ルービックキューブと群

芝浦工業大学　数理科学研究会

～大宮祭研究発表～

平成 28 年 5 月 22 日

※何か不明な点や計算ミス等がありましたら加筆修正しますので指摘をお願いします

制作: 長田　祐輝

目 次

1　研究動機

小学生のころルービックキューブをやっていた. そのときはある解法を見ながら 6 面を揃えていた. しかしそもそもどうやってその解法手順が導けたのかという疑問を抱いた. そこで今回はその解法手順の導出を研究しようと思った.

2　研究目的

研究目的は, バラバラな状態のルービックキューブの情報を数学的に取り出し, その情報だけから, 完成させる手順を計算によって求めることである.

3　さまざまな用語の説明

ベクトルとは数の組のことである.
(例) $(1, 2, 2, 1, 0, 0, 0, 0)$

置換とは次のようなものである：

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

4　ルービックキューブの用語および記号の定義

4.1　面を表す記号および回転記号の導入

定義 4.1.　ルービックキューブの面に次のように名前を付けておく：
上面 $\cdots U$, 下面 $\cdots D$, 左面 $\cdots L$, 右面 $\cdots R$, 前面 $\cdots F$, 後面 $\cdots B$.
また, 次のように U, D, L, R, F, B は面を回転させる記号としても用いられる：
$U \cdots$ 上面を時計回りに 90 度回転, $D \cdots$ 下面を時計回りに 90 度回転, $L \cdots$ 左面を時計回りに 90 度回転,
$R \cdots$ 右面を時計回りに 90 度回転, $F \cdots$ 前面を時計回りに 90 度回転, $B \cdots$ 後面を時計回りに 90 度回転.
これら U, D, L, R, F, B の面の回転操作のことを単位操作という.

定義 4.2.　ルービックキューブをちゃんと回して得られる変化全体の集合を G で表す. すなわち例えば, ルービックキューブを分解してまた組み立てるという操作は禁止とする.
また, G の元 g, h に対して g を行ってから h を行う変化を g と h の積といい, gh と書く.
G を集合の記号を用いて書けば以下のようになる：

$$G = \{X_1 X_2 \cdots X_n \,|\, n \in \mathbb{N},\ X_i \in \{L, R, U, D, F, B\},\ (i = 1, 2, \ldots, n)\}.$$

このとき, G は L, R, U, D, F, B によって生成されるといい, $G = \langle L, R, U, D, F, B \rangle$ と書く.

例 4.1.　単位操作 R を行ってから, F を行う変化を RF で表す. この変化 RF は G に属す.

4.2　キューブの名称

定義 4.3.　ルービックキューブのシールが 3 枚貼られている小立方体を 3 面体という. シールが 2 枚貼られている小立方体を 2 面体という. シールが 1 枚貼られている小立方体を 1 面体という. (図 1 参照)

