

An n-dimensional Rubik Cube

Joe Buhler
Reed College, Portland, OR 97202

Brad Jackson
University of California, Santa Cruz, CA 95064

Dave Sibley
Pennsylvania State University, University Park, PA 16802

The Magic Cube Puzzle (known variously as Rubik's Cube, the Hungarian Cube, Bűvös Kocka, damn thing, etc.) was designed by Ernő Rubik, a professor of architecture in Budapest, Hungary. This diabolically difficult device has received a surprising amount of public attention - speed competitions are mentioned on TV news programs, a national newsmagazine used it on its cover to symbolize the intricacies of the world situation, and a 13 year-old explained on a TV talk show why adults have greater difficulty with the puzzle. The literature on the Magic Cube includes a book giving an introduction to group theory via the Cube ([17]), and a great number of solution manuals and compendiums of useful moves (e.g. [1], [8], [9], [11], [15]).

The Magic Cube has attracted considerable attention in the mathematical community not only because it is an attractive and difficult geometrical puzzle but also because it is susceptible to mathematical investigation. The totality of all reachable configurations can be identified with a large finite group; indeed one could choose to regard the Cube as a remarkably compact and efficient presentation of an interesting group.

This perspective on the Magic Cube is only indirectly relevant to the problem of finding a solution to the puzzle, but it does illuminate many aspects of the device. For instance,

it leads to an understanding of "reachable" and "unreachable" configurations. The total number of reachable configurations is equal to the order of the group. It turns out that only $1/12$ of all configurations are reachable - if one disassembles and then reassembles a Magic Cube at random the probability that it can then be solved is only $1/12$. In addition this group-theoretic analysis sheds some light (e.g. [18]) on the intriguing and very difficult unsolved problem of finding the smallest integer N such that any configuration can be solved in at most N moves (this integer is sometimes called the length of God's algorithm).

The primary goal of this paper is to study the group theory in more general versions of this kind of geometrical transformation group. Several variants of the Magic Cube have appeared, some based on different underlying polyedra. However, our primary example is a puzzle that hasn't appeared in the stores yet: an n -dimensional cube puzzle. We will explicitly determine the group of this object as a subgroup of a certain "wreath product" and thereby determine the number of configurations obtainable and determine the constraints satisfied by reachable configurations. The case $n = 4$ has been treated in some detail in [7].

The first section of this paper reviews some facts about imprimitive permutation groups and certain wreath products; this section can be used for reference. The next section contains a reasonably down-to-earth discussion of the group of the usual 3-dimensional cube. This yields certain constraints that reachable configurations must satisfy. By using some elementary facts from group theory we show that all configurations that satisfy these

conditions are in fact reachable; this is done without exhibiting a solution algorithm. The fourth section describes a very general construction of a geometrical transformation group associated to arrangements of hyperplanes in \mathbb{R}^n ; this seems to encompass all known generalizations of the Magic Cube. The rest of the paper contains a detailed analysis of the case of an n-dimensional cube; the basic definitions and theorems follow the pattern of the 3-dimensional cube in a natural way.

1. Imprimitive permutation groups. Suppose that Y is a finite set and that \equiv is an equivalence relation on Y . A bijection $f:Y \rightarrow Y$ is said to preserve the equivalence relation if

$$y_1 \equiv y_2 \quad \text{implies that} \quad f(y_1) \equiv f(y_2)$$

for all y_1, y_2 in Y . Note that f then determines a well-defined permutation on the set of equivalence classes.

A permutation group on Y is a subgroup of the group $\text{Sym}(Y)$ of all permutations (bijections) on Y . A permutation group $G \subset \text{Sym}(Y)$ is said to be imprimitive if each element of G preserves a given nontrivial equivalence relation. (An equivalence relation on a set is trivial if all elements in the set are equivalent or no two distinct elements of the set are equivalent.) Such an equivalence relation is sometimes called a G -congruence.

Example: Let G be the group (of order 8) of symmetries of the square. We can think of G as a permutation group on the set Y of 4 vertices of the square. Each element of G preserves the equivalence relation "being on diagonally opposite corners" on Y ; there are two

equivalence classes each containing two elements.

