群論で解き明かす
ルービックキューブの数理 (1)

川辺治之

2010 年 9 月 1 日

群の定義

集合 G が次の条件を満たすとき、G を群という.

(G1) 演算 $\cdot : G \times G \to G$ が定義されている.

(G2) 結合則 $\forall f, g, h \in G, (f \cdot g) \cdot h = f \cdot (g \cdot h)$ が成り立つ.

(G3) 単位元 $\exists g \in G, \forall f \in G, gf = fg = f$ が存在する.
この g を 1 と表記する.

(G4) 逆元 $\forall f \in G, \exists g \in G, f \cdot g = g \cdot f = 1$ が存在する.
この g を f^{-1} と表記する.

一人ゲーム

- それぞれの局面では，有限個の許される手がある．
- 有限の手の並び (手順) で解に到達できる．
- 偶然に左右されたり，無作為に選ばれる手はない．
- それぞれの手を行うことの効果はすべてわかっている．
- それぞれの手が許されるかどうかは，現在のゲームの状態にだけ依存していて，それまでの手がどうであったかに依存しない．

置換パズル

置換パズルとは，小片の有限集合 T を使った次の四つの条件を満たす一人ゲームのこと．

- パズルのそれぞれの手は， $\mathbb{Z}_n = \{1, 2, \ldots, n\}$ の元の置換に対応している．($n > 1$ は，パズルの構成によって決まる整数)
- 一つの置換に対応する手が複数ある場合，それぞれの手を行った結果の状態は区別できない．
- それぞれの手 M は「可逆」，つまり M に対して，M を行った結果の状態から M を行う前の状態に戻す手が存在する．
- T の置換 f_1 に対応する手を M_1 とし，T の置換 f_2 に対応する手を M_2 とすると，$M_1 * M_2$ (M_1 に引き続いて M_2 を行う) は次のどちらかとなる．
  - ゲームの規則では許されない手
  - 置換 $f_1 * f_2$ に対応する手

置換パズルの例

- 15 パズル
- ルービックキューブ
- ライツアウト
- …

群の例

- C_n : 位数 n の巡回群 $\{0, 1, \ldots, n-1\}$
- S_n : n 次の対称群 (n 個の対象の置換全体からなる群)
- A_n : n 次の交代群 (n 個の対象の偶置換全体からなる群)

A_n は S_n の指数 2 の部分群

ルービックキューブの単位操作

- U : ルービックキューブの上面を (上から見て) 時計回りに 90 度回転させる操作
- D : ルービックキューブの下面を (下から見て) 時計回りに 90 度回転させる操作
- L : ルービックキューブの左面を時計回りに 90 度回転させる操作
- R : ルービックキューブの右面を時計回りに 90 度回転させる操作
- F : ルービックキューブの前面を時計回りに 90 度回転させる操作
- B : ルービックキューブの後面を時計回りに 90 度回転させる操作

この略記法を**シングマスター記法**という.

部分群

群 G の部分集合 H で，G から引き継いだ演算 $*$ が群の条件 (G1)-(G4)(のすべての G を H で置き換えたもの) を満たすものを，G の**部分群**といい，
$H \subset G$ と表記する．

群の準同型写像

G_1, G_2 を群とし，$*_1$ を G_1 の群の演算とし，$*_2$ を G_2 の群の演算とする．
関数 $f : G_1 \to G_2$ は，任意の $a, b \in G_1$ に対して

$$f(a *_1 b) = f(a) *_2 f(b)$$

が成り立つとき，**準同型写像**という．

群の同型

準同型写像 $f : G_1 \to G_2$ は，それが (集合の間の関数として) 全単射となるとき，**同型写像**という.
このとき，G_1 と G_2 は**同型**といい，$G_1 \cong G_2$ と表記する.
群 G から自分自身への同型写像を**自己同型写像**という.
G の自己同型写像全体の群を $\mathrm{Aut}(G)$ と表記する.

準同型写像の核

$f : G_1 \to G_2$ を二つの群の間の準同型写像とする．e_2 を G_2 の単位元とするとき，集合

$$\ker(f) = \{g \in G_1 \mid f(g) = e_2\}$$

を f の**核**という.
$\ker(f)$ は G_1 の部分群となる.

