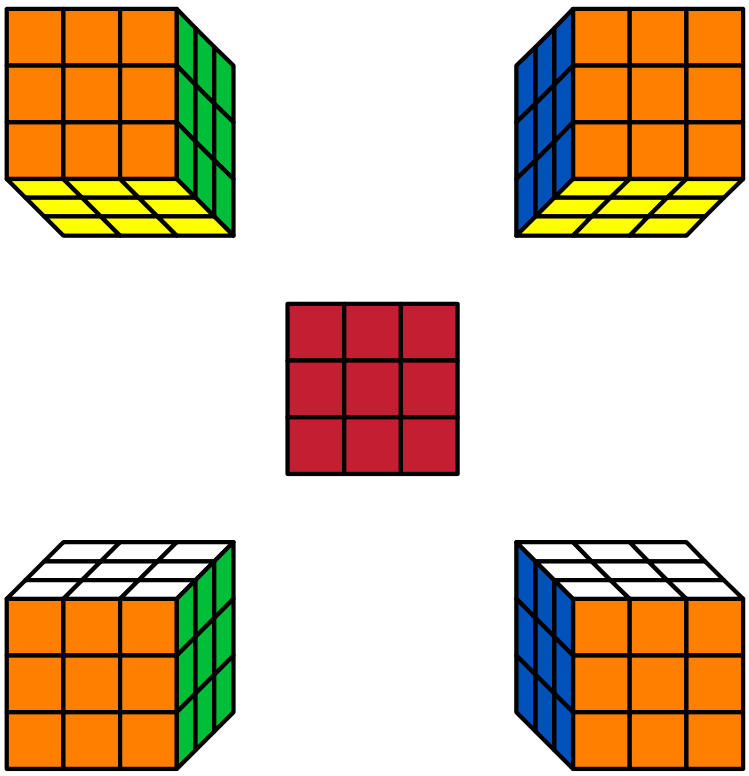
Group Theory: The Rubik's Cube

David Fudge
Western Illinois University

April 23, 2018

A Rubik's cube contains 6 faces, each of a distinct color. These six colors are blue, green, orange, red, white, and yellow. Each face of the cube can be rotated by increments of 90 degrees. Here's a visualization of the Cube, with the center square being the unseen face in the back:



Let $S = \{B, G, O, R, W, Y\}$ be the set of single clockwise rotations for a Rubik's Cube, where the letter of each element corresponds with the color of the center cubie (an individual cube within the whole Rubik's Cube), which stays fixed. For example, B is the action of rotating the face with blue as its center cubie.

1 Some Definitions and Proofs

Definition 1.1. *A set H is a **subgroup** of a group G, denoted $H \leq G$, if and only if*

(1) $H \subseteq G$,

(2) $H \neq \emptyset$, and

(3) for any $a, b \in H$, $ab^{-1} \in H$.

Proposition 1.1. *Let $H = \{g_1, g_2, g_3, ..., g_n\}$ where $g_1, g_2, g_3, ..., g_n \in G$. Therefore, $H \leq G$.*

Proof. By Definition 1.1, $H \leq G$ if and only if H satisfies three conditions.
(1) H is clearly a subset of G since all elements in H are also in G.
(2) H is clearly nonempty since it contains, for example, g_1.
(3) Take $a, b \in H$. Since $H \neq \emptyset$, $a^{-1}, b^{-1} \in H$. So $aa^{-1} \in H$. So the identity of G, $aa^{-1} = e$, is an element of H. Thus, $ab^{-1} \in H$.
So by (1), (2), (3), and by Definition 1.1, $H \leq G$. □

Definition 1.2. *Let a and b be elements of a group H. H is called **abelian** if and only if the group operation is commutative such that $ab = ba$.*

Example 1.1. *Consider a Rubik's Cube. Let the set $S = \{B, G, O, R, W, Y\}$ be the group consisting of 90 degree rotations where each element corresponds with the color of the center cubie of any given face. The group S is not abelian.*

Proof. Suppose that before any rotation is applied to a Rubik's Cube, each face of the cube can be expressed as a matrix whose elements are denoted by their color.