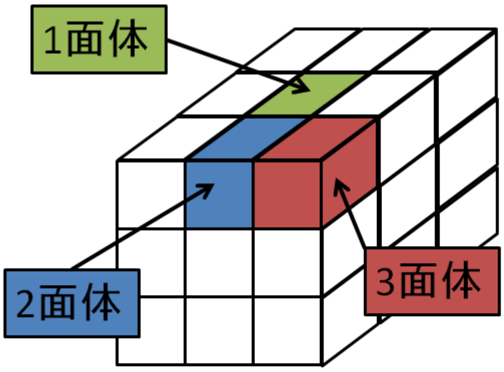

図 1: 3 面体, 2 面体, 1 面体

4.3　3 面体の番号付けと ′+′ 印

定義 4.4.　ルービックキューブの 3 面体に図 2 のように番号と ′+′ 印を振っていく：

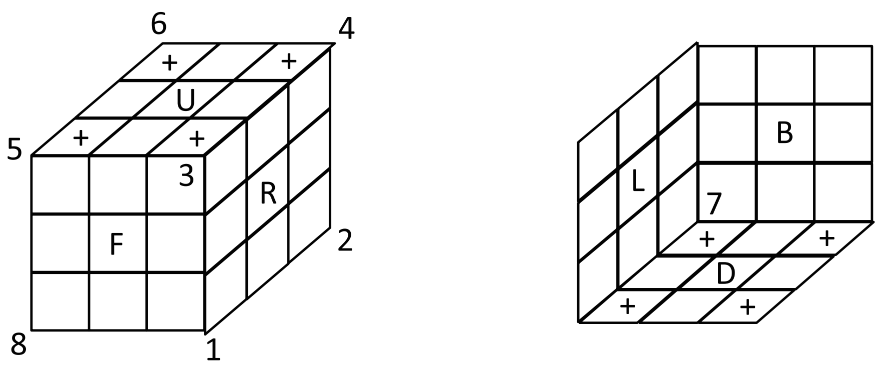

図 2: 3 面体の'+' 印と頂点の番号

4.4　2 面体の番号付けと ′+′ 印

定義 4.5.　ルービックキューブの 2 面体に図 3 のように番号と ′+′ 印を振っていく：

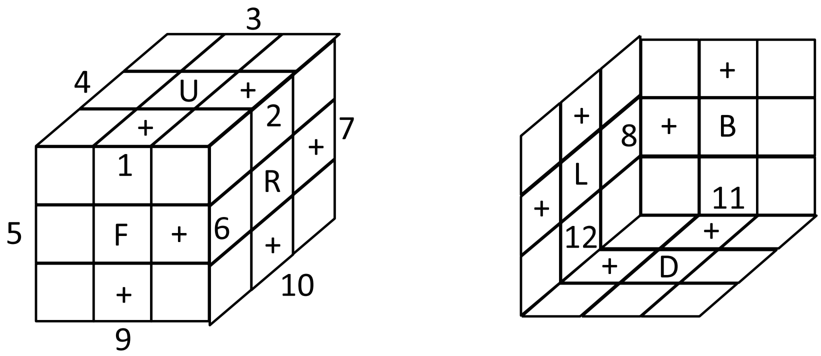

図 3: 2 面体の'+' 印と頂点の番号

4.5　その他の記号の定義

定義 4.6.　V 頂点の集合 $V=\{1,2,3,4,5,6,7,8\}$ とする. E を辺の集合 $E=\{1,2,3,4,5,6,7,8,9,10,11,12\}$ とする. C_3^8 は C_3 の 8 個の直積である. C_3 とは 位数 3 の巡回群で, $C_3=\{0,1,2\}$ であり, C_3 上の加法を足して 3 で割ったあまりを対応させせる演算とする. C_2^{12} も同様に定義する. S_V は $|V|=8$ 文字の置換全体の集合とする. S_E も同様に定義する. $\vec{v}$ は写像 $\vec{v}:G\to C_3^8$ で, G の元に対して, 3 面体の向きを表す C_3^8 の元を対応させせる写像である. 詳しくは, 小節 4.6 を参照せよ. 写像 $\vec{w}:G\to C_2^{12}$ も同様に定義する. ρ は写像 $\rho:G\to S_V$ で, G の元に対して, 3 面体の入れ替えを表す置換を対応させせる写像である. 詳しくは, 小節 4.6 を参照せよ. 写像 $\sigma:G\to S_E$ も同様に定義する.

4.6　ルービックキューブの可能な変化に対する 4 つ組の定義

次にルービックキューブの可能な変化に対して次のような 4 つ組を対応させる.
例えば, R (右面を時計回りに 90 度回転させる操作) は以下のような 4 つ組で表される :

$$\vec{v}(R)=(1,2,2,1,0,0,0,0)$$
$$\rho(R)=\begin{pmatrix}1&2&3&4\\3&1&4&2\end{pmatrix}$$
$$\vec{w}(R)=(0,1,0,0,0,0,0,0,0,1,0,0)$$
$$\sigma(R)=\begin{pmatrix}2&6&7&10\\7&2&10&6\end{pmatrix}.$$

まず, $\rho(R)$ について説明する. 先ほどの 3 面体の番号付けに対して R を施すと, 図 4 より, 例えば, 頂点 1 は頂点 3 に移動するので, 1 の移先を 3 と書く. 他も同様に定義する.

