THE FIRST LAW OF CUBOLOGY FOR THE RUBIK’S REVENGE

STEFANO BONZIO — ANDREA LOI — LUISA PERUZZI

(COMMUNICATION BY ANATOLIJ DVUREČENSKIJ)

ABSTRACT. We state and prove the first law of cubology of the Rubik’s Revenge and provide necessary and sufficient conditions for a randomly assembled Rubik’s Revenge to be solvable.

©2017

Mathematical Institute
Slovak Academy of Sciences

1. Introduction

Erno Rubik, in 1974, invented the most famous and appreciated puzzle of all times that still goes under his name as Rubik’s Cube. A few years later, in 1981, Peter Sebesteny, following Rubik’s idea, invented his own cube, called the Rubik’s Revenge, as it was meant to be a more difficult puzzle with respect to the original.

The Rubik’s Cube attracted the attention of many mathematicians (see, e.g., [2], [9], [10]) and in most cases they successfully gave a group theoretical analysis and solution to the puzzle. The puzzle fascinated also computer scientists, whose interests are mainly focused in the God’s number, namely the least number of moves needed to solve the Cube from any position, see for example [17], [14], [16], [11], [6]. Strategies strictly connected to the Rubik’s Cube have been recently applied also in cryptography [18], [7], while some physicists were inspired by the Cube as a model for complex systems of different kinds [5], [13].

Any Cubemaster knows that dismantling the cube and reassembling it randomly may cause in most of the cases the puzzle not to be solvable anymore. A question arises naturally: under which conditions a cube is solvable? The answer came a few years after the Cube was born. Indeed, Bandelow [2] has provided necessary and sufficient conditions for the solvability of the cube in a Theorem which he has christened “the first law of cubology” (see Theorem 2.1 below). As far as we know, the same question has not been answered for the Rubik’s Revenge. Our aim is then providing an answer to this question.

The paper is structured as follows: in the first section we present a review of the main interesting results, in our perspective, concerning Rubik’s Cube. In the second section we go through the analysis of Rubik’s Revenge and state Theorem 3.1 which represents “the first law of cubology” for it, and prove some corollaries of our analysis. For example we provide necessary and sufficient conditions for a randomly assembled Rubik’s Revenge to be solvable. Our proof is based on the algebraic tools on the Rubik’s Revenge developed in [12]. To authors’ best knowledge reference [12] is the only place where a group theoretical approach to the Revenge is given (the reader is
referred e.g. to [1] and to several places in the web for the description of the instructions needed to solve the Rubik’s Revenge).

2. Review on the Rubik’s Cube

The Rubik’s cube is composed by 26 small cubes, which we will refer to as “cubies” (as in [4]). A quick look and one can notice that 8 are corner cubies, i.e. cubies with 3 visible coloured faces, 12 are edge cubies, with just 2 visible faces and the remaining 6 have one visible face: the center cubies.

The cube, obviously, has 6 faces, each of which can be moved clockwise or anticlockwise. Moving a face implies the movement of any of the cubies lying in the moved slice, with the exception of the center piece, occupying the same (spatial) position (centers are fixed).

Solving the cube means having every face of a unique colour: centers, being fixed, establish which colour the face shall have. For example, if one sees a face with the center coloured in white, when the cube is solved, the whole face will be of white colour. Of course, the same applies to all the other faces.

Any Cubemaster knows that if the cube is disassembled and then reassembled randomly, it may happen that it is not solvable anymore, as pieces shall be assembled following a precise pattern. On the other hand, mathematicians know that such problems can be studied using group theory [9], [12], [10], [8].

It is easily verified that the moves of the cube form a group, generated by the basic moves, generally referred to as $R, L, F, B, U, D$ (as in [2] and [10]).

Corner and edge cubies can be moved as well as twisted, so they can change position (in space) as well as orientation. Hence, a natural way to describe a pattern is introducing permutations for position changes and orientation for twisting. In this way, a random pattern corresponds to a configuration, that can be described by a 4-tuple $(\sigma, \tau, x, y)$, as done in [2]. Permutations involving corner cubies are necessarily disjoint from the ones involving edges, as this is imposed by the construction of the cube itself. So $\sigma$ refers to a permutation of corners, while $\tau$ is a permutation on edges. Thus, in principle, $\sigma \in S_8$, while $\tau \in S_{12}$. When the cube is solved, clearly $\sigma = \text{id}_{S_8}$ and $\tau = \text{id}_{S_{12}}$.

