Regular Paper

Square Subgroup of Rubik's Cube Group

Osamu Ikawa[1,a) Osamu Shimabukuro[2,b)]

Received: July 25, 2012, Accepted: January 11, 2013

Abstract: In this paper, we treat the subgroup of a Rubik's Cube group generated by using only half-turns of the faces. We describe the subgroup as the abstract group forms without using any computers.

Keywords: Rubik's Cube group, square subgroup

1. Introduction

Rubik's Cube has provided a fascination over the decades. The structure of a Rubik's Cube group interests many researchers. $2 \times 2 \times 2$ and $3 \times 3 \times 3$ Rubik's Cubes are treated in this paper. The set of all cube operations is a finite group whose binary operation is as composition of operations. We call this a Rubik's Cube group. We denote $2 \times 2 \times 2$ and $3 \times 3 \times 3$ Rubik's Cube groups by G_2 and G_3 respectively. Rotating faces by 90 degrees are generators of these groups. The square subgroup is the subgroup of the Rubik's Cube group generated by using only half-turns of the faces. We denote the square subgroups of $2 \times 2 \times 2$ and $3 \times 3 \times 3$ Rubik's Cube groups by Q_2 and Q_3 respectively. The order of Q_2 and Q_3 was calculated by Joyner [4] with GAP, which is a computer algebra program [2]. His book contains a chapter for the square group (Ref. [4], p.191). But he did not spend much effort to do it by hand, but rather used a computer at the end. If we used a computer, we could not know the reason why the properties of a Rubik's Cube group hold.

It is known that the Rubik's Cube group is decomposed into a chain of length two, using the square subgroup as the intermediate subgroup. Kunkle and Cooperman improved an upper bound of "God's number," which is the minimum number of moves required to solve any state of a Rubik's Cube, using a property of the square subgroup [3]. We need to analyze to the properties of a Rubik's Cube group to get a "God's number." Therefore, we attempt to study the square subgroup of a Rubik's Cube group to a simpler analysis of "God's number." In this paper, we describe Q_2 and Q_3 as the subgroups of G_2 and G_3 respectively without using a computer. By this, we describe Q_2 and Q_3 as the abstract group forms. Of course, we know the order of Q_2 and Q_3 by this.

The terminology used in this paper is as follows: $2 \times 2 \times 2$ and $3 \times 3 \times 3$ Rubik's Cubes are subdivided into some smaller cubes, which we call subcubes. There are three kinds of subcubes in a $3 \times 3 \times 3$ Rubik's Cube, that is, center, edge and corner subcubes. Here the center, edge and corner subcubes are one-face, two-face and three-face subcubes, respectively. A $2 \times 2 \times 2$ Rubik's Cube is subdivided into eight subcubes.

2. $2 \times 2 \times 2$ Square Subgroup

Let $\mathfrak{S}_n$ be the symmetric group of degree n, $\mathfrak{A}_n$ the alternating group of degree n, $\mathfrak{B}_n$ the complement of $\mathfrak{A}_n$ in $\mathfrak{S}_n$, and $\mathbb{Z}_k$ the abelian group $\mathbb{Z}/k\mathbb{Z}$. The group $\mathfrak{S}_n$ acts on $(\mathbb{Z}_k)^n$ naturally such that

$$\sigma(\mu_1, \cdots, \mu_n) = (\mu_{\sigma^{-1}(1)}, \cdots, \mu_{\sigma^{-1}(n)}) \quad \text{for} \quad \sigma \in \mathfrak{S}_n.$$

We define a subgroup T_k^n of $(\mathbb{Z}_k)^n$ by

$$T_k^n = \left\{ (\mu_1, \cdots, \mu_n) \in (\mathbb{Z}_k)^n \,\middle|\, \sum_{i=1}^n \mu_i = 0 \right\},$$

which is isomorphic to $(\mathbb{Z}_k)^{n-1}$. Since the action of $\mathfrak{S}_n$ on $(\mathbb{Z}_k)^n$ makes T_k^n invariant, we can define a semi-direct product $\mathfrak{S}_n \ltimes T_k^n$ as the following:

$$(\sigma_2, \nu_2)(\sigma_1, \nu_1) = (\sigma_2\sigma_1, \sigma_2\nu_1 + \nu_2)$$
$$\text{for} \quad \sigma_1, \sigma_2 \in \mathfrak{S}_n \text{ and } \nu_1, \nu_2 \in T_k^n.$$

Each inverse element of the group is given by

$$(\sigma, \nu)^{-1} = (\sigma^{-1}, -\sigma^{-1}\nu) \quad \text{for} \quad \sigma \in \mathfrak{S}_n \text{ and } \nu \in T_k^n.$$