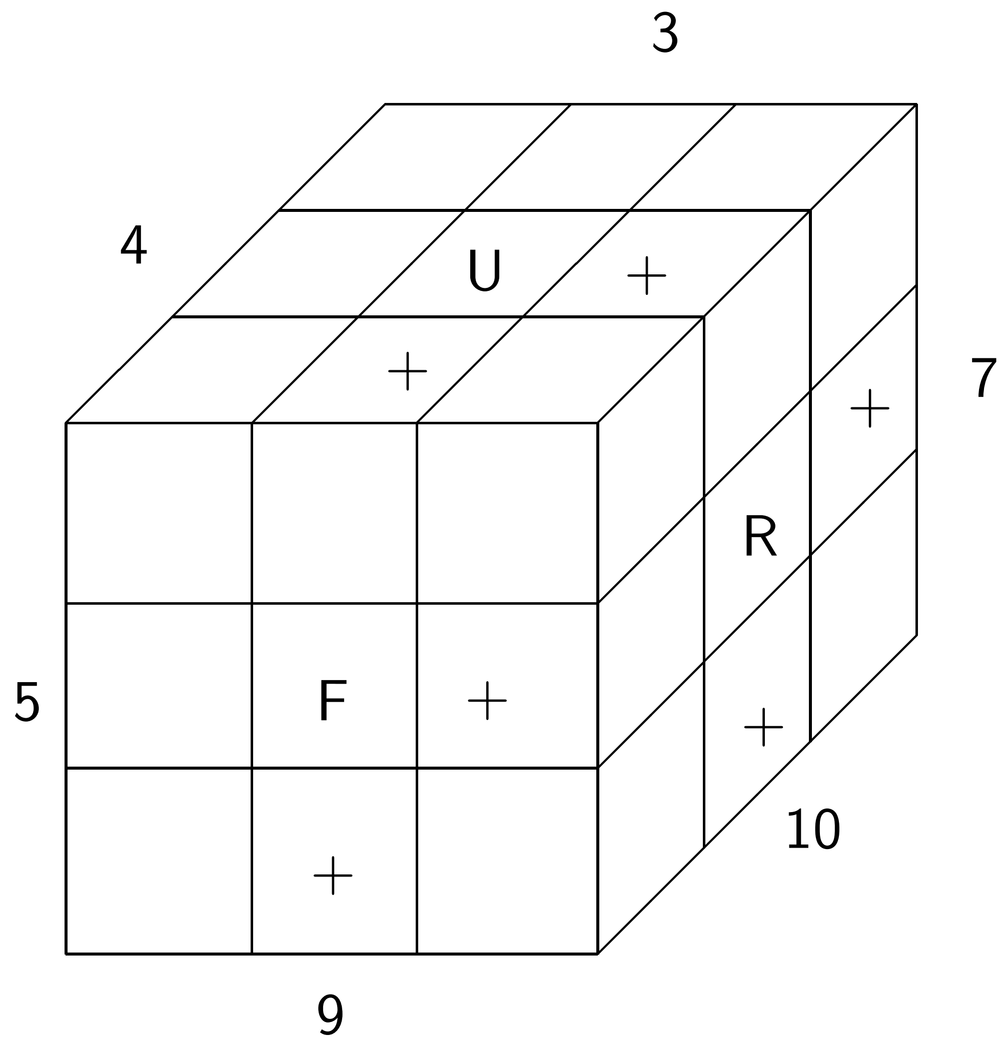
ルービックキューブ群

$3 \times 3 \times 3$ ルービックキューブ群:

$$G = \langle R, L, U, D, F, B \rangle$$

H :ルービックキューブの規則に従ったすべての手順だけでなく，規則に従わない手順もすべて含めた**規則を無視したルービックキューブ群**.
ルービックキューブをいったん 3 面体や 2 面体に分解して，組み立て直してもよい．(しかし，小方体に貼られたシールをはがして貼り直すことはできない．)

