior. Depois de aplicado o movimento RUR^{-1}, é preciso recair em dos três casos apresentados e aplicar novamente o movimento correspondente. Nesse exemplo, basta fazer U^{-1} que recaímos no caso "cubinho canto na direita".

Figura 65 – Camada Laranja: corrigido

Fonte: o Autor, 2016

Realize as quatro etapas citadas acima para cada um dos quatro cubinhos canto que vão completar a camada laranja.

Figura 66 – Camada Laranja



Fonte: o Autor, 2016

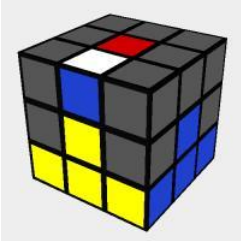
7.1.4 Quarto passo – Segunda Camada

Neste passo, vamos finalizar a camada do meio do cubo. Como a camada laranja já está completa, as peças que faltam para completar este passo são os cubinhos borda da segunda camada.

Este passo está dividido em duas etapas.

- procure no topo do cubo por cubinhos borda que não tenham a cor vermelha. Por exemplo, considere o cubinho borda azul/branco no topo do cubo.

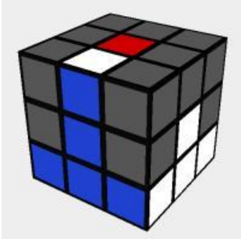
Figura 67 – Segunda Camada: etapa 1



Fonte: o Autor, 2016

- aplique o movimento U, U^{-1} ou U^2 até alinhar a cor da lateral deste cubinho borda com a do cubinho centro correspondente. Neste exemplo, a cor da lateral do cubinho borda é azul, sendo assim, é preciso girar o topo até que esta faceta azul se alinhe com o centro azul.