Orientations can be characterized using vectors. As corners are eight and they have three visible faces, they may assume three possible different orientations, so the vector describing corners’ orientation is $x \in (\mathbb{Z}_3)^8$; while edge cubies are twelve, but they have only two possible orientation, the vector is $y \in (\mathbb{Z}_2)^{12}$.

Let us make clear how to calculate a random configuration of the Rubik’s Cube. We assume the convention that we look at the Cube in order to have the white face on top and the red in front. Then we associate a number to the spatial position of each corner as well as of each edge. We assign a number from 1 to 8 to the position occupied by each corner. We number 1 the up-front-left corner and then associate numbers 2, 3, 4 just counting the others standing in the upper face clockwise. For corners standing in the down face, the down-front-left corner is assigned number 5 and the others take 6, 7 and 8 counting clockwise.

The same can be done with respect to edges: we assign numbers from 1 to 4 for the spatial positions of edges in the up face, starting from the front-up and counting then clockwise on the upper face. We number 5 the front-left position in the middle layer and then counting clockwise

\footnote{The idea is suggested by Bandelow [2] who uses the suggestive terminology of “second skin” for the spatial positions occupied by cubies.}
THE FIRST LAW OF CUBOLOGY FOR THE RUBIK’S REVENGE

Figure 1. Enumeration of the spatial positions occupied by corners.

we give numbers 6, 7 and 8 to the others in the same layer. Finally we assign numbers from 9 to 12 to edge spatial positions in the down face, with 9 assigned to the front-down and the other counting clockwise.

Figure 2. Enumeration of the spatial positions for edges.

Now let us see how to assign $x_i \in \mathbb{Z}_3$ for each $i \in \{1, \ldots, 8\}$. First of all, we decide that for corners having a white sticker, the latter is assigned with number 0 and the other stickers take number 1 and 2 moving clockwise on the cubie’s faces, starting from the white one, as done in [4]. Similarly, for corners having a yellow sticker, it takes number 0 and the others 1 and 2 counting clockwise.

Figure 3. Example of assignation of numbers to stickers for corner cubies.

The convention for calculating components of vector $x$ for a random configuration is the following: we associate to the corner living in the $i$-th spatial position the orientation number $x_i \in \mathbb{Z}_3$,
defined as the number of the corner’s sticker lying on the white or yellow face of the cube. Referring for example to the random configurations illustrated in both sides of Figure 3, we would get $x_4 = 2$, as the corner standing in position four has the stickers that takes 2 in the up face of the cube.

We proceed similarly for edges, i.e., we establish that for edges having a white or a yellow sticker, those ones take number 0 and the other stickers take 1 (examples in the left-hand side of Figure 4). For the remaining 4 edges, we decide that red and orange stickers take 0, while green and blue ones take 1 (examples in the right-hand side of Figure 4).

![Figure 4. Assignation of numbers to stickers for edge cubies.](image)

Determining $y$ is done fixing four sides to look at the cube: up (white), down (yellow), front (red) and back (orange). We associate to the edge living in the $i$-th spatial position the orientation number $y_i \in \mathbb{Z}_2$, defined as the number of the edge sticker lying respectively on the white, yellow, red or orange face of the cube. For the random configuration illustrated in the left-hand side of Figure 4 we have $y_4 = 1$, as the edge occupying position 4 has its blue sticker (taking number 1) lying in the upper face of the Cube; similarly $y_8 = 0$ since the edge in position 8 has its yellow sticker (taking number 0) living in the front face of the Cube. Following the same principle for different stickers’ colours and for the random configuration illustrated in the right-hand side of Figure 4 we have $y_1 = 1$ and $y_8 = 0$. It is clear for the convention we have introduced that whenever the Cube is solved we have $x_i = 0$ for all $i \in \{1, \ldots, 8\}$ and $y_i = 0$ for all $i \in \{1, \ldots, 12\}$.

We say that a configuration is valid if one can reach the configuration $(\text{id}_{S_8}, \text{id}_{S_{12}}, 0, 0)$, i.e. the configuration where the cube is solved, by a finite number of moves. The “first law of cubology” (Theorem 1, page 42) provides necessary and sufficient conditions for a configuration to be valid.

**Theorem 2.1 (First law of cubology).** A configuration of the Rubik’s Cube is valid if and only if

i) $\text{sgn}(\sigma) = \text{sgn}(\tau)$;

ii) $\sum_i x_i \equiv 0 \pmod{3}$;

iii) $\sum_i y_i \equiv 0 \pmod{2}$.