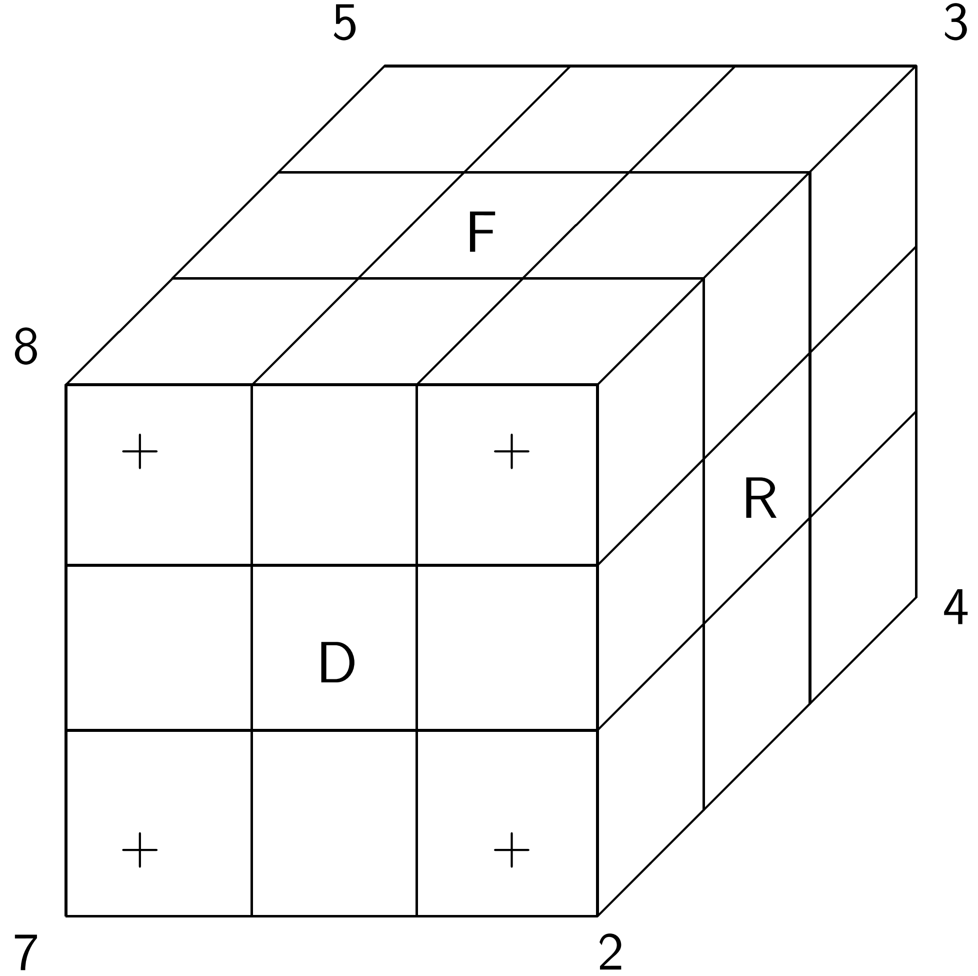
2 面体の向きと辺の番号付け



残りの面については，2 面体の dl，db，lf，lu，bl および bu 面に基準参照印 (‘$+$’ 印) をつける．

3 面体の向きと辺の番号付け

3 面体の向きについては，下側のすべての小面と，上側のすべての小面に基準参照印 (‘$+$’ 印) をつける．



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配置は決定される．

(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．

3 面体の向き

それぞれの 3 面体の 120 度単位の捻りを位数 3 の巡回群 C_3 と同一視する.

$$v : H \to C_3^8$$

それぞれの手順 $g \in H$ に対してその手順の結果における 3 面体の向きを対応付ける関数
捻る角度が時計回りに 120 度の何倍かで向きを表す.

X	$\vec{v}(X)$
F	(2,0,1,0,1,0,0,2)
U	(0,0,0,0,0,0,0,0)
D	(0,0,0,0,0,0,0,0)
B	(0,1,0,2,0,2,1,0)
R	(1,2,2,1,0,0,0,0)
L	(0,0,0,0,1,2,1,2)

2 面体の向き

それぞれの 2 面体の反転を位数 2 の巡回群 C_2 と同一視する.

$$w : H \to C_2^{12}$$

それぞれの手順 $g \in H$ に対してその手順の結果における 2 面体の向きを対応付ける関数
反転させる角度が 180 度の何倍かで向きを表す.

X	$\vec{w}(X)$
F	(1,0,0,0,0,0,0,0,1,0,0,0)
U	(1,0,1,0,0,0,0,0,0,0,0,0)
$F \cdot U$	(1,0,1,0,1,0,0,0,1,0,0,0)
$U \cdot F$	(1,1,1,0,0,0,0,0,1,0,0,0)
B	(0,0,0,0,0,0,1,1,0,0,0,0)
D	(0,0,0,0,0,0,0,0,0,1,0,1)
R	(0,1,0,0,0,0,0,0,0,1,0,0)
L	(0,0,0,0,1,0,0,0,1,0,0,0)

補題:向き付けの合成

$$\vec{v}(h) = \rho(g)(\vec{v}(gh) - \vec{v}(g))$$

より

$$\vec{v}(gh) = \vec{v}(g) + \rho(g)^{-1}(\vec{v}(h))$$

$\vec{w}(gh)$ についても同様.