Fix a nontrivial equivalence relation \equiv on the finite set Y . Let X denote the set of equivalence classes. If $G \subset \text{Sym}(Y)$ preserves \equiv then by the observation above we get a well-defined homomorphism $\alpha: G \rightarrow \text{Sym}(X)$. The kernel is contained in the group of permutations that fix each equivalence class as a set but permute elements within each class.

To simplify the discussion we will assume that each equivalence class $x \in X$ contains m elements. If $G_{\max} \subset \text{Sym}(Y)$ denotes the maximal permutation group on Y that preserves \equiv then the situation can be nicely summarized in the language of group theory by saying that there is an exact sequence:

$$1 \rightarrow \prod_{x \in X} \text{Sym}(x) \rightarrow G_{\max} \xrightarrow{\alpha} \text{Sym}(X) \rightarrow 1$$

Since each class x has m elements the group $\text{Sym}(x)$ is isomorphic (non-canonically) to the usual symmetric group S_m . To make this completely explicit let \bar{m} denote $\{1, 2, \dots, m\}$ and choose a bijection $f_x: x \rightarrow \bar{m}$. The map that takes a permutation $s \in \text{Sym}(x)$ on the class x to $f_x \circ s \circ f_x^{-1} \in S_m = \text{Sym}(\bar{m})$ is an isomorphism.

Lemma 1: There is a homomorphism $\beta: \text{Sym}(X) \rightarrow G_{\max}$ such that $\alpha \circ \beta$ is the identity map.

Proof: For each x in X choose a numbering $f_x: x \rightarrow \bar{m}$ as above. (One could regard the collection of all of these numberings as a bijection $f: Y \rightarrow X \times \bar{m}$.) If y is in the equivalence class x and $s \in \text{Sym}(X)$ then define $\beta(s) \in \text{Sym}(Y)$ by the formula,

$$\beta(s)(y) = f_{sx}^{-1}(f_x(y)).$$

In words, this defines $\beta(s)$ to be the unique permutation on Y that preserves Ξ , induces the permutation s on the equivalence classes X , and takes the i -th element of the class x to the i -th element of the class sx for $1 \leq i \leq m$ (with respect to the given numberings). It is easy to check that $\beta(s)$ preserves Ξ , β is a homomorphism, and that $\alpha(\beta(s)) = s$ so that the proof of the lemma is finished.

This lemma says that the exact sequence above splits and that G_{\max} is then isomorphic to a semidirect product. If X has n elements then $G_{\max} \cong (S_m)^n \rtimes S_n$ where $(S_m)^n$ denotes the product of n copies of S_m and $\text{Sym}(X) \cong S_n$ acts by permuting these copies. Note that this isomorphism is not canonical; it depends on the choice of the numbering functions f_x .

This group is a complete monomial group which is a special case of a wreath product. Before giving a general description of these groups we give an example that will play a prominent role later in the discussion of the n -dimensional cube.

Example: Let $C = \{(x_i) \in \mathbb{R}^n : -1 \leq x_i \leq 1 \text{ for each } i\}$ be the n -cube centered at the origin in real n -space \mathbb{R}^n . The standard basis vectors e_1, \dots, e_n are the midpoints of the facets (= $n-1$ -dimensional faces) of the n -cube. A symmetry of C is a rigid motion of \mathbb{R}^n that maps C to itself. It is clear that any symmetry takes e_i to $\pm e_j$ for some j . The matrix of such an orthogonal transformation must be monomial (i.e. have exactly one nonzero entry in each row and column) with nonzero entries equal to ± 1 . Thus the group of symmetries of C is the group of order $2^n n!$ of $n \times n$ monomial matrices with nonzero entries equal to ± 1 . The orientation-preserving symmetries form a subgroup of index 2;

this subgroup contains all matrices of determinant +1. The group of symmetries is sometimes called the hyperoctahedral group; it is isomorphic to the wreath product (see below) $\{+1\} \wr S_n$. It can also be thought of as a permutation group on the $2n$ vectors $\pm e_i$. In fact it is the maximal permutation group on those vectors that preserves the equivalence relation "is the negative of".