次に $\vec{v}(R)$ について説明する. 例えば $\vec{v}(R)$ の第 1 成分には頂点 1 の $'+'$ 印を移先の頂点 (頂点 3) の $'+'$ 印に合わせるために時計回りにどれだけひねるかを表す数字を書く. 他も同様に定義する.

次に $\sigma(R)$ について説明する. $\sigma(R)$ は $\rho(R)$ と同様に定義する. 各 2 面体が R という操作によってどう変化したかを置換を用いて表したものが $\sigma(R)$ である. 簡単に言えば $\sigma(R)$ は 2 面体の変化を表す.

最後に, $\vec{w}(R)$ の説明をする. $\vec{w}(R)$ は $\vec{v}(R)$ と同様に定義する. $\vec{w}(R)$ は簡単に言えば 2 面体の向きを表すベクトルである. 詳しくは図 5 によって説明する.

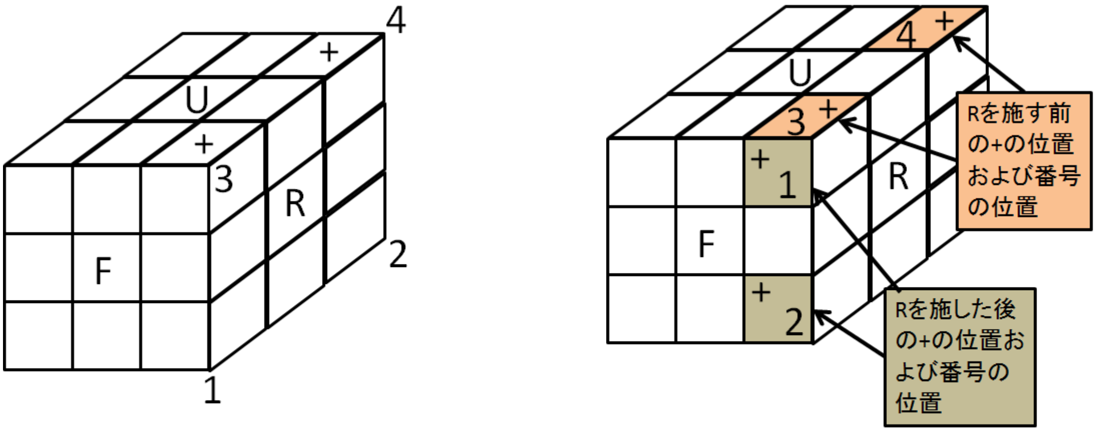

図 4: R を施したあとの 3 面体の'+' 印および頂点の番号

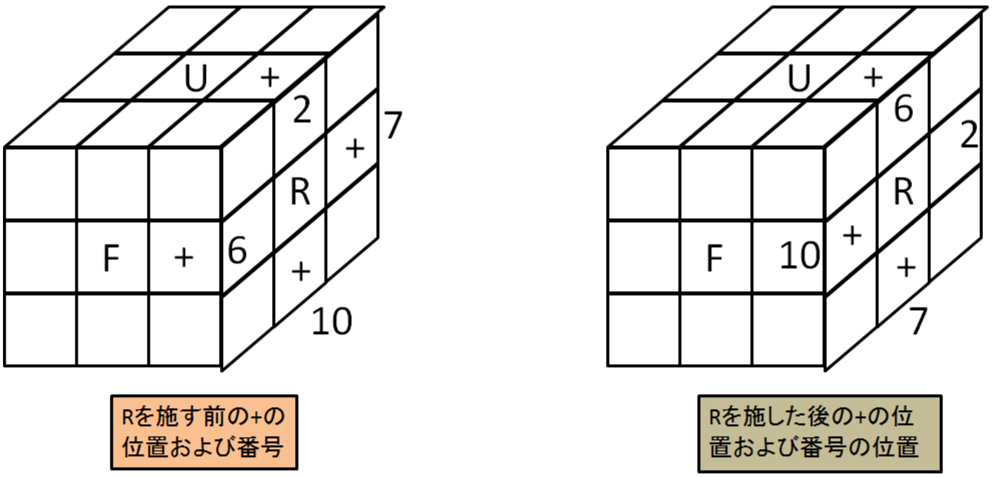

図 5: R を施したあとの 2 面体の'+' 印および頂点の番号

U	$(0,0,0,0,0,0,0,0)$	D	$(0,0,0,0,0,0,0,0)$
	$\begin{pmatrix} 3 & 4 & 5 & 6 \\ 5 & 3 & 6 & 4 \end{pmatrix}$		$\begin{pmatrix} 1 & 2 & 7 & 8 \\ 2 & 7 & 8 & 1 \end{pmatrix}$
	$(1,0,1,0,0,0,0,0,0,0,0,0)$		$(0,0,0,0,0,0,0,0,0,1,0,1)$
	$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$		$\begin{pmatrix} 9 & 10 & 11 & 12 \\ 10 & 11 & 12 & 9 \end{pmatrix}$