(内部) 半直積

群 G の部分群 H_1 および H_2 が次の条件を満たすとき，G を H_1 と H_2 の **半直積**といい,

$$G = H_1 \rtimes H_2$$

と表記する.

(a) $G = H_1 \cdot H_2 = \{h_1 \cdot h_2 \mid h_1 \in H_1, h_2 \in H_2\}$
(b) H_1 および H_2 に共通の元は G の単位元 1 のみ.
(c) H_1 は G の正規部分群

(外部) 半直積

準同型写像

$$\phi : H_2 \to \mathrm{Aut}(H_1)$$

が与えられたとき，集合 $H_1 \times H_2$ に対する乗法を

$$(x_1, y_1) \cdot (x_2, y_2) = (x_1 \cdot \phi(y_1)(x_2), y_1 \cdot y_2)$$

と定義すると，この演算により $H_1 \times H_2$ は群となる．この群を (外部) **半直積**といい，$H_1 \rtimes_\phi H_2$ と表記する．

H と同型な半直積

S_V : 8 個の 3 面体の置換全体の集合
S_E : 12 個の 2 面体の置換全体の集合

$$H' = (C_3^8 \rtimes S_V) \times (C_2^{12} \rtimes S_E)$$

H の二つの元 h および h' を
$h = (v, r, w, s), h' = (v', r', w', s') \in C_3^8 \times S_V \times C_3^8 \times S_V$ とし，H の演算を
$h \cdot h' = (v, r, w, s) \cdot (v', r', w', s') = (v + P(r)(v'), rr', w + P(s)(w'), ss')$ とする.

$$\begin{array}{rcl} \iota : H & \rightarrow & (C_3^8 \rtimes S_V) \times (C_2^{12} \rtimes S_E) \\ g & \longmapsto & (v(g), \rho(g), w(g), \sigma(g)) \end{array}$$

は準同型写像となり，群の同型 $H \cong H'$ を与える.

ルービックキューブの手順の表現

それぞれの $g \in G$ を四つ組

$$(\vec{v}(g), \rho(g), \vec{w}(g), \sigma(g))$$

と同一視する．ここで

- $\rho(g)$ は，g によるキューブの 3 面体の集合 V の置換
- $\sigma(g)$ は，g によるキューブの 2 面体の集合 E の置換
- $v(g)$ および $w(g)$ は，それぞれ 3 面体および 2 面体の向き

キューブ理論の第 2 基本定理

次の条件を満たすとき，そしてそのときに限り，ルービックキューブは，四つ組 $(\vec{v}, r, \vec{w}, s)$ ($r \in S_8$, $s \in S_{12}$, $\vec{v} \in C_3^8$, $\vec{w} \in C_2^{12}$) に対応する配置となることができる．

(a) $sgn(r) = sgn(s)$ (「置換の奇偶性一致」)

(b) $v_1 + \ldots + v_8 \equiv 0 \pmod 3$ (3 面体の「総捻り量保存」)

(c) $w_1 + \ldots + w_{12} \equiv 0 \pmod 2$ (2 面体の「総反転量保存」)

証明の概略 ($\Longrightarrow$)

(a) 単位操作が条件を満たすこと、および sgn が準同型であることより.
(b) 手順の長さによる帰納法
(c) 手順の長さによる帰納法

証明の概略 ($\Longleftarrow$)

- $((0,0,1,0,0,0,-1,0),1,\vec{0},1)$ の場合
  $g=(R^{-1}D^2RB^{-1}U^2B)^2$
- $(\vec{0},1,(1,1,0,0,0,0,0,0,0,0,0,0),1)$ の場合
  $g=LFR^{-1}F^{-1}L^{-1}U^2RURU^{-1}R^2U^2R$
- $(\vec{0},r,\vec{0},s)$ の場合
  次の 3 種類の手順が存在すること
  - 任意の三つの 2 面体の巡換だけで，それ以外の小方体の向きおよび位置を変えない手順
  - 任意の三つの 3 面体の巡換だけで，それ以外の向きおよび位置を変えない手順
  - 任意の二つの 2 面体の互換および任意の二つの 3 面体の互換だけで，それ以外の向きおよび位置を変えない手順