If G is a group, X is a set, and H is a permutation group on X then the wreath product $G \wr H$ is defined to be the set of all pairs (f, s) where $s \in H$ and $f: X \rightarrow G$. Multiplication is defined by

$$(f, s)(g, t) = (h, st) \quad \text{where} \quad h(x) = f(x)g(sx) .$$

If $H = \text{Sym}(X)$ then this is called a complete monomial group. If X has n elements so that $\text{Sym}(X) \cong S_n$ then this group can be given several more concrete interpretations:

- 1) $G \wr S_n \cong$ the set of all $n \times n$ monomial matrices with nonzero entries from G ; the group operation is induced by multiplication of matrices and the group operation on G .
- 2) $G \wr S_n \cong$ the semidirect product $G^n \rtimes S_n$ with S_n acting by permuting the n copies of G .

(We remark that we make all group actions operate on the left so that, for example, permutations in S_n are multiplied from right to left.)

If G' denotes the commutator subgroup of G then the abelianization G/G' is an abelian group. Consequently if (f, s) is an element of the complete monomial group $G \wr \text{Sym}(X)$ then the image of the product $\prod_{x \in X} f(x)$ in G/G' is well-defined (i.e.

is independent of the ordering of terms in the product). In fact it is easy to use the group operation defined above to check that $\chi(f,s) = \left[\prod_{x \in X} f(x) \right]$ gives a homomorphism

$$\chi: G \sim \text{Sym}(X) \rightarrow G/G'$$

If the complete monomial group is thought of as the group of $n \times n$ monomial matrices then this homomorphism is given by the image of the product of all nonzero entries of a matrix. We will call this map the canonical character of the complete monomial group.

Now return to the earlier situation: G_{\max} is a maximal imprimitive permutation group on a finite set Y in which each of the equivalence classes $x \in X$ has m elements. For all x choose a numbering $f_x: x \rightarrow \bar{m}$. We obtain an isomorphism $G_{\max} \cong S_m \sim \text{Sym}(X)$ and a canonical character $\chi: G_{\max} \rightarrow S_m/S'_m = S_m/A_m = \{+1\}$.

Proposition 1: The map χ is independent of the choice of numberings.

Proof: Let g be an element of G_{\max} and let $s = \alpha(g)$ be its image in $\text{Sym}(X)$. By retracing the definition of the isomorphism $G_{\max} \cong S_m \sim \text{Sym}(X)$ we find the canonical character is the image of the product

$$\prod_{x \in X} f_{sx} \circ g \circ f_x^{-1}$$

in the quotient $S_m/A_m = \{+1\}$. Any other numbering on the class x is of the form $\sigma \circ f_x$ where σ is some element of S_m . If the numbering is changed on the class x two terms in the above product are changed. The terms in the product can be reordered at will (since the image lies in an abelian group) so we put the two terms next to each other. The σ and σ^{-1} then cancel so that the value of the character χ is unchanged. This proves the proposition.

We will call χ the canonical character of G_{\max} . In the sequel we will also need a slightly more general construction, although it will be relevant only for the motions of the vertices of the n -cube.

Say that two numberings $f_x: x \rightarrow \bar{m}$ and $F_x: x \rightarrow \bar{m}$ of the m -element set x are equivalent if $F_x \circ f_x^{-1}$ is in the alternating group $A_m = \text{Alt}(\bar{m})$. An orientation on x is an equivalence class of numberings. There are two possible orientations on a finite set. A map $g: x \rightarrow x'$ of oriented sets is orientation-preserving if $f_{x'} \circ g \circ f_x^{-1}$ is in A_m (where f_x and $f_{x'}$ are chosen from the orientations in question).

Now assume that Y is a finite set equipped with an equivalence relation as above for which each equivalence class has m elements. Assume further that each class x is supplied with an orientation. Let G_{\max}^O denote the maximal permutation group on Y that respects the given equivalence relation and induces orientation-preserving maps on the equivalence classes. Thus if g is in G_{\max}^O then its restriction to the elements in the class x gives a map from x to sx (where $s = \alpha(g)$) that is orientation-preserving. It is now possible to repeat the Proposition above in this context and to obtain a well-defined canonical character $\chi: G_{\max}^O \rightarrow A_m/A_m'$ that is independent of any choices.

Remarks:

- 1) Since $A_m = A_m'$ for $m > 4$ this map is trivial unless $m = 3$ or $m = 4$.
- 2) This procedure could be applied to any permutation group H in S_m ; one would define H -equivalent numberings and obtain a canonical character $\chi: G_{\max, H} \rightarrow H/H'$.