Under the preparation for the above-mentioned notations, we shall briefly review that

$$G_2 = \mathfrak{S}_8 \ltimes T_3^8. \tag{1}$$

The group $\mathfrak{S}_8$ in Eq. (1) means that we can change the eight corner positions of each subcube of Rubik's Cube as desired. Each subcube has three distinct colors on their three exposed faces. The color orientation of each subcube is expressible in an element of $\mathbb{Z}_3$. The group T_3^8 means that the sum of the color orientations ($\in \mathbb{Z}_3$) is a conservative constant by operating on a Rubik's Cube (Ref. [4], §11.2.1). Conversely it is known that every element of $\mathfrak{S}_8 \ltimes T_3^8$ can be realized by an element of G_2. Hence we get the above expression. Note that G_2 is isomorphic to a group generated by operations of corner subcubes in a $3\times3\times3$ Rubik's Cube.

[1] Department of Mathematical and Physical Sciences, Faculty of Arts and Sciences, Kyoto Institute of Technology, Kyoto 606–8585, Japan

[2] Faculty of Engineering, General Education (Mathematics), Sojo University, Ikeda, Kumamoto 860–0082, Japan

[a)] ikawa@kit.ac.jp

[b)] osamu@ed.sojo-u.ac.jp

In Cotten's theses readers can study about the properties of G_2 in more details [1].

Let's consider the square subgroup Q_2. The rotations of 90 degrees induce the cyclic permutations of length 4 to the positions of the corner subcubes. These are odd permutations. Thus the rotations of 180 degrees induce even permutations to the positions of the corner subcubes. The color orientation of each corner subcube does not change by these rotations of 180 degrees. Hence Q_2 is a subgroup of $\mathfrak{A}_8$. When Q_2 acts on corner subcubes, there are two orbits and each orbit has four corner subcubes. We call these orbits $\{1,3,5,7\}$ and $\{2,4,6,8\}$ (refer to **Fig. 1**). We define subgroups $\mathfrak{S}_4^{(o)}$ and $\mathfrak{S}_4^{(e)}$ of $\mathfrak{S}_8$ as follows:

$$\begin{aligned}\mathfrak{S}_4^{(o)} &= \{\sigma \in \mathfrak{S}_8 \mid \sigma(k) = k \quad (k = 2,4,6,8)\}(\cong \mathfrak{S}_4),\\ \mathfrak{S}_4^{(e)} &= \{\sigma \in \mathfrak{S}_8 \mid \sigma(k) = k \quad (k = 1,3,5,7)\}(\cong \mathfrak{S}_4),\end{aligned}$$

and denote by $\tilde{f}$ the isomorphism from $\mathfrak{S}_4^{(o)}$ onto $\mathfrak{S}_4^{(e)}$ which is induced from a bijection $f : \{1,3,5,7\} \to \{2,4,6,8\}; i \mapsto i+1$. Then $\mathfrak{S}_4^{(o)} \times \mathfrak{S}_4^{(e)}$ is a subgroup of $\mathfrak{S}_8$. Denote by $\mathfrak{A}_4^{(o)}$ the alternating group of $\mathfrak{S}_4^{(o)}$, and put $\mathfrak{B}_4^{(o)} = \mathfrak{S}_4^{(o)} - \mathfrak{A}_4^{(o)}$. For an element $x_{(o)} \in \mathfrak{S}_4^{(o)}$ and a subset $X^{(o)} \subset \mathfrak{S}_4^{(o)}$, put $x_{(e)} = \tilde{f}(x_{(o)})$ and $X^{(e)} = \tilde{f}(X^{(o)})$, respectively. Define a subgroup Q_2^* of G_2 by

$$\begin{aligned}Q_2^* &= \{(\sigma,\tau) \in \mathfrak{S}_4^{(o)} \times \mathfrak{S}_4^{(e)} \mid \epsilon(\sigma) = \epsilon(\tau)\}\\ &= (\mathfrak{A}_4^{(o)} \times \mathfrak{A}_4^{(e)}) \cup (\mathfrak{B}_4^{(o)} \times \mathfrak{B}_4^{(e)}),\end{aligned}$$

where ϵ is the signature of a permutation. Then we have

$$Q_2 \subset Q_2^* \subset \mathfrak{A}_8 \subset \mathfrak{S}_8 \subset G_2.$$

To study Q_2 in detail, the positions of each subcube of a $2 \times 2 \times 2$ Rubik's Cube are labeled. The positions of each subcube of a $3 \times 3 \times 3$ Rubik's Cube need to be labeled later. We label the positions of each subcube of the $3 \times 3 \times 3$ Rubik's Cube and regard the corner subcube of the $3 \times 3 \times 3$ Rubik's Cube as the position of each subcube of a $2 \times 2 \times 2$ Rubik's Cube. Each of center subcubes is labeled 'U', 'F', 'D', 'L', 'R' and 'B' after Up, Front, Down, Left, Right and Back. The positions of corner subcubes and edge subcubes are labeled as the following.