L	$(0,0,0,0,1,2,1,2)$	R	$(1,2,2,1,0,0,0,0)$
	$\begin{pmatrix} 5 & 6 & 7 & 8 \\ 8 & 5 & 6 & 7 \end{pmatrix}$		$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$
	$(0,0,0,0,1,0,0,1,0,0,0,0)$		$(0,1,0,0,0,0,0,0,0,1,0,0)$
	$\begin{pmatrix} 4 & 5 & 8 & 12 \\ 5 & 12 & 4 & 8 \end{pmatrix}$		$\begin{pmatrix} 2 & 6 & 7 & 10 \\ 7 & 2 & 10 & 6 \end{pmatrix}$
F	$(2,0,1,0,2,0,0,1)$	B	$(0,1,0,2,0,1,2,0)$
	$\begin{pmatrix} 1 & 3 & 5 & 8 \\ 8 & 1 & 3 & 5 \end{pmatrix}$		$\begin{pmatrix} 2 & 4 & 6 & 7 \\ 4 & 6 & 7 & 2 \end{pmatrix}$
	$(1,0,0,0,0,0,0,0,1,0,0,0)$		$(0,0,0,0,0,0,1,1,0,0,0,0)$
	$\begin{pmatrix} 1 & 5 & 6 & 9 \\ 6 & 1 & 9 & 5 \end{pmatrix}$		$\begin{pmatrix} 3 & 7 & 8 & 11 \\ 8 & 3 & 11 & 7 \end{pmatrix}$

表 1: 単位操作の 4 つ組

表 1 に, 単位操作に対する 4 つ組を表にまとめた.

例 4.2. 2 つ単位操作を続けた場合の 4 つ組の求め方を考える. 例えば, R を行ったあとに, F を行う場合を考える. R を行ったあとの 3 面体の $'+'$ 印の位置および頂点の入れ替えは次の図 6 の通り. また, 続けて