3) If all orientations on the classes x are reversed it can be verified that for $m = 3$ and $m = 4$ the canonical character becomes $\chi(g)^{-1}$.

4) The proof of the proposition above is reminiscent of the verification that the transfer homomorphism in group theory is well-defined. In fact if H is the subgroup of G_{\max} that fixes a class x as a set and H_x is the subgroup that fixes the elements of x then it can be verified that the canonical map is essentially the map $G_{\max} \rightarrow H/H_x H'$ obtained as a quotient of the transfer homomorphism.

2. The 3-cube. The usual 3-dimensional Magic Cube is certainly one of the few things that deserves the overworked mathematical adjective "well-known". We briefly recall some of the details in order to describe the associated finite group.

The Magic Cube appears to consist of a $3 \times 3 \times 3$ array of smaller colored cubes. The initial, or solved, configuration is the arrangement in which all 6 sides of the Cube are monochromatic. Henceforth the small cubes will be called cubelets and their faces facelets; the position of a cubelet will be called a cubicle. There are 54 visible colored facelets, 9 on each of the 6 sides of the Cube.

A move (or generating move, or generator) consists of turning all 9 cubelets on a side as a block through a half turn (180°) or a quarter turn (90°) in either direction. A process is a sequence of moves. The object of the puzzle is to devise an algorithm that converts a random configuration (easily obtained by a few unthinking

moves) to the solved configuration by a suitable process.

By a little experimentation one rapidly discovers that no internal facelets ever appear. In fact there is no middle cubelet. These facts can be verified by disassembling the device (by prying off an edge cubelet from a face that is rotated 45°) to reveal Professor Rubik's ingenious mechanism.

Thus there are exactly 26 cubelets and 54 facelets. They are of three types: the 6 center cubelets (each with one colored facelet), the 12 edge cubelets (each with two colored facelets), and the 8 corner cubelets (each with three colored facelets). Moves, and hence processes, take corner cubelets only to corner cubicles; similarly for edges and centers.

In order to evaluate the position or configuration ^{of the Cube} we will fix the positions of the center cubelets; for instance one could require that the red center cubelet be on the top, the blue center on the left, etc. Since experimentation (or an examination of the underlying mechanism) shows that the relative positions of the center cubelets are fixed anyway this is no real loss of generality. A configuration (or position) of the Cube is then any permutation of the edge and corner facelets that can be obtained by dumping the corner and edge cubelets onto a table and then reassembling the Cube. A reachable configuration is one that can be obtained by a process (i.e. a sequence of moves).

Let Y_c denote the set of corner facelets, Y_e the set of edge facelets, and $Y = Y_c \cup Y_e$. The fundamental problem is then the following:

Describe the group $H \subset \text{Sym}(Y)$ that is generated by moves.

The elements of H correspond to reachable configurations.

Let $G \subset \text{Sym}(Y)$ be the permutation group on Y consisting of permutations that can be obtained by the "dump" moves described above. The group G is substantially smaller than the group $\text{Sym}(Y) \approx S_{48}$ of all $48!$ permutations. In fact elements of G must satisfy some obvious constraints: corner (resp. edge) facelets must be taken to corner (resp. edge) facelet positions (so that G is contained in $\text{Sym}(Y_c) \times \text{Sym}(Y_e)$), elements of G must preserve the equivalence relation of "being on the same cubelet", and, finally, the clockwise order of the three facelets on a corner cubelet must be preserved.

With these remarks it is easy to count the total number of configurations (i.e. to find the order of G). There are $12!$ ways to put the 12 edge cubelets into the edge cubicles and two possible orientations for each edge cubelet within a given cubicle. There are $8!$ ways to rearrange the positions of the corner cubelets and three possible orientations of a cubelet in a given cubicle. Hence the total number of configurations is

$$3^8 8! 2^{12} 12! = 519024039203878272000 \approx 1.5 \times 10^{20} .$$

It turns out that H is a proper subgroup of G . Thus there are configurations that can be realized by dumping the Cube and reassembling it that can not be obtained by processes. In fact H is a subgroup of index 12 in G ; only $1/12$ of all configurations are reachable. Thus no matter how furiously you manipulate your Cube you will see at most

$$3^8 8! 2^{12} 12! / 12 = 43252003274489856000 \approx 4.3 \times 10^{19}$$

positions. If someone has tampered with your Cube (by dumping randomly or by interchanging facelets) then you may not be able

to even obtain the solved configuration.