We denote rotation of the faces 'U', 'D', 'R', 'L', 'F' and 'B' anti-clockwise by g_U, g_D, g_R, g_L, g_F and g_B, respectively. Then

$$\begin{aligned}g_U^2 &= (5,7)(6,8), \quad g_D^2 = (1,3)(2,4), \quad g_R^2 = (1,7)(4,6),\\ g_L^2 &= (3,5)(2,8), \quad g_F^2 = (1,5)(2,6), \quad g_B^2 = (3,7)(4,8),\end{aligned}$$

where (i,j) is a transposition. We get the following formulae immediately.

			8	(8)	7						
			(5)	U	(7)						
			5	(6)	6						
□	□	□	□	□	□	□	□	□	□	□	□
□	L	(12)	□	F	(11)	□	R	(10)	□	B	(9)
□	□	□	□	□	□	□	□	□	□	□	□
			2	(1)	1						
			(2)	D	(4)						
			3	(3)	4						

Fig. 1 Labeled Rubik's Cube.

Formula 1.

$$\begin{aligned}&g_D^2 g_L^2 g_D^2 g_F^2 = (2,6)(4,8), \ g_D^2 g_F^2 g_D^2 g_L^2 = (2,8)(4,6),\\ &g_L^2 g_F^2 g_L^2 g_D^2 = (2,4)(6,8), \qquad (2)\\ &g_D^2 g_R^2 g_D^2 g_F^2 = (1,5)(3,7), \ g_D^2 g_F^2 g_D^2 g_R^2 = (1,7)(3,5),\\ &g_R^2 g_F^2 g_R^2 g_D^2 = (1,3)(5,7), \qquad (3)\\ &g_D^2 g_F^2 = (1,5,3)(2,6,4), \qquad (4)\end{aligned}$$

where $g_D^2 g_F^2$ means the first operation g_F^2 and the second g_D^2. For instance $(1,5,3)$ is a cyclic permutation $1 \to 5 \to 3 \to 1$.

The group $\mathfrak{A}_4^{(o)}$ has a unique subgroup $V^{(o)}$ of order 4, that is,

$$V^{(o)} = \{1, (1,3)(5,7), (1,5)(3,7), (1,7)(3,5)\} \cong (\mathbb{Z}_2)^2.$$

Then $V^{(o)}$ is a normal subgroup of $\mathfrak{A}_4^{(o)}$, which is abelian. We have

$$\mathfrak{A}_4^{(o)} = V^{(o)} \cup \{(1,3,5)^{\pm 1}, (3,7,5)^{\pm 1}, (1,5,7)^{\pm 1}, (1,7,3)^{\pm 1}\}.$$

Define $a_{(o)} = (1,5,3) \in \mathfrak{A}_4^{(o)} - V^{(o)}$ and $b_{(o)} = (1,3) \in \mathfrak{B}_4^{(o)}$ then $a_{(e)} = (2,6,4)$ and $g_D^2 = b_{(o)} b_{(e)}$.

Formula 2. *Define $a_{(o)} = (1,5,3)$ and $b_{(o)} = (1,3)$, then the following holds.*