From this theorem we get that the probability for a randomly assembled Rubik’s cube to be solvable is $\frac{1}{12}$ and hence one gets:

**Corollary 2.1** (Theorem 2, page 44). The total number of possible patterns is $\frac{8! \cdot 3^8 \cdot 12^8 \cdot 2^{12}}{12}$.

2 By possible patterns we mean the ones in the valid configuration.
Some relevant mathematical properties of the Rubik’s Cube follow from the above theorem, see [2] and [9] for details.

3. Configurations of the Rubik’s Revenge

The Rubik’s Revenge has been created a few years after the original Rubik’s cube: every face is composed by four slices instead of three. The Rubik’s Revenge is composed by 56 cubies: 8 are corner cubies exactly as in the original Cube, 24 are edge cubies and the remaining 24 are center cubies. At first glance, the big difference with the Rubik’s Cube is that center pieces are not fixed anymore (clearly, also the number of edges is duplicated). As center cubies can be moved, they do not determine which colour a face shall assume solving the Revenge. However, it is enough to choose a random corner to determine the colour that every face shall assume. Throughout the paper we mean the Revenge oriented so to have the white face on top and the red one in front. Hence the white-red-green corner, for example, shall occupy the up-front-left position in the solved Cube. In order to have that, after a quick look to the Revenge, we search the white-red-green corner and establish that position one is exactly located where such corner is living in, hence we rotate the whole cube so to have such a corner standing in the up-front-left position.

As for the original Cube, the set of moves naturally inherits the structure of a group, denoted by $M$. This group is generated by the twelve clockwise rotations of slices denoted by $R,L,F,B,U,D,R,R,F,U,L,B,D$ where $R,L,F,B,U,D$ are twists of the external slices, respectively, right, left, front, back, up and down face, while $C_R,C_F,C_U,C_L,C_B,C_D$ are the twists of the central-front, central-right, central-up, central-left, central-back and central down slice respectively (some of which is illustrated in Fig. 5).

Any of those elements has order 4.

The number of stickers one can find on the Revenge is equal to 96, so we may define an homomorphism

$$\varphi: M \rightarrow S_{96},$$

which sends a move $m \in M$ to a permutation $\varphi(m) \in S_{96}$ induced on the Revenge by the move $m$. The image $\varphi(M) \subset S_{96}$ corresponds to those permutations in $S_{96}$ induced by moves of the Revenge.

Remark 3.1. The inclusion $\varphi(M) \subset S_{96}$ is (obviously) strict. For example, it may never happen that an element of $M$ send a corner to the position occupied by a center or an edge.
We can then define the group of the Rubik’s Revenge \( G := \phi(M) \). By the well known “isomorphism theorem”, \( G = M/\ker(\phi) \), i.e., it is the group of the moves we get identifying all the combination of moves leading to the identical permutation.

Consider the subset of \( S_{96} \) corresponding to permutations and/or orientation changes of corners, edges and center cubies. The set all of these permutations will be called the \textit{space of the configuration of the Revenge} and will be denoted by \( S_{\text{Conf}} \).

Remark 3.2. It is known that a single edge cubie can not be flipped\(^3\); however we may theoretically think to flip a single edge (and hence changing its orientation) by swapping its stickers. Therefore, unlike the Rubik’s Cube, the cardinality of \( S_{\text{Conf}} \) is larger than the number of patterns we can get by dismantling and reassembling the cube.

Clearly \( G \subset S_{\text{Conf}} \subset S_{96} \) and \( |S_{\text{Conf}}| < 96! \). More precisely
\[
|S_{\text{Conf}}| = (24!)^2 \cdot 2^{24} \cdot 3^8 \cdot 8!.
\] (1)

The group \( G \) acts on the left on \( S_{\text{Conf}} \):
\[
G \times S_{\text{Conf}} \longrightarrow S_{\text{Conf}}
\]
\[
(g, s) \mapsto g \cdot s
\]
where \( \cdot \) represents the composition in \( S_{96} \). This gives raise to a left action of \( M \) on the space of configurations, by \( m \cdot s = g \cdot s \), where \( g = \phi(m) \), and vice-versa. For this reason, from now on, we will not make any distinction between the two actions on \( S_{\text{Conf}} \). Notice that the action of \( G \) on \( S_{\text{Conf}} \) is free (in contrast with that of \( M \)), i.e., if \( g \cdot s = s \) then \( g = \text{id} \). Hence this action yields a bijection between the group \( G \) and the orbit \( G \cdot s = \{ g \cdot s \mid g \in G \} \) of an arbitrary \( s \in S_{\text{Conf}} \), obtained by sending \( g \in G \) into \( g \cdot s \in S_{\text{Conf}} \).