The number of reachable configurations is bigger than the current guess of the age of the universe in seconds. Thus it is unlikely that you'll see anything but a terribly minute fraction of these configurations in your lifetime. Moreover most "random" configurations that you see are probably being seen for the first and last time by human eyes. It is amusing to note that the Ideal Toy Corporation, who first marketed the Cube in this country on a large scale, claimed in their promotional material that there were "more than 3 billion positions" of the Cube.

In order to prove that H is of index 12 in G it is necessary to analyze the structure of G a little more closely. Let Ξ_c and Ξ_e denote the equivalence relation "being on the same cubelet" on the sets Y_c and Y_e of corner and edge facelets. The sets X_c and X_e of equivalence classes can of course be identified with the sets of corner and edge cubes respectively. Orient the three facelets on a given corner by saying that a numbering is correctly oriented if it increases in a clockwise direction as viewed from outside the Cube. Let G_e denote the maximal permutation group on Y_e that respects Ξ_e and let G_c denote the maximal permutation group on Y_c that respects Ξ_c and induces orientation-preserving maps on the corners. In more concrete terms G_e (resp. G_c) represents the edge (resp. corner) configurations that can be obtained by dumping and reassembling the edge (resp. corner) cubelets. In any case, it is clear that $G = G_e \times G_c$.

There are natural surjections $G_c \rightarrow \text{Sym}(X_c)$, $G_e \rightarrow \text{Sym}(X_e)$. In concrete terms this just means that dump processes can be viewed as permuting the cubelets without caring about the action

on facelets. We can now describe the first "non-obvious" constraint satisfied by reachable configurations. Let \bar{g} denote the image of an element g of G_c (resp. G_e) in $\text{Sym}(X_c)$ (resp. $\text{Sym}(X_e)$) and let $\text{sgn}(s) \in \{\pm 1\}$ denote the parity of a permutation s .

PARITY-LAW: If $g = (g_c, g_e) \in G_c \times G_e = G$ lies in the subgroup H of reachable configurations then $\text{sgn}(\bar{g}_c) = \text{sgn}(\bar{g}_e)$. In other words, the parity of the corner cubelet permutation determined by a process is equal to the parity of the edge cubelet permutation.

Proof: Any process can be realized as a sequence of quarter turns. Any quarter turn simultaneously does a 4-cycle on the 12 edge cubelets and a 4-cycle on the 8 corner cubelets since the 4 corners and edges on the face being turned are permuted cyclically. 4-cycles are odd permutations so the corner and edge permutations can be odd or even; however the parity of these two permutations must be the same at all times (i.e. after an odd number of quarter turns the parity of the permutation in $\text{Sym}(X_c) = S_8$ must be odd and the parity in $\text{Sym}(X_e) = S_{12}$ must also be odd; after an even number of quarter turns both permutations are even).

This proves the parity constraint.

Remark: It is clear that the parity constraint is true of exactly 1/2 of the elements of $G = G_c \times G_e$.

Let H_c (resp. H_e) be the projection of H onto G_c (resp. G_e). Thus H_c corresponds to the reachable configurations of corner cubelets and H_e corresponds to reachable configurations of edge cubelets. There are two more "non-obvious" constraints on H ; they concern the "twists" or orientations of the cubelets.

Any quarter turn moves 8 edge facelets. In fact a quarter turn is a product of two disjoint 4-cycles in $\text{Sym}(Y_e)$. Since this is an even permutation it follows that $H_e \subset G_e \cap \text{Alt}(Y_e)$, i.e. that the permutation of the edge facelets is always even. It is easy to check that this is equivalent to the following constraint:

EDGE-TWIST LAW: If χ_e is the canonical character on G_e (see the previous section) then H_e is contained in the kernel of χ_e .

Proof: Let g be a fixed quarter turn. Choose a numbering $Y_e = X_e \times \bar{2}$ so that $\chi_e(g)$ is obviously equal to 1 (e.g. by giving all facelets lying on the face being turned the number 1).

Proposition 1 says that the value of the canonical character is independent of the choice of numberings. Hence the value of the canonical character on any move or process is 1.