$$\begin{aligned}g_U^2 g_D^2 &= g_D^2 g_U^2 = (1,3)(5,7)(2,4)(6,8) \in V^{(o)} \times V^{(e)},\\ g_R^2 g_L^2 &= g_L^2 g_R^2 = (1,7)(3,5)(2,8)(4,6) \in V^{(o)} \times V^{(e)},\\ g_F^2 g_B^2 &= g_B^2 g_F^2 = (1,5)(2,6)(3,7)(4,8) \in V^{(o)} \times V^{(e)},\\ g_U^2 g_R^2 &= (1,5,7)(4,8,6) \in a_{(o)}^2 V^{(o)} \times a_{(e)}^2 V^{(e)},\\ g_U^2 g_L^2 &= (3,7,5)(2,6,8) \in a_{(o)}^2 V^{(o)} \times a_{(e)}^2 V^{(e)},\\ g_U^2 g_F^2 &= (1,7,5)(2,8,6) \in a_{(o)} V^{(o)} \times a_{(e)} V^{(e)},\\ g_U^2 g_B^2 &= (3,5,7)(4,6,8) \in a_{(o)} V^{(o)} \times a_{(e)} V^{(e)},\\ g_D^2 g_R^2 &= (1,7,3)(2,4,6) \in a_{(o)}^2 V^{(o)} \times a_{(e)}^2 V^{(e)},\\ g_D^2 g_L^2 &= (1,3,5)(2,8,4) \in a_{(o)}^2 V^{(o)} \times a_{(e)}^2 V^{(e)},\\ g_D^2 g_F^2 &= (1,5,3)(2,6,4) \in a_{(o)} V^{(o)} \times a_{(e)} V^{(e)},\\ g_D^2 g_B^2 &= (1,3,7)(2,4,8) \in a_{(o)} V^{(o)} \times a_{(e)} V^{(e)},\\ g_R^2 g_F^2 &= (1,5,7)(2,4,6) \in a_{(o)}^2 V^{(o)} \times a_{(e)}^2 V^{(e)},\\ g_R^2 g_B^2 &= (1,7,3)(4,8,6) \in a_{(o)}^2 V^{(o)} \times a_{(e)}^2 V^{(e)},\\ g_L^2 g_F^2 &= (1,3,5)(2,6,8) \in a_{(o)}^2 V^{(o)} \times a_{(e)}^2 V^{(e)},\\ g_L^2 g_B^2 &= (3,7,5)(2,8,4) \in a_{(o)}^2 V^{(o)} \times a_{(e)}^2 V^{(e)}.\end{aligned}$$

Theorem 3. *Put $a_{(o)} = (1,5,3)$ and $b_{(o)} = (1,3)$, then*

$$\begin{aligned}Q_2 = &(V^{(o)} \times V^{(e)}) \cup (a_{(o)} V^{(o)} \times a_{(e)} V^{(e)}) \cup (a_{(o)}^2 V^{(o)} \times a_{(e)}^2 V^{(e)})\\ &\cup (b_{(o)} V^{(o)} \times b_{(e)} V^{(e)}) \cup (b_{(o)} a_{(o)} V^{(o)} \times b_{(e)} a_{(e)} V^{(e)})\\ &\cup (b_{(o)} a_{(o)}^2 V^{(o)} \times b_{(e)} a_{(e)}^2 V^{(e)}).\end{aligned}$$

Proof. Define a subgroup $\tilde{Q}_2$ of Q_2^* by

$$\begin{aligned}\tilde{Q}_2 = &(V^{(o)} \times V^{(e)}) \cup (a_{(o)} V^{(o)} \times a_{(e)} V^{(e)}) \cup (a_{(o)}^2 V^{(o)} \times a_{(e)}^2 V^{(e)})\\ &\cup (b_{(o)} V^{(o)} \times b_{(e)} V^{(e)}) \cup (b_{(o)} a_{(o)} V^{(o)} \times b_{(e)} a_{(e)} V^{(e)})\\ &\cup (b_{(o)} a_{(o)}^2 V^{(o)} \times b_{(e)} a_{(e)}^2 V^{(e)}).\end{aligned}$$

We shall show $\tilde{Q}_2 \subset Q_2$. By Formula 1 Eq. (2), $\{1\} \times V^{(e)} \subset Q_2$. By Formula 1 Eq. (3), $V^{(o)} \times \{1\} \subset Q_2$. Thus $V^{(o)} \times V^{(e)} \subset Q_2$. By Formula 1 Eq. (4), $a_{(o)} a_{(e)} = g_D^2 g_F^2 \in Q_2$. Hence

$$(V^{(o)} \times V^{(e)}) \cup (a_{(o)} V^{(o)} \times a_{(e)} V^{(e)}) \cup (a_{(o)}^2 V^{(o)} \times a_{(e)}^2 V^{(e)}) \subset Q_2.$$

Since $b_{(o)}b_{(e)} = g_D^2 \in Q_2$, we have $\tilde{Q}_2 \subset Q_2 \subset Q_2^*$. Because $\#(\tilde{Q}_2) = 2^5 \cdot 3$ and $\#(Q_2^*) = 2^5 \cdot 3^2$, we have $Q_2 = \tilde{Q}_2$ or $Q_2 = Q_2^*$. Since the following isomorphism holds:

$$\mathfrak{A}_4^{(o)}/V^{(o)} = \{V^{(o)}, a_{(o)}V^{(o)}, a_{(o)}^2V^{(o)}\} \cong \mathbb{Z}_3,$$

the group $\mathfrak{A}_4^{(o)}/V^{(o)}$ is abelian. Since $Q_2 \subset Q_2^*$,

$$Q_2 = (Q_2 \cap (\mathfrak{A}_4^{(o)} \times \mathfrak{A}_4^{(e)})) \cup (Q_2 \cap (\mathfrak{B}_4^{(o)} \times \mathfrak{B}_4^{(e)})).$$