Remark 3.3. It is easily seen that the space of configuration \( S_{\text{Conf}} \) is a subgroup of \( S_{96} \) containing \( G \) as a subgroup. Then the left action \( g \cdot s, g \in G \) and \( s \in S_{\text{Conf}} \), can be also seen as the multiplication in \( S_{\text{Conf}} \) and the orbit \( G \cdot s \) of \( s \in S_{\text{Conf}} \) is nothing but the right coset of \( G \) in \( S_{\text{Conf}} \) with respect to \( s \).

In order to characterize mathematically the notion of configuration we have to label center and edge cubies. Indeed, corners are univocally identified by the colours of their faces, but ambiguity may arise concerning edges and centers.

In order to describe positions of each edge (or center) by permutations, we have to label all of them. A number between 1 and 24 is the label for center cubies. Once all centers have been marked, the position of each of them in a random pattern can be described by a permutation \( \rho \in S_{24} \).

Regarding corners, things work like in the Rubik’s cube, so a permutation \( \sigma \in S_8 \) describes their positions.

The twenty-four edge cubies can be devided in twelve pairs, namely those ones with the same colour. The two members of a pair are labelled with different letters: \( a \) and \( b \), respectively. This is enough to provide a description of edges’ positions by using a permutation \( \tau \in S_{24} \). We refer to an edge labelled with \( a \) (respectively \( b \)) as an edge of type \( a \) (respectively type \( b \)). Obviously the type is not dependent on the position the edge is lying in.

Describing orientations of corners can be achieved by a vector \( x \in (\mathbb{Z}_3)^8 \) in the same way described in the previous section.

\(^3\) This is mathematically proved in [12: Theorem 2], and is also a physical constrain (see http://www.instructables.com/id/How-to-put-a-4x4-Rubiks-Cube-Together/, for a detailed description on the construction of the Rubik’s Revenge).
Remark 3.4. Due to the convention introduced above that the white-red-green corner is always set in the up-front-left position, i.e., in position 1, it will always happen that \( x_1 = 0 \).

In order to introduce such a vector for edges’ orientation, we have to describe the spatial positions for edges. We proceed as done for the Rubik’s cube (see Figure 2), by using only twelve numbers (instead of 24) and the label \( a \) and \( b \).

Concerning edges orientation, we can do the same as for the Rubik’s Cube, shifting to two 12-tuple \( y_a = (y_{1a}, y_{2a}, \ldots, y_{12a}) \), with \( y_{ia} \in \mathbb{Z}_2 \) and \( y_b = (y_{1b}, y_{2b}, \ldots, y_{12b}) \), with \( y_{ib} \in \mathbb{Z}_2 \) (edges are twenty-four, divided in pairs \( a \) and \( b \)).

It follows that the space of configurations \( S_{Conf} \) is in bijection with the set of 5-tuples \((\sigma, \tau, \rho, x, y)\), where \( \sigma \in S_8 \), \( \tau \in S_{24} \), \( \rho \in S_{24} \), while \( x \in (\mathbb{Z}_3)^8 \) and \( y \in (\mathbb{Z}_2)^{24} \). From now on we identify \( S_{Conf} \) with such 5-tuples. The 5-tuple \((\text{id}_{S_8}, \text{id}_{S_{24}}, \text{id}_{S_{24}}, 0, 0)\) will be called the initial configuration.

At the beginning of the section we claimed that the group of the moves \( M \) is generated by twelve elements. In fact, having introduced the formal notion of configuration, we may notice that nine generators are enough, as three moves involving central slices can be constructed as compositions of other basic moves. Notice, for example that \( C_L := L^{-1}C_R L \) (center-left) and the same applies to other central moves that we will refer to as \( C_B \) (center-back) and \( C_D \) (center-down).

**Definition 3.1.** A configuration of the Rubik’s Revenge is valid when it is in the orbit of the initial configuration under the action of \( G \).

We now present some basic facts concerning orbits, needed in the proof of Theorem 3.1.

**Lemma 3.1.** If two configurations \((\sigma, \tau, \rho, x, y)\) and \((\sigma', \tau', \rho', x', y')\) are in the same orbit then \( \text{sgn}(\sigma) \text{sgn}(\rho) = \text{sgn}(\sigma') \text{sgn}(\rho') \).