Remark: Choose a numbering. In an arbitrary configuration say that an edge cubelet is flipped if its facelet with number 1 is in the number 2 facelet position of its edge cubicle (i.e. the number 2 facelet position of the edge cubelet in that cubicle in the solved configuration). The above law says that in any reachable configuration the number of flipped edges is even.

Finally we come to the corners. From section 1 we know that $G_c \simeq A_3 \sim \text{Sym}(X_c)$ and that there is a canonical character $\chi_c: G_c \rightarrow A_3$.

CORNER-TWIST LAW: H_c is contained in the kernel of χ_c .

Proof: As above choose an obvious numbering (consistent with the orientations) so that a given quarter turn is trivially in the kernel of χ_c . The law then follows from Proposition 1.

Remarks:

- 1) This law also follows trivially from the fact that an element of order 4 must be in the kernel of any map to a group of order 3.
- 2) If all orientations are reversed (i.e. "clockwise" is replaced by "counterclockwise" above) then by remark 3) at the end of the preceding section the kernel of the canonical character is unchanged
- 3) As for edges, this constraint can be phrased in terms of twists on the corner cubelets. For each corner cubelet x in an arbitrary configuration let $t_x \in \{0, 1, 2\}$ be the number of clockwise twists of the cubelet that are necessary to align its facelet numbers with the facelet numbers of the cubelet that would be there in the solved configuration. The corner-twist law says that the sum of all t_x is divisible by 3 in any reachable configuration. One explicit way to specify enough of a numbering to compute this is to first choose a pair of colors on opposite faces. These will be called dominant (or chief) colors. Each corner cubelet contains exactly one dominant facelet. At each corner in an arbitrary configuration count the number of clockwise twists necessary to bring the dominant color into the facelet position of the dominant color in the solved configuration (this is easy to see by using the center colors as a reference). The sum of these 8 twists should be divisible by 3. Thus you can find out whether the corners of your Cube have been tampered with without actually having to solve the Cube (though for some people the latter method would be faster). A similar procedure exists for verifying the edge-twist law (e.g. [4] or [15]).

3. The group H. The results of the previous section show that the group H, whose elements are in one-to-one correspondence with reachable configurations, is contained in an explicit subgroup of the group G of all configurations. In fact it is not hard to use a solution algorithm to show that H is exactly equal to this subgroup. A careful examination of any of the known solution algorithms will show that they describe how to take any configuration that satisfies the three constraints of the previous section and to apply a process to obtain the solved configuration. By applying this backwards we see that any configuration satisfying the three constraints is reachable. Thus

$$H = \{(g_c, g_e) : \text{sgn}(\bar{g}_c) = \text{sgn}(\bar{g}_e), \chi_e(g_e) = 1, \chi_c(g_c) = 1\} .$$

The goal of this section is to give a proof of this that does not rely on a solution algorithm. Instead we will use some results from group theory. The astute reader will observe that the existence of a solution algorithm, albeit an extremely inefficient one, is implicit in the proof of this result.

Theorem 1: The natural projections $\alpha_c: H_c \rightarrow \text{Sym}(X_c)$, $\alpha_e: H_e \rightarrow \text{Sym}(X_e)$ are surjective.

Remark: Thus any permutation of the 8 corners can be realized by a suitable process; similarly for the edges. Of course the parity-law says that they can not necessarily be realized simultaneously.

Proof 1: In diagram 1 we give a process. It transposes adjacent corners. It is easy to check that by suitably transposing adjacent corners any two corners can be transposed. Since $\text{Sym}(X_c) = S_8$ is generated by transpositions it follows that $\alpha_c(H_c) = \text{Sym}(X_c)$ as claimed. (Recall that the effect of the map α_c is to "forget" the corner orientation; thus in this proof we are merely concerned with the positions of the corner cubelets and not their orientation

within a cubicle.)

The process in diagram 1 gives a transposition of adjacent edges so the same proof works for the edges.

Proof 2: This proof uses a much deeper result on permutation groups but it has the virtue of applying without change to the n-cube.