Figura 68 – Segunda Camada: etapa 2

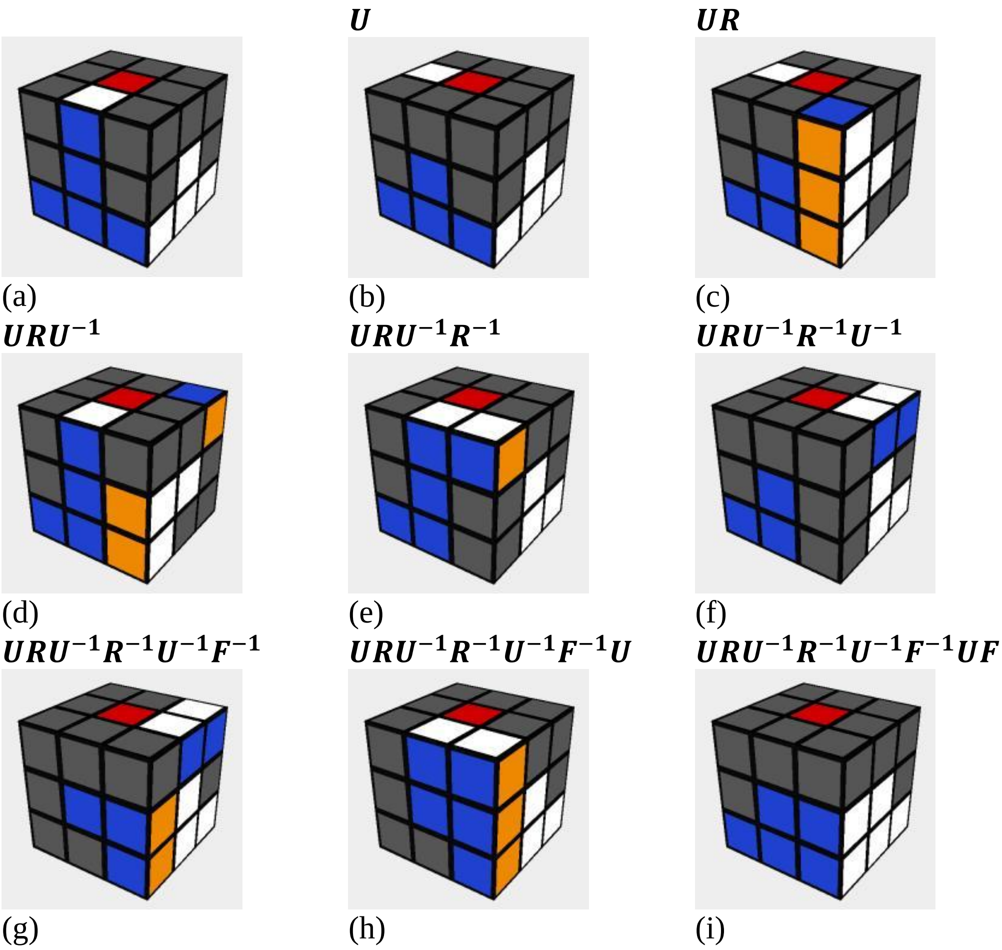


Fonte: o Autor, 2016

Confira os dois movimentos para as possíveis posições dos cubinhos borda no topo do cubo:

- **Cubinho borda para direita ($URU^{-1}R^{-1}U^{-1}F^{-1}UF$)**

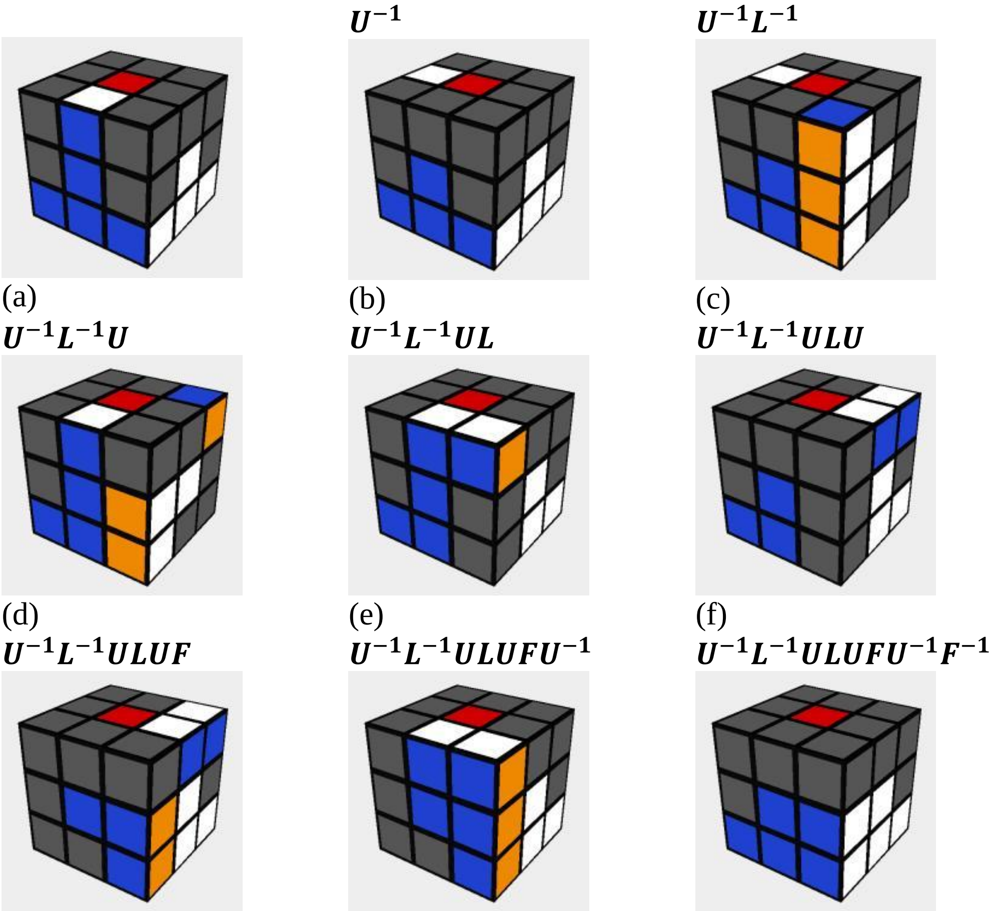
Figura 69 – Segunda Camada: movimento 1



Legenda: (a) – direita; (b) a (i) – movimentação.
Fonte: o Autor, 2016

- **Cubinho borda para esquerda ($U^{-1}L^{-1}ULUFU^{-1}F^{-1}$)**

Figura 70 – Segunda Camada: movimento 2



(a); (b) U^{-1}; (c) $U^{-1}L^{-1}$

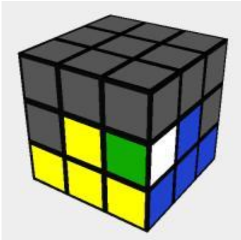
(d) $U^{-1}L^{-1}U$; (e) $U^{-1}L^{-1}UL$; (f) $U^{-1}L^{-1}ULU$

(g) $U^{-1}L^{-1}ULUF$; (h) $U^{-1}L^{-1}ULUFU^{-1}$; (i) $U^{-1}L^{-1}ULUFU^{-1}F^{-1}$

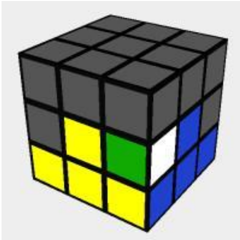
Legenda: (a) – esquerda; (b) a (i) – movimentação.
Fonte: o Autor, 2016

- **Cubinho borda já na segunda** – Caso o cubinho borda já esteja na segunda camada, porém, na posição errada, é preciso levá-lo para o topo. Vamos ilustrar como usar o caso “Cubinho borda para a esquerda” para que este cubinho borda errado seja removido. Feito isso, você deve voltar e realizar um dos dois casos já apresentados.

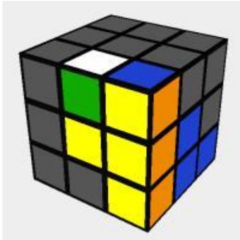
Figura 71 – Segunda Camada: na segunda


(a)

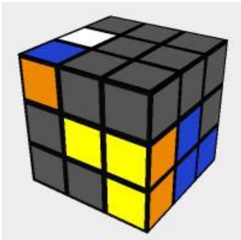
U^{-1}


(b)

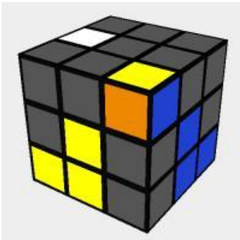
$U^{-1}L^{-1}$


(c)

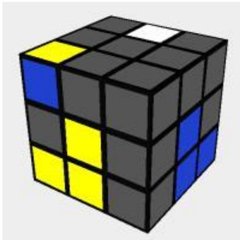
$U^{-1}L^{-1}U$


(d)

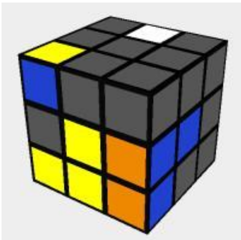
$U^{-1}L^{-1}UL$


(e)

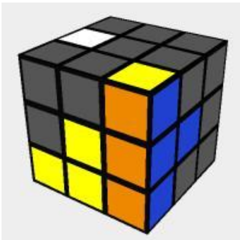
$U^{-1}L^{-1}ULU$


(f)

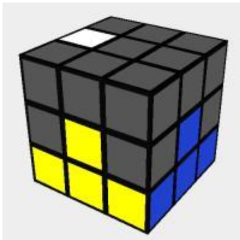
$U^{-1}L^{-1}ULUF$


(g)

$U^{-1}L^{-1}ULUFU^{-1}$


(h)