**Proof.** If \((\sigma, \tau, \rho, x, y)\) and \((\sigma', \tau', \rho', x', y')\) are in the same orbit, then \((\sigma', \tau', \rho', x', y') = g \cdot (\sigma, \tau, \rho, x, y)\), for some \( g \in G \). Hence it is enough to show that basic moves \( R, L, F, B, U, D, C_R, C_F, C_U \) preserve condition \( \text{sgn}(\sigma) \text{sgn}(\rho) = \text{sgn}(\sigma') \text{sgn}(\rho') \).

The action of \( g \) on corners is disjoint from the action of centers. It is easy to notice that any move among \( \{R, L, F, B, U, D\} \) consists of a 4-cycle on both corners and centers, hence \( \text{sgn}(\sigma') = -\text{sgn}(\sigma) \) and \( \text{sgn}(\rho') = -\text{sgn}(\rho) \), hence \( \text{sgn}(\sigma) \text{sgn}(\rho) = \text{sgn}(\sigma') \text{sgn}(\rho') \). On the other hand, moves \( C_R, C_F, C_U \) are identities on corners and consist of two 4-cycles on centers, implying that \( \text{sgn}(\sigma) = \text{sgn}(\sigma') \) and \( \text{sgn}(\rho) = \text{sgn}(\rho') \), hence \( \text{sgn}(\sigma) \text{sgn}(\rho) = \text{sgn}(\sigma') \text{sgn}(\rho') \) also in this case. \( \square \)

**Lemma 3.2.** If \((\sigma, \tau, \rho, x, y)\) and \((\sigma', \tau', \rho', x', y')\) are configurations in the same orbit then \( \sum x_i' \equiv \sum x_i \pmod{3} \).
Proof. The proof works exactly as for the analogous property valid for the Rubik’s Cube \cite{2}. □

Before stating the main result of this paper, we make some considerations concerning edge cubies. We are aware of the fact that in a random configuration, an edge of type $a$ (resp. $b$) can occupy either an $a$-position or a $b$-position, as sketched for example in Figure 7. Hence, using the information encoded in $\tau \in S_{24}$ we may associate to any edge a number $i_{t,s}$, with $t,s \in \{a,b\}$, where $i_t$ indicates the spatial position, while $s$ refers to the type of the edge. There are always orientation numbers associated to any edge $i_{t,s}$ which will be $y_{i_{t,s}} := y_i$.

![Figure 7. Letters a,b represents label associated to edges. In the above configuration we notice an edge of type $a$ in position 1$^a_a$ and an edge of type $b$ in position 1$^b_b$. In position 2 we find two edges of type $b$, hence 2$^b_b,b$ and 2$^a_a,b$. Notice that the two edges in position 2 have two different orientations, namely $y_{2^b_b,b} = 1$, $y_{2^a_a,b} = 0$.]

We can now give the conditions for a configuration to be valid: this is actually the “first law of cubology” for the Rubik’s Revenge:

**Theorem 3.1.** A configuration $(\sigma, \tau, \rho, x, y)$ is valid if and only if
1. $\text{sgn}(\sigma) = \text{sgn}(\rho)$,
2. $\sum_i x_i \equiv 0 \pmod{3}$
3. $y_{i_{t,s}} = 1 - \delta_{t,s}$, for all $i = 1, \ldots, 12$,

where $\delta_{a,a} = \delta_{b,b} = 1$ and $\delta_{a,b} = \delta_{b,a} = 0$.

Next section is dedicated to the proof of this theorem. Our proof will not be constructive, i.e. we do not show the moves actually needed to solve the cube, as we will use some group-theoretical results. Here we present some corollaries.

**Corollary 3.1.** The order of $G$ is $\frac{(24!)^2 \cdot 8! \cdot 3^7}{2}$.

**Proof.** Since the action of $G$ is free, then $|G| = |G \cdot s|$ for all $s \in S_{\text{Conf}}$. It follows that $|G| = \frac{|S_{\text{Conf}}|}{N}$, where $N$ is the number of orbits. Theorem 3.1 yields $N = 2 \cdot 3 \cdot 2^{24}$ and the results follows by \cite{1}. □
The corollary above agrees with result presented in the last section of [12].

In order to study the solvability of the Revenge we give the following:

**Definition 3.2.** A randomly assembled Rubik’s Revenge is a pattern of the Revenge obtained by any permutation and/or orientation change of corners, edges[^4] and center cubies of the solved Revenge.

**Corollary 3.2.** The probability that a randomly assembled Rubik’s Revenge is solvable is \( \frac{1}{2^{12} \cdot 3} \).