False

First note that $\alpha_c(H_c)$ is generated by 4-cycles. It is easy to check that the image is doubly transitive (by showing, for instance, how to put arbitrary corners into diagonally opposite corner cubicles) and hence primitive. A theorem of Jordan and Marggraff (see [10] or [6]) says that any primitive permutation group on n objects that contains a k -cycle for $k > 1$ is $n-k+1$ transitive. Hence $\alpha_c(H_c)$ is 5-transitive. Any permutation group on n objects that is m -transitive for $m > n/2$ contains the alternating group. Hence $\alpha_c(H_c) = \text{Sym}(X_c)$. The proof for the edges is the same.

Now let K_c be the kernel of $\alpha_c: H_c \rightarrow \text{Sym}(X_c)$ and let K_e be the kernel of $\alpha_e: H_e \rightarrow \text{Sym}(X_e)$. In order to obtain the structure of the groups H_c and H_e (and then H) we must describe these kernel groups.

In concrete terms (i.e. after the corners and edges have been numbered) we can think of K_c as a "twist-vector" consisting of an 8-tuple with components from $\{0,1,2\}$ and K_e as a 12-tuple with components from $\{0,1\}$. In each case the i -th component represents the twist of the cubelet in the i -th cubicle.

Note that $S_8 = \text{Sym}(X_C)$ acts on $(\mathbb{Z}/3\mathbb{Z})^8$ and that K_C must be preserved under this action. Indeed, if $x \in K_C$ then the conjugate of x by $g \in H_C$ is given by permuting the 8-components of x by $\alpha_C(g)$. A similar statement is true for K_e .

Proposition 2: If p is a prime and $K \subset (\mathbb{Z}/p\mathbb{Z})^n$ is a subgroup that is invariant under the action of S_n , and if K contains a vector with 2 unequal components, then K contains the subgroup of order p^{n-1} consisting of those vectors $x = (x_1, \dots, x_n)$ whose component sum $x_1 + \dots + x_n$ is 0 mod p .

Proof: If x is such a vector let x' be the vector obtained by transposing the unequal components. Then $x' \in K$ by the assumption on K . The vector $x-x' \in K$ has 0 in all but 2 components. By adding this vector to itself a suitable number of times one obtains a vector with nonzero components equal to 1 and -1 (using the fact that p is a prime). This vector and its permutations clearly generate the indicated subgroup; indeed we can obtain any desired values in the first $n-1$ components. This finishes the proof.

Theorem 2: With the identifications above,

$$K_C = \{(x_i) \in (\mathbb{Z}/3\mathbb{Z})^8 : \sum x_i \equiv 0 \pmod{3}\}$$

$$K_e = \{(x_i) \in (\mathbb{Z}/2\mathbb{Z})^{12} : \sum x_i \equiv 0 \pmod{2}\} .$$

Proof: By the corner-twist and edge-twist laws we know that K_C and K_e must be proper subgroups of $(\mathbb{Z}/3\mathbb{Z})^8$ and $(\mathbb{Z}/2\mathbb{Z})^{12}$. If we square the process in Diagram 1 we obtain an element that fixes the corner and edge positions. Hence we get elements of the kernel groups K_C

and K_e ; by inspection they have two unequal components. The theorem then follows from the preceding Proposition.

Since K_c is of index 3 in $(\mathbb{Z}/3\mathbb{Z})^8$ it follows that H_c is of index 3 in G_c . Since the canonical character χ_c is of order 3 its kernel is of index 3 and we conclude that $H_c = \ker(\chi_c)$. For similar reasons $H_e = \ker(\chi_e)$.

In concrete terms (i.e. after choosing numberings) we have a diagram

$$\begin{array}{ccccccc}
 0 & \rightarrow & K_c & \rightarrow & H_c & \rightarrow & \text{Sym}(X_c) \rightarrow 1 \\
 & & \cap & & \downarrow & & \cong \\
 0 & \rightarrow & (\mathbb{Z}/3\mathbb{Z})^8 & \rightarrow & (\mathbb{Z}/3\mathbb{Z}) \wr S_8 & \rightarrow & S_8 \rightarrow 1
 \end{array}$$

in which K_c and H_c have index 3 in the corresponding groups on the bottom row. There is a similar diagram for H_e .

The group H generated by all processes is a subgroup of the direct product $H_c \times H_e$; it projects surjectively onto either component. There is a standard classification theorem for such subgroups of direct products (e.g. [6], p. 63): any subgroup of $G_1 \times G_2$ that projects surjectively onto the components must be of the form

$$\{(g_1, g_2) : f_1(g_1) = f_2(g_2)\}$$

where $f_i: G_i \rightarrow T$ are surjective homomorphisms onto a common group T . Thus subgroups of a direct product are determined by isomorphic quotient groups of G_1 and G_2 .