$$\text{Blue Face: } \begin{bmatrix} b & b & b \\ b & b & b \\ b & b & b \end{bmatrix} \qquad \text{Green Face: } \begin{bmatrix} g & g & g \\ g & g & g \\ g & g & g \end{bmatrix} \qquad \text{Orange Face: } \begin{bmatrix} o & o & o \\ o & o & o \\ o & o & o \end{bmatrix}$$

$$\text{Red Face: } \begin{bmatrix} r & r & r \\ r & r & r \\ r & r & r \end{bmatrix} \qquad \text{White Face: } \begin{bmatrix} w & w & w \\ w & w & w \\ w & w & w \end{bmatrix} \qquad \text{Yellow Face: } \begin{bmatrix} y & y & y \\ y & y & y \\ y & y & y \end{bmatrix}$$

First, consider the operation WY. The matrix of the face with the yellow center cubie is transformed into $\begin{bmatrix} g & g & g \\ y & y & y \\ y & y & y \end{bmatrix}$. Next, consider the operation YW. The matrix of the face with

the yellow center cubie is transformed into $\begin{bmatrix} g & y & y \\ g & y & y \\ w & y & y \end{bmatrix}$. Thus $WY \neq YW$. By Definition 1.2, S cannot be abelian. □

Definition 1.3. *Consider a group G. If $M_1, M_2 \in G$, then $M_1M_2M_1^{-1}M_2^{-1}$ is the* ***commutator*** *of G. The commutator $M_1M_2M_1^{-1}M_2^{-1}$ is abbreviated as $[M_1, M_2]$. Also, if $M_1M_2 = M_2M_1$, it is said that M_1 and M_2* ***commute****.*

Proposition 1.2. *If $M_1, M_2 \in G$, then $[M_1, M_2] = e$ if and only if M_1 and M_2 commute.*

Proof. This proof requires two steps.
(1) First, let's prove that if $[M_1, M_2] = e$, then M_1 and M_2 commute. Let's assume that $[M_1, M_2] = e$. So,

$$\begin{aligned}
& M_1M_2M_1^{-1}M_2^{-1} = e && \text{(By Definition 1.3)} \\
\Rightarrow\ & M_1M_2M_1^{-1}M_2^{-1}M_2 = eM_2 \\
\Rightarrow\ & M_1M_2M_1^{-1}e = M_2 \\
\Rightarrow\ & M_1M_2M_1^{-1} = M_2 \\
\Rightarrow\ & M_1M_2M_1^{-1}M_1 = M_2M_1 \\
\Rightarrow\ & M_1M_2e = M_2M_1 \\
\Rightarrow\ & M_1M_2 = M_2M_1.
\end{aligned}$$

So by Definition 1.3, M_1 and M_2 commute.
(2) Next, let's prove that if M_1 and M_2 commute, then $[M_1, M_2] = e$. Let's assume that M_1 and M_2 commute such that

$$\begin{aligned}
& M_1M_2 = M_2M_1 && \text{(By Definition 1.3)} \\
\Rightarrow\ & M_1M_2M_1^{-1} = M_2M_1M_1^{-1} \\
\Rightarrow\ & M_1M_2M_1^{-1} = M_2e \\
\Rightarrow\ & M_1M_2M_1^{-1} = M_2 \\
\Rightarrow\ & M_1M_2M_1^{-1}M_2^{-1} = M_2M_2^{-1} \\
\Rightarrow\ & M_1M_2M_1^{-1}M_2^{-1} = e \\
\Rightarrow\ & [M_1, M_2] = e. && \text{(By Definition 1.3)}
\end{aligned}$$

So by (1) and (2), $[M_1, M_2] = e$ if and only if M_1 and M_2 commute. □

Definition 1.4. *Let H and G be groups where $h \in H$ and $\rho : H \to G$. The function ρ is called a* ***homomorphism*** *if and only if $\rho(xy) = \rho(x)\rho(y)$.*

Definition 1.5. *Let g be an element of a group G, and let $f : G \to G$ be given by $f(x) = g^{-1}xg$. Then f is called* ***conjugation*** *by g.*

Proposition 1.3. *Let g be an element of a group G, and let $f : G \to G$ be given by $f(x) = g^{-1}xg$. Conjugation by g is a homomorphism.*