**Proof.** In a randomly assembled Rubik’s Revenge center and edge cubies are not labelled, thus centers can always be moved so to have condition 1 in Theorem 3.1 satisfied. The 24 equations in condition 3 are reduced to 12: this can be obtained by assigning a label \( a \) or \( b \) to each edge in a pair, depending on its orientation, in such a way that \( y_{i,s} = 1 - \delta_{i,s} \).

We have already mentioned (see footnote 3) the fact that the Revenge sold on the market is different from the Revenge we consider in this paper. In fact, the most relevant feature of the Revenge sold on the market is that any member of a pair of edges of the same colours is different from its companion. This has the physical effect that it is impossible to assemble the cube putting an edge of type \( a \) (respectively type \( b \)) in a ‘b-position’ (respectively \( a \)-position), without changing the orientation of both edges in a pair. This yields that condition 3 in Theorem 3.1 can be always achieved, due to the internal mechanism of the Revenge. Thus (surprisingly enough) we get:

**Corollary 3.3.** The probability that a randomly assembled Rubik’s Revenge sold on the market is solvable is \( \frac{1}{3} \).

### 4. Proof of Theorem 3.1

We first introduce some already known results [12] on the structure of \( G \) which are of fundamental importance for proving Theorem 3.1.

In order to prove the theorem we describe some significant subgroups of \( G \), denoted by \( C \), \( Z \) and \( E \) respectively. \( C \) is the subgroup of \( G \) which permutes corner cubies (no matter the action on orientation), and act as the identity on other pieces. \( Z \) is the subgroup permuting centers only, leaving corners and edges fixed; \( E \) permutes edges only[^5]. The proofs of these results can be found in [12]. However they are included in the present paper for sake of completeness. Notice that our proofs are essentially the same, but in terms of the action of \( G \) on \( S_{\text{Conf}} \).

**Theorem 4.1.** \( C \cong A_8 \), the alternating group of even permutation.

We report to [8] for the proof of the above theorem. In the next theorem we make use of the commutator, formally for \( m, n \in G \), \([m, n] = m \cdot n^{-1} \cdot m^{-1} \cdot n^{-1}\). Center cubies are 24, hence necessarily \( Z \leq S_{24} \).

**Theorem 4.2.** \( Z \cong A_{24} \), the alternating group of even permutation.

---

[^4]: Here we allow also edge flips (see Remark 3.2).

[^5]: Since each may assume three different orientations, it is known [8], [12] that the subgroup of corners corresponds to the wreath product \( H = S_8 \wreath Z_3 \). However, we aim at describing the quotient subgroup \( C = H/T \), where \( T \) is the (normal) subgroup consisting of all al possible twists.
Proof. We first show that $A_{24} \leq Z$. The move
\[ z = [C_F, C_U, U^{-1}] \] (2)
is a 3-cycle on center and an identity on edges and corners. In fact, it is easy to check that the
action of $z$ on the initial configuration gives: $z \cdot (\text{id}_{S_8}, \text{id}_{S_{24}}, \text{id}_{S_{24}}, 0, 0) = (\text{id}_{S_8}, \text{id}_{S_{24}}, \rho_1, 0, 0)$, where
$\rho_1$ is 3-cycle.

Observe that any three target centers can be moved to the positions permuted by $z$ by a certain
$g \in G$. Such a $g$ admits an inverse $g^{-1} \in G$, hence by $g \cdot z \cdot g^{-1}$ we may cycle any center cubies. As $A_{24}$ is generated by any 3-cycle on a set of twenty-four elements, we have the desired inclusion.

For $Z \leq A_{24}$, we show that any odd permutation involving centers permutes necessarily also
corners or edges, hence it cannot be in $Z$. Indeed, suppose that there exist $\alpha \in Z$ s.t. $\text{sgn}(\alpha) = -1$. Such an $\alpha$ shall be obtained as a sequence of basic moves. Without loss of generality we can assume that $\alpha$ is a sequence of $L, R, U, D, F, B$, since the moves $C_R, C_F, C_U$ consist of an even permutation on centers. On the other hand, $L, R, U, D, F, B$ induces a 4-cycle on centers. However, all those moves must have permuted corners too, thus there exist a $\beta = (\beta_1, \beta_2) \in S_8 \times E$, s.t. $\text{sgn}(\beta) = -1$. Hence $\beta_1 \neq \text{id}_{S_8}$, implying that $\alpha \notin Z$, the desired contradiction.