Define a normal subgroup N of Q_2 by

$$N = Q_2 \cap (\mathfrak{A}_4^{(o)} \times \mathfrak{A}_4^{(e)}), \qquad (5)$$

then the set $\{g_\alpha^2 g_\beta^2 \mid \alpha, \beta = U, D, R, L, F, B\}$ is a generator system of N. Denote by φ the natural projection from $\mathfrak{A}_4^{(o)}$ onto $\mathfrak{A}_4^{(o)}/V^{(o)}$. Then the map defined by

$$F : \mathfrak{A}_4^{(o)} \times \mathfrak{A}_4^{(e)} \to \mathfrak{A}_4^{(o)}/V^{(o)}; (x_{(o)}, y_{(e)}) \mapsto \varphi(x_{(o)}y_{(o)}^{-1})$$

is a surjective homomorphism since $\mathfrak{A}_4^{(o)}/V^{(0)}$ is an abelian group, and

$$\begin{aligned}\mathrm{Ker}\, F &= (V^{(o)} \times V^{(e)}) \cup (a_{(o)}V^{(o)} \times a_{(e)}V^{(e)}) \cup (a_{(o)}^2V^{(o)} \times a_{(e)}^2V^{(e)}) \\ &\not\supset \mathfrak{A}_4^{(o)} \times \mathfrak{A}_4^{(e)} = Q_2^* \cap (\mathfrak{A}_4^{(o)} \times \mathfrak{A}_4^{(e)}).\end{aligned}$$

By Formula 2, $N \subset \mathrm{Ker}\, F$. Thus $Q_2 \neq Q_2^*$. Therefore Q_2 must be equal to $\tilde{Q}_2$. □

Applying Theorem 3, we know many facts. For instance, we know that it is impossible to get the following state (**Fig. 2**) of a Rubik's Cube using only a half-turn of the faces since the state corresponds to $((1, 3, 5), 1) \in Q_2^* - Q_2$.

In the rest of this section, we study the structure of the normal subgroup N of Q_2 defined by Eq. (5). We prepare the following formulae in order to do this.

Formula 4. *Put* $a_{(o)} = (1, 5, 3)$*, then*

$$\begin{aligned}a_{(o)}(1, 3)(5, 7) &= (1, 5)(3, 7)a_{(o)} = (3, 5, 7),\\ a_{(o)}(1, 5)(3, 7) &= (1, 7)(3, 5)a_{(o)} = (1, 3, 7),\\ a_{(o)}(1, 7)(3, 5) &= (1, 3)(5, 7)a_{(o)} = (1, 7, 5).\end{aligned}$$

For $a_{(o)} = (1, 5, 3)$, define an automorphism $\sigma_{(o)}$ of $V^{(o)}$ by $xa_{(o)} = a_{(o)}\sigma(x)$ $(x \in V^{(o)})$. Since $xa_{(o)}^2 = a_{(o)}\sigma_{(o)}(x)a_{(o)} = a_{(o)}^2\sigma_{(o)}^2(x)$, $\ldots$, we have $xa_{(o)}^k = a_{(o)}^k\sigma_{(o)}^k(x)$. For $x \in V^{(o)}$, the value of $\sigma_{(o)}(x)$ is calculated by Formula 4. A homomorphism $\varphi_{(o)} : \mathbb{Z}_3 = \{1, a_{(o)}, a_{(o)}^2\} \to \mathrm{Aut}(V^{(o)})$ is defined by $\varphi_{(o)}(a_{(o)}^k)(x) = \sigma_{(o)}^k(x)$. Identifying $\mathbb{Z}_3$ with $\{1, a_{(e)}, a_{(e)}^2\}$ we can define an automorphism $\sigma_{(e)}$ of $V^{(e)}$ and a homomorphism $\varphi_{(e)}$ from $\mathbb{Z}_3$ into $\mathrm{Aut}(V^{(e)})$ in a similar way. Define a homomorphism $(\varphi_{(o)}, \varphi_{(e)}) : \mathbb{Z}_3 \to \mathrm{Aut}(V^{(o)} \times V^{(e)})$ by $a_{(o)}^k \mapsto (\varphi_{(o)}(a_{(o)}^k), \varphi_{(e)}(a_{(e)}^k))$.

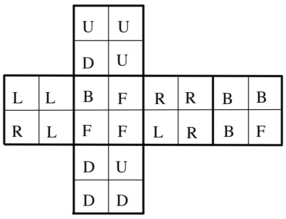

Fig. 2 Example.