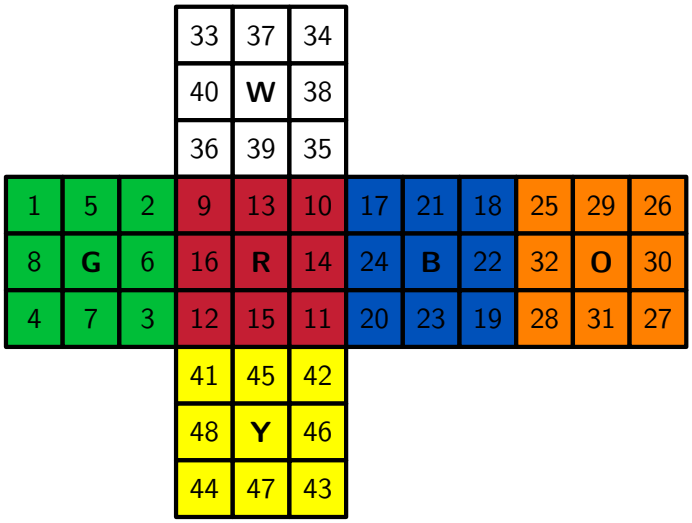
Proof. Let $x, y \in G$. By Definition 1.4, conjugation by g is a homomorphism if and only if $f(xy) = f(x)f(y)$. Note that

$$\begin{aligned} f(xy) &= g^{-1}(xy)g && \text{(By Definition 1.5)} \\ &= g^{-1}xyg \\ &= (g^{-1}x)(yg) \\ &= (g^{-1}x)e(yg) \\ &= (g^{-1}x)(gg^{-1})(yg) \\ &= g^{-1}xgg^{-1}yg \\ &= (g^{-1}xg)(g^{-1}yg) \\ &= f(x)f(y). && \text{(By Definition 1.5)} \end{aligned}$$

So conjugation by g is clearly a homomorphism. □

2 GAP and defining the Rubik's Cube

The Rubik's Cube group can be expressed as a permutation, namely as an element of the set of all permutations of {1,2,3,...,48} (i.e. S_{48}). To define the Rubik's Cube as a permutation, refer to the figure below.



(1)

Figure 1 can be expressed as a permutation group, given a few observations. When the action R is performed, the edge cubies on the red face is a cycle where $(13, 14, 15, 16)$ is the said cycle. However, since the edges are each "'connected"' to an edge of each of the four adjacent faces, we also have the cycle $(39, 24, 45, 6)$. Similarly, the corner cubies need to be accounted for the red face; this means that along with the cycle $(9, 10, 11, 12)$, there is also $(36, 17, 42, 3)$ and $(35, 20, 41, 2)$. Thus, the action of rotating the red face is $R = (13, 14, 15, 16)(39, 24, 45, 6)(9, 10, 11, 12)(36, 17, 42, 3)(35, 20, 41, 2)$. This logic can be applied to the other five faces where O, B, W, Y, G are products of five cycles of length 4.

Definition 2.1. *An **even permutation** is a permutation that can be written as a product of an even number of transpositions (i.e. cycles of length 2). Similarly, an odd permutation is a product of an odd number of transpositions.*

Proposition 2.1. *Each face rotation $Rot \in S$ is an odd permutation. However, not all permutations in the Rubik's Cube group is odd.*

Proof. Note that

$$Rot = (abcd)(efgh)(ijkl)(mnop)(qrst),$$

where a,b,c, ..., t are labels for a face of a cubie. Note that R can alternatively be written as

$$\begin{aligned} Rot &= (bda)(bc)(fhe)(fg)(jli)(jk)(npm)(no)(rtq)(rs) \\ &= (ad)(ba)(bc)(eh)(fe)(fg)(il)(ji)(jk)(mp)(nm)(no)(qt)(rq)(rs). \end{aligned}$$

Now we know that *Rot* is a product of 15 transpositions. Thus, all face rotations alone are odd permutations. □

Proposition 2.2. *The order of the Rubik's Cube group is* $2^{27}3^{14}5^{3}7^{2}11$.

Proof. Let's first have the presumption that all orientations of the Rubik's Cube are possible. This means that we have two things to consider: cubie position and cubie orientation. For both, it is necessary to split both of them into the corners and edges of the cube. The following is shown through sheer observation:

(1) Consider corner cubie position. Since there is a finite quantity of spots at which corner cubies can be placed, there are 8 possible positions.

(2) Consider corner cubie orientation. For any given spot that a corner cubie is placed, the cubie has 3 possible orientations.

(3) Consider edge cubie position. Since there is a finite quantity of spots at which edge cubies can be placed, there are 12 possible positions.

(4) Consider edge cubie orientation. For any given spot that an edge cubie is placed, it has 2 possible orientations.