これらから (a) を満たす $S_E\times S_V$ の指数 2 の部分群が生成できる

第 2 基本定理からの帰結

$$
\begin{aligned}
G_0 = \{ \quad & (\vec{v}, r, \vec{w}, s) \mid r \in S_8,\ s \in S_{12}, \\
& \vec{v} = (v_1, v_2, \ldots, v_8), v_i \in \{0,1,2\}, v_1 + \ldots + v_8 \equiv 0 \pmod 3, \\
& \vec{w} = (w_1, w_2, \ldots, w_{12}), w_i \in \{0,1\}, w_1 + \ldots + w_{12} \equiv 0 \pmod 2) \}
\end{aligned}
$$

とする．G_0 には，3 面体の総捻り量保存および 2 面体の総反転量保存の条件はあるが，置換の奇偶性一致条件はない．2 項演算 $\cdot : G_0 \times G_0 \to G_0$ を次のように定義する．

$$
(\vec{v}, r, \vec{w}, s) \cdot (\vec{v}', r', \vec{w}', s') = (\vec{v} + P(r)(\vec{v}'), r \cdot r', \vec{w} + P(s)(\vec{w}'), s \cdot s')
$$

この 2 項演算により，G_0 は群となる．

$$
[H : G_0] = |H| / |G_0| = 6
$$

ルービックキューブ群 G

次の同型写像が存在する.

$$G_0 \cong (C_3^7 \rtimes S_8) \times (C_2^{11} \rtimes S_{12})$$

ルービックキューブ群 G は，次の準同型写像の核となる.

$$\begin{array}{ccc} \phi : G_0 & \longrightarrow & \{1, -1\} \\ (\vec{v}, r, \vec{w}, s) & \longmapsto & sgn(r)sgn(s) \end{array}$$

また，G は G_0 の指数 2 の正規部分群で

$$|G| = 8! \cdot 12! \cdot 2^{10} \cdot 3^7$$

となる.

剰余類

G を群とし， H を G の部分群とする．群の演算を乗法 $*$ で表記して，g を G の元とするとき，G の部分集合 $g * H = \{g * h | h \in H\}$ を G における H の**左剰余類**といい，G の部分集合 $H * g = \{h * g | h \in H\}$ を G における H の**右剰余類**という．
G が可換群の場合には，左剰余類と右剰余類は一致する．

完全代表系

H を G の部分群とし， C を G における H の左剰余類とする．G の元 g に対して，$C = g * H$ が成り立つとき，g を剰余類 C の**代表**という．G の部分集合 $\{x_1, x_2, \ldots, x_m\}$ で重複なしに (すなわち，すべての $x_i * H$ は互いに素となる)

$$G/H = \{x_1 * H, \ldots, x_m * H\}$$

となるものを**完全代表系**という．

部分群法

$G = \langle R, L, F, B, U, D \rangle$ をルービックキューブ群とし，部分群の系列

$$G_n = \{1\} \ \subset \ G_{n-1} \ \subset \ \cdots \ \subset \ G_1 \ \subset \ G_0 = G$$

を用いて次の処理を実行する.

- 与えられたルービックキューブの配置を元 $g_0 \in G$ とする.
- すべての $0 \leq k < n$ について，G_k/G_{k+1} の完全代表系

$$G_k/G_{k+1} = \bigcup_{i=1}^{r_k} g_{k+1,i} G_{k+1} \qquad (r_k > 1)$$

を決めておく.

部分群法

- (初期処理) (ある $i \in \{1, \ldots, r_1\}$ について) $g_0 \in g_{1,i}G_1$ となるとき，$g_1 = g_{1,i}$ および $g'_1 = g_1^{-1}g_0$ とする．($g'_1 \in G_1$ となる．)
- (再帰的処理) $g'_k \in G_k$ がすでに定義されていて，(ある $j \in \{1, \ldots, r_k\}$ について) $g'_k \in g_{k+1,j}G_{k+1}$ となるとき，$g_{k+1} = g_{k+1,j}$ および $g'_{k+1} = g_{k+1}^{-1}g'_k$ とする．($g'_{k+1} \in G_{k+1}$ となる．)
- 得られた値をすべてまとめると $1 = g_n^{-1}g_{n-1}^{-1}g_{n-2}^{-1} \cdots g_1^{-1}g_0$ となり，

$$g_0 = g_1 g_2 \cdots g_{n-1} g_n$$

がえられる．

コーナー/エッジ法

$$G_4 = \{1\} \ \subset \ G_3 \ \subset \ G_2 \ \subset \ G_1 \ \subset \ G_0 = G$$

- G_1 : どの 3 面体の位置を変えない部分群
- G_2 : どの 3 面体および 2 面体の位置も変えない部分群
- G_3 : どの 3 面体および 2 面体の位置も変えず，どの 3 面体の向きも変えない部分群
- $G_4 = \{1\}$