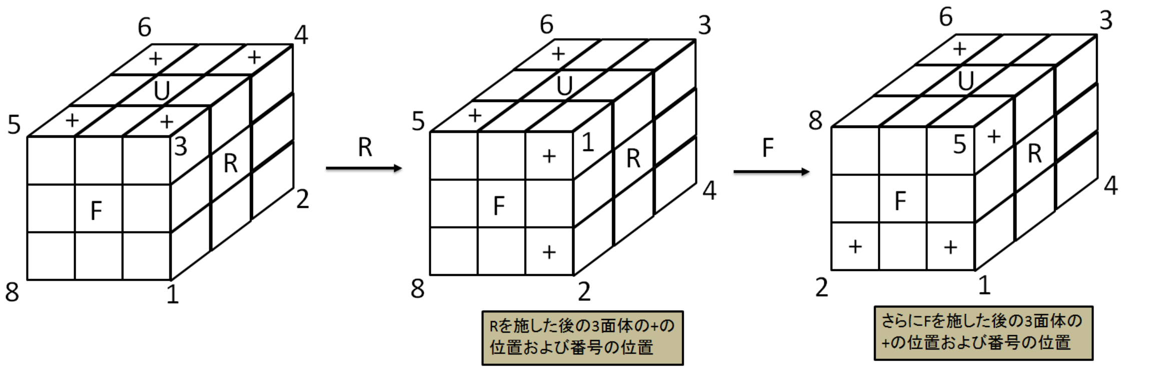

図 6: RF を行ったときの 3 面体の'+' 印よび番号の位置

F を行ったあとの 2 面体の $'+'$ 印の位置および頂点の入れ替えは次の図 7 の通り. よって最初の状態と最後の状態の変化をみれば $\vec{v}(RF)$, $\rho(RF)$, $\vec{w}(RF)$ および $\sigma(RF)$ が求まる :

$$
\begin{aligned}
\vec{v}(RF) &= (2,1,2,1,2,0,0,1) \\
\rho(RF) &= \begin{pmatrix} 2 & 3 & 4 & 5 & 8 \\ 8 & 4 & 2 & 3 & 5 \end{pmatrix} \\
\vec{w}(RF) &= (1,1,0,0,0,0,0,0,1,1,0,0) \\
\sigma(RF) &= \begin{pmatrix} 1 & 2 & 5 & 6 & 7 & 9 & 10 \\ 6 & 7 & 1 & 2 & 10 & 5 & 9 \end{pmatrix}.
\end{aligned}
$$

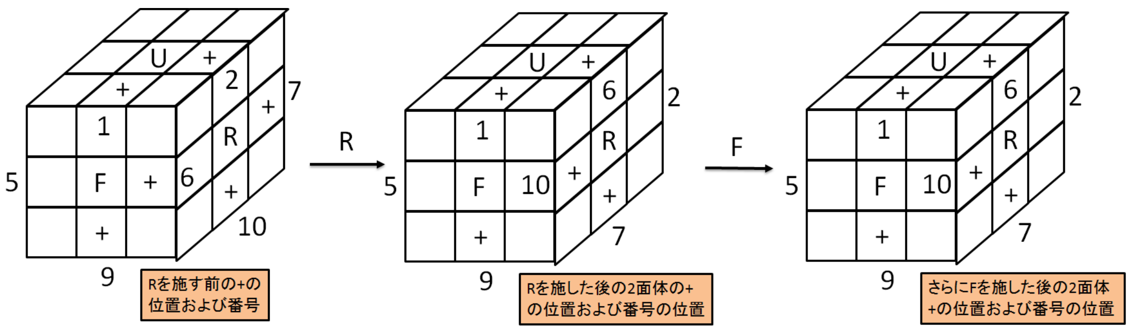

図 7: RF を行ったときの 2 面体の'+' 印よび番号の位置

定理 4.7. G の元 g, h に対して, 次が成り立つ :

$$
\begin{aligned}
&v_i(gh) = v_i(g) + v_{\rho(g)(i)}(h), \ \ (i = 1, 2, \ldots, 8) \\
&\rho(gh) = \rho(g)\rho(h), \\
&w_i(gh) = w_i(g) + w_{\sigma(g)(i)}(h), \ \ (i = 1, 2, \ldots, 12) \\
&\sigma(gh) = \sigma(g)\sigma(h).
\end{aligned}
$$

ただし, $v_i(g)$ は $\vec{v}(g)$ の第 1 成分を表し, $w_i(g)$ は $\vec{w}(g)$ の第 i 成分を表す. また 置換の演算は関数の合成により計算するが, そのときの関数の合成は左から順番に写していくことにする. すなわち, $(\rho(g)\rho(h))(i) := \rho(h)(\rho(g)(i))$ とする.