We can define a semi-direct product $\mathbb{Z}_3 \ltimes (V^{(o)} \times V^{(e)})$ as the following:

$$(a_{(o)}^k, x_1, y_1)(a_{(o)}^l, x_2, y_2) = (a_{(o)}^{k+l}, (x_2, y_2)(\varphi_{(o)}, \varphi_{(e)})(a_{(o)}^l)(x_1, y_1)).$$

Then

$$\begin{aligned}(a_{(o)}^k, x_1, y_1)(a_{(o)}^l, x_2, y_2) &= (a_{(o)}^{k+l}, (x_2, y_2)(\varphi_{(o)}(a_{(o)}^l)x_1, \varphi_{(e)}(a_{(e)}^l)y_1))\\ &= (a_{(o)}^{k+l}, x_2\sigma_{(o)}^l(x_1), y_2\sigma_{(e)}^l(y_1)). \qquad (6)\end{aligned}$$

Thanks to Theorem 3, the normal subgroup N defined by Eq. (5) is expressed as

$$N = (V^{(o)} \times V^{(e)}) \cup (a_{(o)}V^{(o)} \times a_{(e)}V^{(e)}) \cup (a_{(o)}^2V^{(o)} \times a_{(e)}^2V^{(e)}).$$

Joyner gave the following propositions without proofs [4]. Our results derive the proofs.

Proposition 5. (Ref. [4], p. 191) $N \cong \mathbb{Z}_3 \ltimes (V^{(o)} \times V^{(e)}) \cong \mathbb{Z}_3 \ltimes (\mathbb{Z}_2)^4$.

Proof. A simple calculation using Formula 4 and Eq. (6) implies that the bijection defined by $F : \mathbb{Z}_3 \ltimes (V^{(o)} \times V^{(e)}) \to N; (a_{(o)}^k, x, y) \mapsto (a_{(o)}^k x, a_{(e)}^k y)$ is a group isomorphism. □

Proposition 6. (Ref. [4], p. 191) *For any subcube, the stabilizer of the subcube which the square subgroup Q_2 acts on 2 × 2 × 2 Rubik's Cube is isomorphic to $\mathfrak{S}_4$.*

Proof. Since the orbits of the corner subcube 1 and 2 are $\{1, 3, 5, 7\}$ and $\{2, 4, 6, 8\}$ respectively, it is sufficient to prove that both stabilizer $\mathrm{Stab}(Q_2 : 1)$ and $\mathrm{Stab}(Q_2 : 2)$ are isomorphic to $\mathfrak{S}_4$. In Q_2, the stabilizer $\mathrm{Stab}(Q_2 : 1)$ is expressed by the following equation:

$$\begin{aligned}\mathrm{Stab}(Q_2 : 1) = {} & (\{1\} \times V^{(e)}) \cup (\{(3, 5, 7)\} \times a_{(e)}V^{(e)})\\ & \cup (\{(3, 5, 7)^2\} \times a_{(e)}^2V^{(e)}) \cup (\{(5, 7)\} \times b_{(e)}V^{(e)})\\ & \cup (\{(5, 7)(3, 5, 7)\} \times b_{(e)}a_{(e)}V^{(e)})\\ & \cup (\{(5, 7)(3, 5, 7)^2\} \times b_{(e)}a_{(e)}^2V^{(e)}).\end{aligned}$$

Hence the map $\mathrm{Stab}(Q_2 : 1) \to \mathfrak{S}_4; (x, y) \mapsto y$ is an isomorphism. Similarly we get $\mathrm{Stab}(Q_2 : 2) \cong \mathfrak{S}_4$. □

3. 3 × 3 × 3 Square Subgroup

Let's briefly review that the 3 × 3 × 3 Rubik's Cube group G_3 is given by

$$G_3 = ((\mathfrak{A}_8 \ltimes T_3^8) \times (\mathfrak{A}_{12} \ltimes T_2^{12})) \cup ((\mathfrak{B}_8 \ltimes T_3^8) \times (\mathfrak{B}_{12} \ltimes T_2^{12})). \qquad (7)$$

Since the relative positions of the corner subcubes are invariant, we may fix them. The motion of corner subcubes of a 3 × 3 × 3 Rubik's Cube are the same as that of a 2 × 2 × 2 Rubik's Cube. There are twelve edge subcubes of a 3 × 3 × 3 Rubik's Cube. The position of each edge subcube of a 3 × 3 × 3 Rubik's Cube is shifted as we like. Each edge subcube has two distinct colors on their two exposed faces. The color orientation of each edge subcube is expressed by an element of $\mathbb{Z}_2$. The group T_2^{12} in Eq. (7) means that the sum of color orientations ($\in \mathbb{Z}_2$) of the edge subcubes is a conservative constant. Each turn of a face by

90 degrees induces a cyclic permutation of length 4 to both the position of a corner subcube and an edge subcube. The cyclic permutation of length 4 is an odd permutation. Hence for each state of a Rubik's Cube, the signature of the position permutation of the corner subcube coincides with that of the position of the edge subcube. Conversely it is known that every element of the group in the right-hand side of Eq. (7) can be realized by an element of G_3. Therefore we get the above expression. Readers can study about the properties of G_3 in Cotten's theses and Joyner's book in more details [1], [4].