Now, given that the Rubik's Cube group is a permutation group and thus all orientations and positions can be expressed in factorial form, it appears that the order of the Rubik's Cube group is $8!12!3^{8}2^{12}$. Later we shall restrict this number by a factor of 12, which gives us $2^{27}3^{14}5^{3}7^{2}11$. □

Now, GAP shall be finally implemented. Upon start-up, the program will show gap> at the bottom line of text. Immediately following to the right of gap> should be typed as such:

$$\mathrm{R} := (13,14,15,16)^{*}(39,24,45,6)^{*}(9,10,11,12)^{*}(36,17,42,3)^{*}(35,20,41,2);;$$

The colon equals (:=) sets the item on the left of the equality to be the item on the right. This is useful when long permutations like R are implemented more than once. The double semicolon (;;) does two things. The semicolon on the left solves for the input so that the program knows it should not expect additional code. The second semicolon suppresses the output of the input (this is often optional, especially when looking at the output is unnecessary). After repeating the process for the other five faces, a new command is used. The command "Group" generates a group comprised of one or more given elements. Call this group "Cube". Specifically,

$$\mathrm{Cube} := \mathrm{Group}([G,R,B,O,W,Y]);$$

Now that it appears that the Rubik's Cube group has been created, let's check that the order of "Cube" is the expected value of $2^{27}3^{14}5^{3}7^{2}11$. Using the commands "FactorsInt" and "Order", the prime factorization of the order can be found. The following statement solves for the prime factorization of the order of "Cube":

FactorsInt(Order(Cube));

Note that the command "FactorsInt" does not give numbers like 5^3, but rather the collection of prime numbers involved in the product that gives the order of the Rubik's Cube.

Proposition 2.3. *Although each single face rotation is an odd permutation, not all permutations in the Rubik's Cube group are odd. That is, there exists some composition of single face rotations that is an even permutation.*

Proof. Consider $G^2 = G \circ G$. Note that from Figure 1, we have

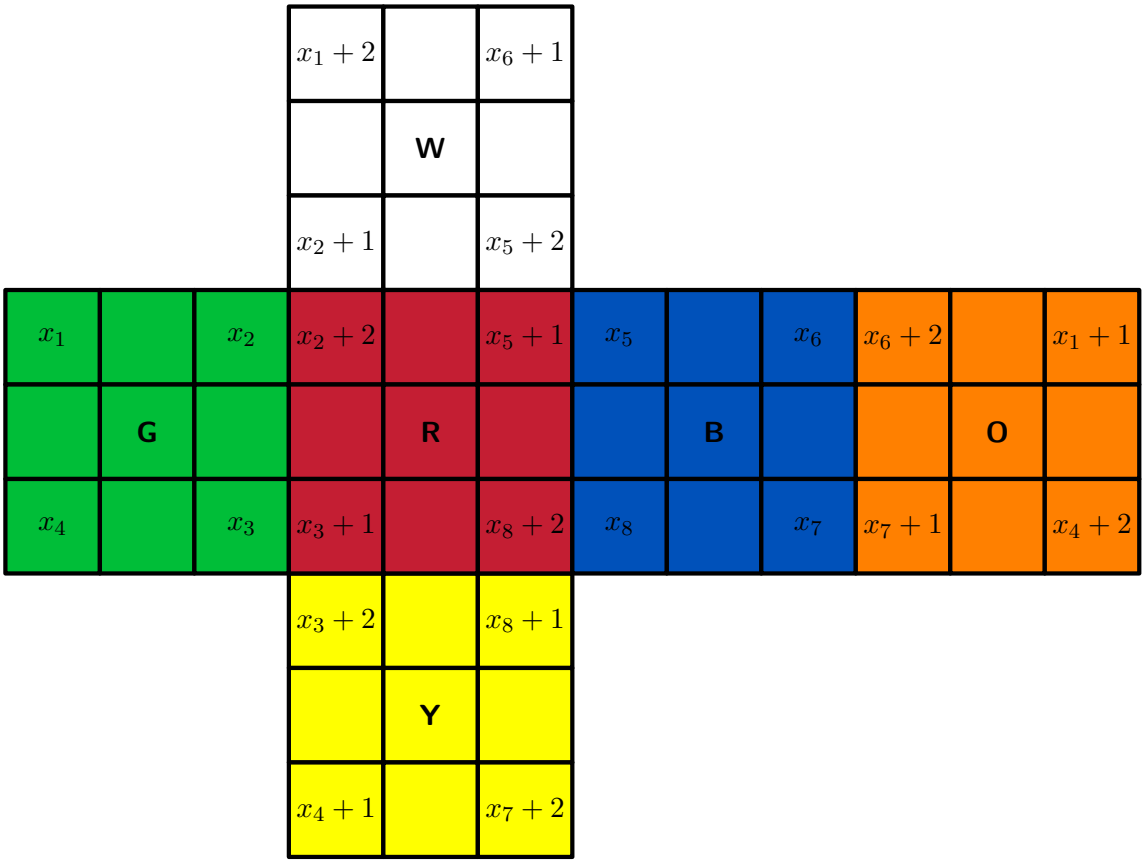
$$G = (1, 2, 3, 4)(5, 6, 7, 8)(9, 41, 27, 33)(12, 44, 26, 36)(16, 48, 30, 40).$$