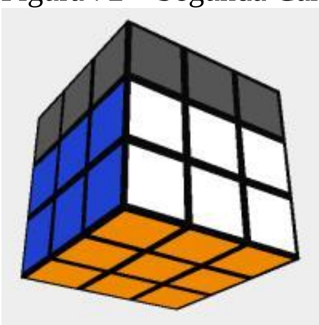
$U^{-1}L^{-1}ULUFU^{-1}F^{-1}$


(i)

Legenda: (a) – na segunda; (b) a (i) – movimentação.
Fonte: o Autor, 2016

Realize as duas etapas para cada um dos quatro cubinhos borda que vão completar a segunda camada do cubo.

Figura 72 – Segunda Camada



Fonte: o Autor, 2016

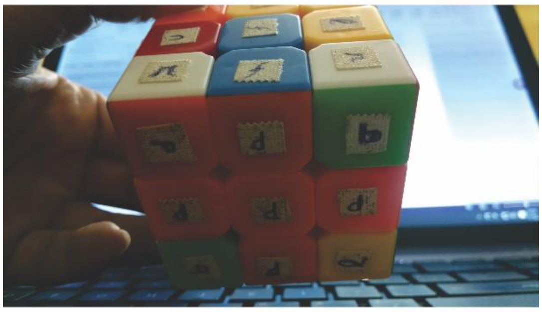
7.3 **Uma aplicação do que foi visto**

Uma boa alternativa de resolução do cubo será mostrada nesse momento. Tudo que foi estudado e praticado nos permite chegar a essa conclusão. Lembre-se que nosso cubo tem uma configuração inicial padrão que será aqui mantida. Vamos aos passos que mostram esse caminho.

a) Primeiro passo

Formaremos uma cruz na base com os cubinhos borda e o cubinho centro. Essa cruz não é complicada de ser feita e com algumas repetições teremos habilidades para essa formação.

Figura 73 – Cruz na base



Fonte: o Autor, 2016

b) Segundo passo

Trabalharemos com os cubinhos canto da base. Esses cubinhos devem encontrar-se inicialmente na face superior e na vertical de seus cubículos. Em seguida, usaremos os movimentos para cada cubinho canto, da seguinte maneira:

- LUL^{-1} para o cubinho canto ldb;
- $R^{-1}U^{-1}R$ para o cubinho canto rbd;
- $L^{-1}U^{-1}L$ para o cubinho canto fbl;
- RUR^{-1} para o cubinho canto frb.

Faremos esses movimentos até que consigamos encaixar cada cubinho canto da base em seus cubículos canto da base e na posição correta.

Figura 74 – Camada abaixo posicionada

Fonte: o Autor, 2016

c) Terceiro passo

Posicionaremos os cubinhos borda fl, fr, bl e br que encontram-se na camada intermediária.

Para os cubinhos borda fl e fr, inicialmente ficarão no cubículo borda fu. Daí, aplicaremos o movimento $U^{-1}L^{-1}ULUFU^{-1}F^{-1}$, para o cubinho borda fl e o movimento $URU^{-1}R^{-1}U^{-1}F^{-1}UF$, para o cubinho borda fr. Caso haja um posicionamento invertido das faces dos cubinhos, repetiremos os movimentos para retirá-los dos cubículos e depois para recolocá-los de maneira correta.

Os cubinhos borda lb e rb, inicialmente ficarão nos cubículos borda lu e ru, respectivamente. Com isso, faremos o movimento $U^{-1}B^{-1}UBULU^{-1}L^{-1}$, para posicionar o cubinho borda lb e o movimento $UBU^{-1}B^{-1}U^{-1}R^{-1}UR$, para posicionar o cubinho borda rb. Caso tenhamos um posicionamento invertido das faces dos cubinhos, repetiremos os movimentos para retirá-los dos cubículos e depois para recolocá-los de maneira correta.