Now we consider the subgroup $E$ of moves involving edges only. Edges are 24 each of which can
assume two different orientation, however no single edge can be flipped [12]. The direct consequence of
this fact is that $E \leq S_{24}$. Actually we can prove

**Theorem 4.3.** $E \cong S_{24}$

Proof. We first show that $A_{24} \leq E$. Indeed the move
\[ e = [C_F^{-1}, [L, U^{-1}]] \] (3)
is of a 3-cycle on edges. As done for centers, one can bring any target edge in the positions switched
by $e$ using an element of $g \in G$ and then solving the mess created by $g^{-1}$. In this way, one obtains
any 3-cycles in $E$, proving the inclusion.

We are left with proving that there is at least an odd permutation in $E$, which implies necessarily
that $E \cong S_{24}$.

Consider the move $C_R$: it gives rise to an even permutation on centers (two 4-cycles) and an odd
one on edges (one 4-cycle). As by Theorem 4.2 $Z \cong A_{24}$, one can find $z_0 \in Z$ such that $z_0 \cdot \varphi(C_R)$
acts as a 4-cycles of edges only. Hence $z_0 \cdot \varphi(C_R) \in E$ and $\text{sgn}(z_0 \cdot \varphi(C_R)) = -1$. □

**Proof of Theorem 3.1.**

($\Rightarrow$) Assuming $(\sigma, \tau, \rho, x, y)$ is valid means that it is in the orbit of the initial configuration
$(\text{id}_{S_8}, \text{id}_{S_{24}}, \text{id}_{S_{24}}, 0, 0)$.

1. By Lemma 3.1 we have that $\text{sgn}(\sigma) \cdot \text{sgn}(\rho) = \text{sgn}(\text{id}_{S_8}) \cdot \text{sgn}(\text{id}_{S_{24}}) = 1$, hence $\text{sgn}(\sigma) = \text{sgn}(\rho)$, for their product must be equal to 1.

2. $\sum_i x_i \equiv 0 (\text{mod } 3)$ follows trivially from Lemma 3.2 and the fact that $(\sigma, \tau, \rho, x, y)$ is valid.

3. In the initial configuration $(\text{id}_{S_8}, \text{id}_{S_{24}}, \text{id}_{S_{24}}, 0, 0)$ it holds $y_{i_i} = 0$ for all $i \in \{1, \ldots, 12\}$ and
$\delta_{a,b} = \delta_{b,a} = 1$, hence $y_{i,s} = 1 - \delta_{t,s} = 0$.

As $(\sigma, \tau, \rho, x, y)$ is in the orbit of the initial configuration, it is obtained by a sequence of basic
moves, thus we need to check that those moves preserve condition $y_{i,s} = 1 - \delta_{t,s}$.

We consider moves splitted in two sets: $M_1 = \{R, U, D, L\}$ and $M_2 = \{F, B, C_R, C_F, C_U\}$; hence
we have two possibilities: we may assume a move, say $m$, either $m \in M_1$ or $m \in M_2$.
Assume $m \in M_1$. Recall that for the convention we have introduced about the assignment of

570
orientation numbers to edges, \( m \) does not change edge cubies’ orientation, so we get \( y_{i,t,s} = 0 \) for all \( i \in \{1, \ldots, 12\} \). Furthermore \( m \) acts on a configuration moving edges occupying an \( a \)-position in edges in \( a \)-position and the same holds for \( b \)-positions and hence \( \delta_{t,s} = 1 \).

Let now \( m \in M_2 \). \( m \) changes orientations of some edges (the ones that it is actually permuting): more precisely it gives raise to a cycle of four edges or to two cycles of four edges each. Let \( i_t,s \) be one of those edges, then \( y_{i_t,s} = 1 \) and \( \delta_{t,s} = 0 \) since \( a \)-positions and \( b \)-positions are swapped by \( m \).

(\( \Leftarrow \)) We have to show that once conditions 1, 2 and 3 are satisfied we are always able to solve the cube. In the random configuration \((\sigma, \tau, \rho, x, y)\) we can check (just by watching the Revenge) whether \( \rho \) is even or odd. If \( \text{sgn}(\rho) = -1 \), it is enough to apply one among \{\( R, L, U, D, F, B \)\} to get \( \text{sgn}(\rho) = +1 \). If \( \text{sgn}(\rho) = +1 \), then \( \rho \in A_{24} \), hence, by Theorem 4.2 \( \rho \in Z \cong A_{24} \), there exists \( z_1 \in Z \) s.t. \( z_1 \cdot (\sigma, \tau, \rho, x, y) = (\sigma, \tau, \text{id}_{S_{24}}, x, y) \).