5 重要な定理

定理 5.1. (キューブ理論の第 1 基本定理) 次の決定過程によって, ルービックキューブの位置は決定される.

(a) どのように 2 面体が置換されたか.

(b) どのように 3 面体が置換されたか.

(c) (基準参照印に対して) どの 2 面体の印が反転したか.

(d) (基準参照印に対して) どの 3 面体の印がどれだけ (時計回りに 120 度または 240 度) 回転したか.

定理 5.2. (キューブ理論の第 2 基本定理)　$(v, r, w, s) \in C_3^8 \times S_V \times C_2^{12} \times S_E$ が規則に従った手順で得られた変化であるための必要十分条件は

(a) $\mathrm{sgn}(r) = \mathrm{sgn}(s)$

(b) $v_1 + \cdots + v_8 \equiv 0 \pmod 3$

(c) $w_1 + \cdots + w_{12} \equiv 0 \pmod 2$.

証明　$(\Rightarrow)$：まず, (a) を示す. $g \in G$ を規則に従った手順で得られた変化とし, それに対応する 4 つ組を $(v, r, w, s) \in C_3^8 \times S_V \times C_2^{12} \times S_E$ とする. $r = \rho(G),\ s = \sigma(g)$ となる. g は単位操作 R, L, U, D, F, B の積でかけるので $g = X_1 X_2 \cdots X_n$ とする. X が R, L, U, D, F, B のいずれかのときは

$$\mathrm{sgn}(r) = \mathrm{sgn}(\rho(X)) = \mathrm{sgn}(\sigma(X)) = \mathrm{sgn}(s)$$

が成り立つ. sgn, ρ, σ は準同型すなわち,

$$\begin{aligned}&\mathrm{sgn}(r_1 r_2) = \mathrm{sgn}(r_1)\mathrm{sgn}(r_2),\\ &\rho(XY) = \rho(X)\rho(Y),\\ &\sigma(XY) = \sigma(X)\sigma(Y)\end{aligned}$$

であるから, 次が成り立つ：

$$\begin{aligned}\mathrm{sgn}(r) &= \mathrm{sgn}(\rho(g)) = \mathrm{sgn}(\rho(X_1 X_2 \cdots X_n)) = \mathrm{sgn}(\rho(X_1)\rho(X_2)\cdots\rho(X_n))\\ &= \mathrm{sgn}(\rho(X_1))\mathrm{sgn}(\rho(X_2))\cdots\mathrm{sgn}(\rho(X_n)) = \prod_{i=1}^{n}\mathrm{sgn}(\rho(X_i)) = \prod_{i=1}^{n}\mathrm{sgn}(\sigma(X_i))\\ &= \mathrm{sgn}(\sigma(X_1))\mathrm{sgn}(\sigma(X_2))\cdots\mathrm{sgn}(\sigma(X_n)) = \mathrm{sgn}(\sigma(X_1)\sigma(X_2)\cdots\sigma(X_n))\\ &= \mathrm{sgn}(\sigma(X_1 X_2 \cdots X_n)) = \mathrm{sgn}(\sigma(g)) = \mathrm{sgn}(s).\end{aligned}$$

これで (a) が証明できた.

次に (b) を示す. X が R, L, U, D, F, B のときは (b) が成り立つことは実際に X の 4 つ組を求めて確かめれば分かる. また, 次が成り立つ：

(i) $(w_1, w_2, \ldots, w_8) \in C_3^8$ に対して,
$w_1 + w_2 + \cdots + w_8 \equiv 0 \pmod 3$
$\Leftrightarrow\ {}^{\exists}(v_1, v_2, \ldots, v_8) \in C_3^8$ s.t. ${}^{\exists}\rho \in S_V$ s.t. $w_i = v_{\rho(i)}\ (i = 1, 2, \ldots, 8),\ v_1 + v_2 + \ldots v_8 \equiv 0 \pmod 3$