Now we consider the square subgroup Q_3. Each turn of a face by 180 degrees induces an even permutation of length 4 to both the position of a corner subcube and an edge subcube. The orientations of each edge subcube and each corner subcube are unchanged. Thus Q_3 is a subgroup of $\mathfrak{A}_8 \times \mathfrak{A}_{12}$. The action of Q_3 on corner subcubes is the same as that of Q_2. When Q_3 acts on edge subcubes, there are three orbits and each orbit has four edge subcubes. In Fig. 1, these orbits are

$$[i] = \{1,3,6,8\}, \quad [ii] = \{2,4,5,7\} \quad \text{and} \quad [iii] = \{9,10,11,12\}.$$

Hence we can define three subgroups $\mathfrak{S}_4^{[i]}$, $\mathfrak{S}_4^{[ii]}$ and $\mathfrak{S}_4^{[iii]}$ of $\mathfrak{S}_{12}$, which are isomorphic to $\mathfrak{S}_4$, such that $\mathfrak{S}_4^{[i]} \times \mathfrak{S}_4^{[ii]} \times \mathfrak{S}_4^{[iii]}$ is a subgroup of $\mathfrak{S}_{12}$ in a similar manner as in Section 2. Define a subgroup Q_3^* of G_3 by

$$\begin{aligned} Q_3^* = Q_2 \times \{(\sigma_1,\sigma_2,\sigma_3) \in \mathfrak{S}_4^{[i]} \times \mathfrak{S}_4^{[ii]} \times \mathfrak{S}_4^{[iii]} \\ \mid \epsilon(\sigma_1)\epsilon(\sigma_2)\epsilon(\sigma_3) = 1\}, \end{aligned}$$

then we have

$$Q_3 \subset Q_3^* \subset \mathfrak{A}_8 \times \mathfrak{A}_{12} \subset G_3.$$

Obviously $\#(Q_3^*) = 2^{13} \cdot 3^4$ holds.

Concerning generators of Q_3, the following holds.

$$\begin{aligned} g_U^2 &= (5,7)_C(6,8)_C(5,7)_E(6,8)_E, \\ g_D^2 &= (1,3)_C(2,4)_C(1,3)_E(2,4)_E, \\ g_R^2 &= (1,7)_C(4,6)_C(4,7)_E(10,11)_E, \\ g_L^2 &= (3,5)_C(2,8)_C(2,5)_E(9,12)_E, \\ g_F^2 &= (1,5)_C(2,6)_C(1,6)_E(11,12)_E, \\ g_B^2 &= (3,7)_C(4,8)_C(3,8)_E(9,10)_E, \end{aligned}$$

where subscripts C and E mean the position of the corner subcube and the edge subcube, respectively. By the above equations, the following formula is obtained.

Formula 7.

$$g_U^2 g_R^2 g_L^2 g_D^2 g_R^2 g_L^2 = (1,3)_E(6,8)_E, \tag{8}$$

$$g_U^2 g_R^2 g_F^2 g_R^2 g_U^2 g_R^2 g_F^2 g_R^2 = (1,6,8)_E, \tag{9}$$

$$\begin{aligned} &g_U^2 g_R^2 g_F^2 g_L^2 g_F^2 g_L^2 g_U^2 g_L^2 g_U^2 g_R^2 g_B^2 g_D^2 g_B^2 g_D^2 g_R^2 g_B^2 g_D^2 g_F^2 g_U^2 g_L^2 g_U^2 g_F^2 \\ &= (5,7)_E(6,8)_E. \end{aligned} \tag{10}$$

The following theorem is the main result of this paper.

Theorem 8. $Q_3 = Q_2 \times \{(\sigma_1,\sigma_2,\sigma_3) \in \mathfrak{S}_4^{[i]} \times \mathfrak{S}_4^{[ii]} \times \mathfrak{S}_4^{[iii]} \mid \epsilon(\sigma_1)\epsilon(\sigma_2)\epsilon(\sigma_3) = 1\}$.