By condition 1. \( \text{sgn}(\sigma) = \text{sgn}(\rho) = \text{sgn}(\text{id}) \), hence in \((\sigma, \tau, \text{id}_{S_{24}}, x, y)\), \( \text{sgn}(\sigma) = +1 \). Then \( \sigma \in A_8 \).

By Theorem 4.1 \( C \cong A_8 \), thus there exists \( c \in C \) such that \( c \cdot (\sigma, \tau, \text{id}_{S_{24}}, x, y) = (\text{id}_{S_{8}}, \tau, \text{id}_{S_{24}}, x, y) \).

Now, we proceed setting edges in their correct positions; \( \tau \) is a permutation of 24 elements, however Theorem 4.3 \( E \cong S_{24} \), hence there is an \( e_1 \in E \) such that \( e_1 \cdot (\text{id}_{S_{8}}, \tau, \text{id}_{S_{24}}, x, y) = (\text{id}_{S_{8}}, \text{id}_{S_{24}}, x, y, x, 0) \). Condition (3) implies that, as all edge cubies are correctly positioned, then they are also correctly oriented, thus \( y = 0 \), so \( (\text{id}_{S_{8}}, \text{id}_{S_{24}}, x, y, x, 0) = (\text{id}_{S_{8}}, \text{id}_{S_{24}}, x, y, x, 0) \).

Now the labelled Revenge has been reduced to Rubik’s Cube, as any pair of edge can be seen as an unique big edge. So we have actually reduced the Rubik’s Revenge to a Rubik’s Cube whose corners can be correctly oriented, since condition 2 is satisfied, see [2] for details.

We have proved that the initial configuration \((\text{id}_{S_8}, \text{id}_{S_{24}}, 0, 0, 0)\) is in the orbit of \((\sigma, \tau, \rho, x, y)\), hence the latter is valid, concluding the proof of the theorem. \( \square \)

REFERENCES

[1] ADAMS, J.: How to Solve Rubik’s Revenge, The Dial Press, New York, 1982.
[2] BANDELOW, C. L.: Inside Rubik’s Cube and Beyond, Birkhäuser, 1982.
[3] BONZIO, S.—LOI, A.—PERUZZI, L.: Black holes as Rubik’s Cubes, submitted.
[4] CHEN, J.: Group theory and the Rubik’s Cube, Notes.
[5] CZECH, B.—LARJO, K.—ROZALI, M.: Black holes as Rubik’s Cubes, Journal of High Energy Physics 8, (2011).
[6] DEMAINE, E. D.—DEMAINE, M. L.—EISENSTAT, S.—LUBIW, A.—WINSLAW, A.: Algorithms for Solving Rubik’s Cubes. In: Proceedings ESA 2011.
[7] DIACONU, A.—LOUKHAOUKHA, K.: An improved secure image encryption algorithm based on Rubik’s Cube principle and digital chaotic cipher, Math. Probl. Eng. 2013, (2013), Art. ID 848392.
[8] FREY, A.—SINGMASTER, D.: Handbook of Cubik Math, Enslow Publishers, 1982.
[9] JOYNER, D.: Adventures in Group Theory, The Johns Hopkins University Press, 2008.
[10] KOSNIOWSKI, C.: Conquer that Cube. Cambridge University Press, 1981.
[11] KUNKLE, D.—COOPERMAN, G.: Twenty-six Moves Suffice for Rubik’s Cube. In: Proceedings of the 2007 International Symposium on Symbolic and Algebraic Computation, 2007.
[12] LEE, C.—LU, M. C.—HUANG, M.—WEAVERDYCK, M. E.: On God’s number(s) for Rubik’s slide, College Math. J. 45(4) (2014).
[13] MILLER, J.: Move-count Means with Cancellation and Word Selection Problems in Rubik’s Cube Solution Approaches, PhD Thesis, Kent State University, 2012.
[14] ROKICKI, T.: Towards God’s number for Rubik’s cube in the quarter-turn metric, College Math. J. 45(4) (2014).
[15] ROKICKI, T.—KOCIEMBA, H.—DAVIDSON, M.—DETHRIDGE, J.: The diameter of the Rubik’s Cube group is twenty, SIAM J. Discrete Math. 27(2) (2013).
[18] VOLTE, E.—PATARIN, J.—NACHEF, V.: Zero Knowledge with Rubik’s Cubes and Non-abelian Groups. Cryptology and Network Security, 12th International Conference, 2013.