Using GAP, we find G^2 (G^*G in GAP) to be

$$(1, 3)(2, 4)(5, 7)(6, 8)(9, 27)(12, 26)(16, 30)(33, 41)(36, 44)(40, 48),$$

which is clearly an even permutation. □

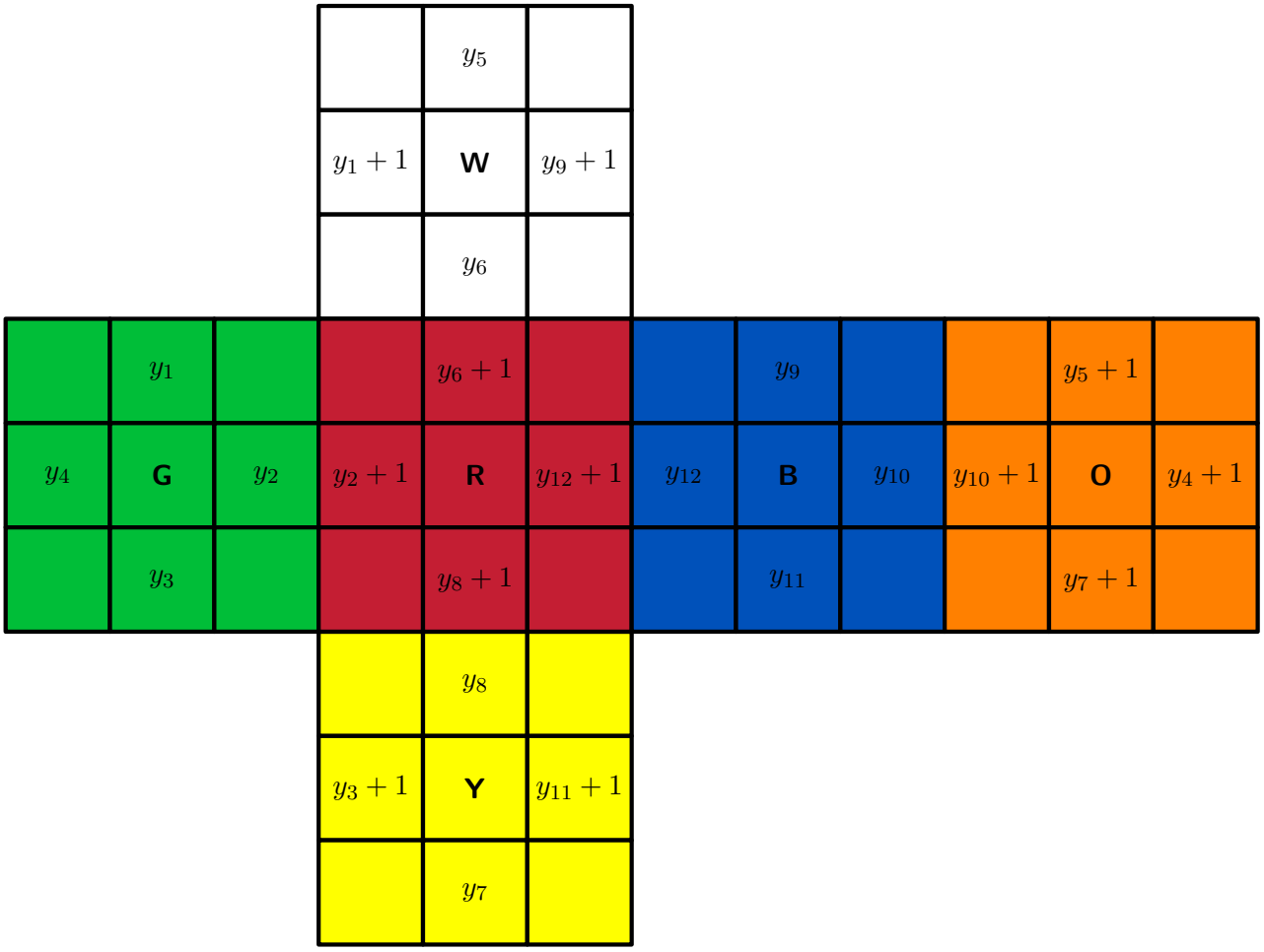
Composition does not usually commute. As a precaution, it is worth noting that GAP performs composition from left to right although the result in this example would be identical to composition performed from right to left. For example, $B \circ O$ and $O \circ B$ are permutations that can easily be calculated on GAP. The results show that $B \circ O \neq O \circ B$