Proof. It is sufficient to prove that $Q_3^* \subset Q_3$ since we proved $Q_3 \subset Q_3^*$. By Formula 7 Eq. (8), $(1,3)_E(6,8)_E \in Q_3$. Since $(1,6)_E(3,8)_E$ is conjugate to $(1,3)_E(6,8)_E \in Q_3$ by an inverse of the element in Formula 7 Eq. (9), $(1,6)_E(3,8)_E \in Q_3$. We can define subgroups $\mathfrak{A}_4^{[k]}$ and $V^{[k]}$ and a subset $\mathfrak{B}^{[k]}$ of $\mathfrak{S}_4^{[k]}$ for $k = i, ii$ and iii as in Section 2. Since $V^{[i]}$ is generated by $(1,3)_E(6,8)_E$ and $(1,6)_E(3,8)_E$, we have $V^{[i]} \times \{1\} \times \{1\} \subset Q_3$. By Formula 7 Eq. (9), $(1,6,8)_E \in Q_3$. Since $\mathfrak{A}_4^{[i]}$ is generated by $(1,6,8)_E$ and $V^{[i]}$, we have $\mathfrak{A}_4^{[i]} \times \{1\} \times \{1\} \subset Q_3$. Similarly, $(\{1\} \times \mathfrak{A}_4^{[ii]} \times \{1\}) \cup (\{1\} \times \{1\} \times \mathfrak{A}_4^{[iii]}) \subset Q_3$. Therefore $\mathfrak{A}_4^{[i]} \times \mathfrak{A}_4^{[ii]} \times \mathfrak{A}_4^{[iii]} \subset Q_3$. By Formula 7 Eq. (10), $(6,8)_E(5,7)_E \in Q_3$ holds. Hence

$$(6,8)_E \mathfrak{A}_4^{[i]} \times (5,7)_E \mathfrak{A}_4^{[ii]} \times \mathfrak{A}_4^{[iii]} = \mathfrak{B}_4^{[i]} \times \mathfrak{B}_4^{[ii]} \times \mathfrak{A}_4^{[iii]} \subset Q_3.$$

Similarly, $(\mathfrak{B}_4^{[i]} \times \mathfrak{A}_4^{[ii]} \times \mathfrak{B}_4^{[iii]}) \cup (\mathfrak{A}_4^{[i]} \times \mathfrak{B}_4^{[ii]} \times \mathfrak{B}_4^{[iii]}) \subset Q_3$. By these relations,

$$\begin{aligned} &\{1\} \times \{(\sigma_1,\sigma_2,\sigma_3) \in \mathfrak{S}_4^{[i]} \times \mathfrak{S}_4^{[ii]} \times \mathfrak{S}_4^{[iii]} \mid \epsilon(\sigma_1)\epsilon(\sigma_2)\epsilon(\sigma_3) = 1\} \\ &\subset Q_3. \end{aligned}$$

By Formula 7 Eq. (10),

$$Q_3 \ni g_U^2 (5,7)_E(6,8)_E = (5,7)_C(6,8)_C.$$

Similarly, since generators of $Q_2 \times \{1\}$ are elements of Q_3, $Q_2 \times \{1\} \subset Q_3$. Hence $Q_3^* \subset Q_3$. □

Acknowledgments The authors would like to thank the referees for their suggestions for improving this paper. The first author was partially supported by the Grant-in-Aid for Scientific Research (# 22540108), Japan Society for Promotion of Science.

References

[1] Cotten, A.: The Group Theoretic Rubik's Cube, Senior Honors Theses, Paper 136 (2009), available from ⟨http://commons.emich.edu/honors/136⟩.

[2] The GAP Group: GAP - Groups, Algorithms, and Programming, Version 4.4.12 (2008), available from ⟨http://www.gap-system.org/⟩.

[3] Kunkle, D. and Cooperman, G.: Twenty-Six Moves Suffice for Rubik's Cube, *Proc. International Symposium on Symbolic and Algebraic Computation (ISSAC '07)*, ACM Press (2007).

[4] Joyner, D.: *Adventures in Group Theory*, The Johns Hopkins University Press, Baltimore and London (2002).

Osamu Ikawa was born in 1965. He received his Ph.D. degree from University of Tsukuba in 1998. He became a professor at Kyoto Institute of Technology in 2012. He has been interested in Rubik's Cube since he was high school student. His research interest is geometry.

Osamu Shimabukuro was born in 1974. He received his Ph.D. from Kyushu University in 2004. He became a lecturer at Fukushima National College of Technology in 2005 and an associate professor at Sojo University in 2012. His current research interest is algebraic combinatorics.