Figura 75 – Camada intermediária posicionada

Fonte: o Autor, 2016

Nesse momento estamos com as duas primeiras camadas, de baixo para cima, posicionadas corretamente. Vamos continuar o processo.

d) Quarto passo

Formaremos uma cruz vermelha na face superior com os cubinhos borda e o cubinho centro. Nesse momento, a camada acima pode ser rotacionada conforme conveniência. Primeiramente, temos que visualizar um “L” invertido de cor vermelha com as faces superiores dos cubículos ul, u e ub. Daí, fazemos o movimento $FRUR^{-1}U^{-1}F^{-1}$, para encontrarmos uma linha horizontal vermelha com as faces superiores dos cubículos ul, u e ur. Em seguida, repetimos o movimento $FRUR^{-1}U^{-1}F^{-1}$, para chegarmos a cruz desejada.

Se, mesmo rotacionando a face acima do cubo, não consigamos o “L” invertido citado anteriormente, temos a opção de visualizarmos um outro “L” invertido de cor vermelha com as faces superiores dos cubículos ub, u e ur. Nesse caso, empregamos o movimento $BLUL^{-1}U^{-1}B^{-1}$, para tentarmos o “L” invertido do primeiro caso. Esse movimento também serve quando, após conseguirmos a linha horizontal vermelha citada anteriormente, quisermos chegar a cruz vermelha que finaliza esse quarto passo.

Figura 76 – Cruz vermelha

Fonte: o Autor, 2016

e) Quinto passo

Posicionaremos os cubinhos borda da face acima em seus cubículos borda correspondentes. Após fazer a cruz vermelha, girando a face acima do cubo, colocaremos apenas um cubinho borda no seu correspondente cubículo borda e esse cubinho borda deverá ser ou o uf ou o ub. Caso não seja possível colocar apenas um dos dois cubinhos borda em seu cubículo borda, aplique um dos movimentos do passo quatro, de preferência o movimento diferente ao último usado. Se a escolha for pelo cubinho borda uf, em seguida faremos o movimento $RUR^{-1}URU^2R^{-1}$, mas se for o cubinho borda ub, faremos o movimento $LUL^{-1}ULU^2L^{-1}$. Se for necessário, repita esses movimentos. Assim, chegaremos ao pretendido.

f) Sexto passo

Posicionaremos todos os cubinhos canto da face acima do cubo em seus cubículos canto, sendo dois cubinhos canto de uma mesma face do cubo posicionados corretamente e os outros dois posicionados com suas faces trocadas, um no sentido horário e o outro no sentido anti-horário. Esse passo é o que pode demorar mais, porém nada tão complicado. Temos algumas características que indicam satisfação e rapidez na passagem desse passo.

Façamos os movimentos $LU^{-1}R^{-1}UL^{-1}U^{-1}RU$ (1), $L^{-1}URU^{-1}LUR^{-1}U^{-1}$ (2), $R^{-1}ULU^{-1}RUL^{-1}U^{-1}$ (3) e $RU^{-1}L^{-1}UR^{-1}U^{-1}LU$ (4) duas vezes cada. Caso tenhamos alguns dos casos abaixo nessas tentativas, tentaremos as dicas correspondentes. Se não tivermos, tentaremos mais uma vez os movimentos de maneira aleatória até que uma dessas dicas apareça. Vamos às possibilidades:

I) Cubinhos canto ulb e urf posicionados corretamente, nos remete à sequência de movimentos $(1), (2), (3)$.

II) Cubinho canto ubr posicionado corretamente, nos leva ao movimento (1).

III) Cubinho canto urf posicionado corretamente, nos indica o movimento (2).

IV) Cubinho canto ulb posicionado corretamente, nos induz ao movimento (3).

V) Cubinho canto ufl posicionado corretamente, nos envia ao movimento (4).

VI) Cubinhos canto ufl e ubr posicionados corretamente, nos conduz à sequência de movimentos $(4), (3), (2)$.