コーナー/エッジ法

1. $g_0 \in G$ を与えられたルービックキューブの配置とする．
2. g_1 を，すべての 3 面体を正しい位置に移す (すなわち，捻られていてもよいが，置換によってすべての 3 面体を揃った位置にあわせる) 手順とする．すると $g_1^{-1}g_0 \in G_1$ となる．ここで $g_1' = g_1^{-1}g_0$ とする．
3. g_2 を，すべての 2 面体を正しい位置に移し (すなわち，3 面体や 2 面体の向きが変わってもよいが，置換によってすべての 2 面体を揃った位置にあわせる)，3 面体の位置は変えない手順とする．すると $g_2^{-1}g_1' \in G_2$ となる．ここで $g_2' = g_2^{-1}g_1'$ とする．
4. g_3 を，どの小方体の位置も変えずに，すべての 3 面体を「揃える」(すなわち，2 面体を反転させてもよいが，3 面体を捻って正しい向きにする) 手順とする．すると $g_3^{-1}g_2' \in G_3$ となる．ここで $g_3' = g_3^{-1}g_2'$ とする．
5. g_4 を，すべての 2 面体を「揃え」て (すなわち，2 面体を反転させて正しい向きにする)，それ以外のどの小方体の位置も向きも変えない手順とする．
6. 最終的な解は $g_0 = g_1g_2g_3g_4$ となる．

シスルスゥエイト法

$$
\begin{aligned}
G_1 &= \langle R, L, F, B, U^2, D^2 \rangle, \\
G_2 &= \langle R, L, F^2, B^2, U^2, D^2 \rangle, \\
G_3 &= \langle R^2, L^2, F^2, B^2, U^2, D^2 \rangle, \\
G_4 &= \{1\}
\end{aligned}
$$

G_2 は $3 \times 3 \times 2$ のルービックドミノの群と同型で，位数は $(8!)^2 \cdot 12$ です.
G_3 は,「平方」群で，その位数は $2^{13} \cdot 3^4$ です.

シスルスウェイト法

- G/G_1 の完全代表系 $\{g_{1,i} \mid 1 \leq i \leq n_1\}$ で，すべての手順 $g_{1,i}$ が高々 7 手となるものがある．($n_1 = 2048$) この完全代表系に含まれる手順は，2 面体の向きを変えるだけ
- G_1/G_2 の完全代表系 $\{g_{2,i} \mid 1 \leq i \leq n_2\}$ で，すべての手順 $g_{2,i}$ が高々 13 手となるものがある．($n_2 = 1082565$) この完全代表系に含まれる手順は，3 面体の向きを変えるだけ
- G_2/G_3 の完全代表系 $\{g_{3,i} \mid 1 \leq i \leq n_3\}$ で，すべての手順 $g_{3,i}$ が高々 15 手となるものがある．($n_3 = 29400$) この完全代表系に含まれる手順は，すべての 3 面体および 2 面体を正しい位置に移す.
- G_3/G_4 の完全代表系 $\{g_{4,i} \mid 1 \leq i \leq n_4\}$ で，すべての手順 $g_{4,i}$ が高々 17 手となるものがある．($n_4 = 663552$)

これより，ルービックキューブのどんな配置も，高々 $7 + 13 + 15 + 17 = 52$ 手で解くことができる.

コシエンバ法

「2 段階アルゴリズム」部分群の系列の群を二つに減らした.

$$
\begin{aligned}
G_0 &= \langle L, R, F, B, U, D \rangle \\
G_1 &= \langle L, R, F^2, B^2, U^2, D^2 \rangle \\
G_2 &= 1
\end{aligned}
$$

第 1 段階：撹乱された配置を G_1 の元に移す手順を探します．G_1 は，3 面体および 2 面体の向きに制約を課し，上下方向の中間層にある 2 面体を同じ中間層に移す元からなります．この目的の状態を見つけるために，プログラムは反復深化 A*(IDA*) 法と呼ばれる探索アルゴリズムを使用する．(探索する手順の長さを延ばしながら表を引いてすべての手順上を反復する．)
第 2 段階：部分群 G_1 に含まれる配置に対して，この部分群に含まれる手順だけを使って，すべての面が揃った状態にする．この段階では，8 個の 3 面体の置換，上面および下面にある 8 個の 2 面体の置換，および上下方向の中間層にある 4 個の 2 面体の置換を行う．