For each single face rotation, we have that $(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8)$ changes to:

$$R : (x_1, x_3 + 2, x_8 + 1, x_4, x_2 + 1, x_6, x_7, x_5 + 2)$$
$$B : (x_1, x_2, x_3, x_4, x_8, x_5, x_6, x_7)$$
$$Y : (x_1, x_2, x_4 + 2, x_7 + 1, x_5, x_6, x_8 + 2, x_3 + 1)$$
$$G : (x_4, x_1, x_2, x_3, x_5, x_6, x_7, x_8)$$
$$W : (x_2 + 2, x_5 + 1, x_3, x_4, x_6 + 2, x_1 + 1, x_7, x_8)$$
$$O : (x_6 + 1, x_2, x_3, x_1 + 2, x_5, x_7 + 2, x_4 + 1, x_8)$$

Clearly $(\sum_{i=1}^{8} x_i) \bmod 3 = (\sum_{i=1}^{8} x_i + 0) \bmod 3$. For each change in the x_i's as shown above, the sums are all equal to $(\sum_{i=1}^{8} x_i) \bmod 3$. Since the sums $(\sum_{i=1}^{8} x_i + 1) \bmod 3$ and $(\sum_{i=1}^{8} x_i + 2) \bmod 3$ do not appear, we can say that only one third of the possible orientations for the corner cubies is possible. Thus we can change our upper bound for the order of the group from $8!12!3^8 2^{12}$ to $\frac{8!12!3^8 2^{12}}{3}$.



For each single face rotation, we have that $(y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8, y_9, y_{10}, y_{11}, y_{12})$ changes to:

$$R : (y_1, y_8, y_3, y_4, y_5, y_2, y_7, y_{12}, y_9, y_{10}, y_{11}, y_6)$$

$$B : (y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8, y_{12}, y_9, y_{10}, y_{11})$$

$$Y : (y_1, y_2, y_7 + 1, y_4, y_5, y_6, y_{11} + 1, y_3 + 1, y_9, y_{10}, y_8 + 1, y_{12})$$

$$G : (y_4, y_1, y_2, y_3, y_5, y_6, y_7, y_8, y_9, y_{10}, y_{11}, y_{12})$$

$$W : (y_6 + 1, y_2, y_3, y_4, y_1 + 1, y_9 + 1, y_7, y_8, y_5 + 1, y_{10}, y_{11}, y_{12})$$

$$O : (y_1, y_2, y_3, y_5, y_{10}, y_6, y_4, y_8, y_9, y_7, y_{11}, y_{12})$$

Clearly $(\sum_{i=1}^{12} y_i) \bmod 2 = (\sum_{i=1}^{12} y_i + 0) \bmod 2$. For each change in the y_i's as shown above, the sums are all equal to $(\sum_{i=1}^{12} y_i) \bmod 2$. Since the sum $(\sum_{i=1}^{12} y_i + 1) \bmod 2$ does not appear, we can say that half of the possible orientations for the corner cubies are actually possible. Thus we can change our upper bound for the order of the group from $\frac{8!12!3^8 2^{12}}{3}$ to $\frac{8!12!3^8 2^{12}}{6}$.

Earlier, it had been shown that each face rotation and its effects on the cubies regardless of orientation was an even permutation. Since the only other kind of permutation is an odd permutation, we can restrict half of all possible moves for the group. Thus we can change our upper bound for the order of the group from $\frac{8!12!3^8 2^{12}}{6}$ to $\frac{8!12!3^8 2^{12}}{12}$. Simplifying the latter number into its prime factorization, we get $2^{27}3^{14}5^3 7^2 11$.