Pode acontecer dessas dicas serem falhas, então, partiremos para os movimentos de maneira aleatória.

g) Sétimo passo

Ajustaremos corretamente os dois cubinhos canto com faces trocadas do sexto passo. Inicialmente trataremos do cubinho canto que precisa de um giro no sentido horário. Temos os seguintes casos:

I) Se o cubinho canto for o urf, usaremos o movimento $FDF^{-1}D^{-1}FDF^{-1}D^{-1}$.

II) Se o cubinho canto for o ufl, usaremos o movimento $F^{-1}DFD^{-1}F^{-1}DFD^{-1}$.

III) Se o cubinho canto for o ulb, usaremos o movimento $BDB^{-1}D^{-1}BDB^{-1}D^{-1}$.

IV) Se o cubinho canto for o ubr, usaremos o movimento $B^{-1}DBD^{-1}B^{-1}DBD^{-1}$.

Após fazermos a correção do cubinho canto que precisou do giro no sentido horário, partiremos imediatamente para o giro no sentido anti-horário do outro cubinho canto. Girando a face acima do cubo e posicionando o cubinho canto que precisa do giro no sentido anti-horário para o lugar do cubinho canto que foi girado no sentido horário, seguiremos para a próxima etapa desse passo. Partindo da posição que havia parado antes do giro da face acima do cubo, seguimos para a última parte desse sétimo passo. Associando à situação anterior, respectivamente, temos:

I) Seguiremos para o movimento $DFD^{-1}F^{-1}DFD^{-1}DF^{-1}$.

II) Seguiremos para o movimento $DF^{-1}D^{-1}FDF^{-1}D^{-1}F$.

III) Seguiremos para o movimento $DBD^{-1}B^{-1}DBD^{-1}B^{-1}$.

IV) Seguiremos para o movimento $DB^{-1}D^{-1}BDB^{-1}D^{-1}B$.

Por fim, desfazemos o giro dado anteriormente e concluímos a resolução do cubo.

Pode acontecer de alguns desses passos serem “saltados”, isto é, uma ou mais dessas passagens aparecerem sem ser preciso fazê-las.

CONCLUSÃO

Esperamos ter contribuído para que uma antiga brincadeira ou um antigo passatempo ou, até mesmo, um antigo jogo desperte interesse pelo entendimento de conceitos matemáticos, independentemente dos que foram usados nesse trabalho. A prática de um determinado pensamento é porta de entrada para o conhecimento do que se pretende.

Nosso objetivo é aguçar o imaginário e fomentar a lógica da razão. O desafio mostra alternativas de realizações e mantém-nos idealizando meios de sobrevivência. É com essa analogia que queremos manter viva a Matemática em nossa Sociedade. Estudar Matemática é trazer mais entendimento sobre a vida, é trazer mais sentido as nossas existências, é raciocinar diante das dificuldades impostas.

REFERÊNCIAS

CHEN, J. Group Theory and the Rubik’s Cube, 2004. Disponível em: <http://www.math.harvard.edu/~jjchen/docs/Group%20Theory%20and%20the%20Rubik's%20Cube.pdf>. Acesso em: 04/08/2016.

FREY, A.; SINGMASTER, D. Handbook of cubik math, Enslow Pub., 1982.

SIMIS, A. Introdução à Álgebra, Monografias de Matemática, nº 23, IMPA, 1977.

MARTINEZ, F.E.B.; MOREIRA, C.G.T.A.; SALDANHA, N.C.; TENGAN, E. Teoria dos Números. Um passeio com Primos e outros Números Familiares pelo Mundo Inteiro, Coleção Projeto Euclides, IMPA, 2013.

RUBIK, E.; VARGA, T.; KÉRI, G.; MARX, G.; VKERDY, T. Rubik’s Cubic Compendium, Oxford University Press, Oxford, 1987.