(ii) $v_1 + v_2 + \cdots + v_8 \equiv 0 \pmod 3$ かつ $v'_1 + v'_2 + \cdots + v'_8 \equiv 0 \pmod 3$ ならば
$(v_1 + v'_1) + (v_2 + v'_2) + \cdots + (v_8 + v'_8) \equiv 0 \pmod 3$

(i) についてだけ証明する：

$(\Rightarrow)$：$v_i = w_i (i = 1, 2, \ldots, 8),\ \rho = 1$(恒等置換) ととればよい.
$(\Leftarrow)$：$v_1 + v_2 + \cdots + v_8 \equiv 0 \pmod 3$ かつ $w_i = v_{\rho(i)}$ で ρ は 8 文字の置換であることから $w_1 + w_2 + \cdots + w_8 \equiv 0 \pmod 3$ が成り立つ.

$g \in G$ とする. $g = X_1 X_2 \cdots X_n,\ X_i \in \{L, R, U, D, F, B\}\ (i = 1, 2, \ldots, n)$ と表せる. n に関する帰納法で示す. $n = 1$ のときは証明済. $n = k$ のとき成り立つと仮定して, $n = k + 1$ のとき成り立つか考える.
$g = X_1 X_2 \cdots X_k X_{k+1}$ のとき,

$$v_i(X_1 X_2 \cdots X_k X_{k+1}) = v_i(X_1 X_2 \cdots X_k) + v_{\rho(X_1 X_2 \cdots X_k)(i)}(X_{k+1}),\ (i = 1, 2, \ldots, 8).$$

帰納法の過程より, $v_1(X_1X_2\cdots X_k)+v_2(X_1X_2\cdots X_k)+\cdots+v_8(X_1X_2\cdots X_k)\equiv 0 \pmod 3$ が成り立つ.
また, $X_{k+1}\in\{L,R,U,D,F,B\}$ であることから $v_1(X_{k+1})+v_2(X_{k+1})+\cdots+v_8(X_{k+1})\equiv 0 \pmod 3$ が成り立つ. ここで, $w_i=v_{\rho(X_1X_2\cdots X_k)(i)}(X_{k+1})$ とおくと, (i) より,

$$w_1+w_2+\cdots+w_8\equiv 0 \pmod 3$$

すなわち

$$v_{\rho(X_1X_2\cdots X_k)(1)}(X_{k+1})+v_{\rho(X_1X_2\cdots X_k)(2)}(X_{k+1})+\cdots+v_{\rho(X_1X_2\cdots X_k)(8)}(X_{k+1})\equiv 0 \pmod 3$$

が成り立つ. よって, (ii) より,

$$\begin{aligned}&v_1(X_1X_2\cdots X_{k+1})+v_2(X_1X_2\cdots X_{k+1})+\cdots+v_8(X_1X_2\cdots X_{k+1})\\&=v_1(X_1X_2\cdots X_k)+v_{\rho(X_1X_2\cdots X_k)(1)}(X_{k+1})+v_2(X_1X_2\cdots X_k)+v_{\rho(X_1X_2\cdots X_k)(2)}(X_{k+1})\\&+\cdots+v_8(X_1X_2\cdots X_k)+v_{\rho(X_1X_2\cdots X_k)(8)}(X_{k+1})\\&\equiv 0 \pmod 3.\end{aligned}$$

よって, (b) が成り立つ.
同様に (c) も示せる.
$(\Leftarrow)$ の証明は略. $\square$

6　今後の課題

今回, 私は数学的な手法を用いて完成までの手順を求めるのではなく, コンピュータの力を借りてプログラミングによって完成までの手順を得た. しかし当初の目的では, コンピュータを用いずに数学的な手法で完成までの手順を得るつもりだった. 今度はコンピュータでのアプローチではなく, 数学的なアプローチで群論を用いて議論してみたい.

7　参考文献

[1]David Joyner(川辺治之), 群論の味わい　置換群で解き明かすルービックキューブと 15 パズル, 共立出版, 2010.