From the structure of H_c and H_e we see that the only possible nontrivial isomorphic quotient of H_c and H_e is $\{\pm 1\}$;

the corresponding subgroup is

$$\{(g_c, g_e) : g_c \in H_c, g_e \in H_e, \text{sgn}(\bar{g}_c) = \text{sgn}(\bar{g}_e)\} .$$

Since the parity-law tells us that H is contained inside this group it follows that H must be equal to this group.

We summarize the content of these results.

Theorem 3: The group G corresponding to all configurations is $G = G_c \times G_e$ where $G_c = (\mathbb{Z}/3\mathbb{Z}) \sim S_8$, $G_e = (\mathbb{Z}/2\mathbb{Z}) \sim S_{12}$. The group H corresponding to reachable configurations is

$$H = \{(g_c, g_e) : \chi_c(g_c) = 1, \chi_e(g_e) = 1, \text{sgn}(\bar{g}_c) = \text{sgn}(\bar{g}_e)\}$$

where χ_c and χ_e are the canonical characters on the respective wreath products.

Remark: The subgroup $H_c = \ker(\chi_e)$ is the unique subgroup of $(\mathbb{Z}/3\mathbb{Z}) \sim S_8$ of index 3. However, there is a subgroup of $(\mathbb{Z}/2\mathbb{Z}) \sim S_{12}$ that is of index 2, surjects onto S_{12} , has K_e as its kernel, and is not the kernel of χ_e . Namely,

$$\{(x, s) \in (\mathbb{Z}/2\mathbb{Z}) \sim S_{12} : (-1)^{\sum x_i} = \text{sgn}(s)\} .$$

4. A more general geometric group. The group of the 3-cube could be regarded as a transformation group on the points of \mathbb{R}^3 . It is generated by applying rigid motions to a half-space determined by a hyperplane. In this section we extend this idea to a much more general context; this seems to encompass all known generalizations of the Magic Cube.

A hyperplane in \mathbb{R}^n is a translate of an $n-1$ -dimensional vector subspace; an arrangement ([2], []) is a finite set of hyperplanes in \mathbb{R}^n . Let \mathcal{E} be an arrangement in \mathbb{R}^n and assume that

for each $h \in H$ we are given a group E_h of orientation-preserving rigid motions of \mathbb{R}^n whose restriction to h is an orientation-preserving rigid motion of the hyperplane h . We will also assume that the other hyperplanes in Σ are permuted among themselves by the elements of E_h :

$$g(h') \in \Sigma \quad \text{for each } g \in E_h, h' \in \Sigma .$$

In the case corresponding to the Magic Cube in \mathbb{R}^3 we would have 6 hyperplanes (two normal to each coordinate axis) and the group E_h would be the cyclic group of order 4 generated by 90° rotations around a suitable normal vector to the plane h .

Any hyperplane h in \mathbb{R}^n splits \mathbb{R}^n into two half-spaces; we arbitrarily label the open half-spaces h^+ and h^- so that there is a disjoint decomposition

$$\mathbb{R}^n = h^+ \cup h \cup h^- .$$

If $h \in \Sigma$ and $g \in E_h$ then since g , and its restriction to h , are orientation-preserving we have

$$g(h^+) = h^+, \quad g(h^-) = g(h^-).$$

We use this fact to define permutations g^+ and g^- of the points of \mathbb{R}^n by

$$g^\pm(x) = \begin{cases} gx & \text{if } x \in h^+ \\ x & \text{if } x \in h \cup h^- . \end{cases}$$

Thus $g^\pm \in \text{Sym}(\mathbb{R}^n)$ moves an open half-space.

Now we let $H = H(\Sigma, \{E_h\})$ be the subgroup of $\text{Sym}(\mathbb{R}^n)$ that is generated by all of the g^+ and g^- as g ranges over all E_h , $h \in \Sigma$. The fundamental problem for any Σ and $\{E_h\}$ is to describe this group.

The group H is finite. Indeed, the hyperplanes in Σ partition \mathbb{R}^n into a finite number of cells that are permuted by H . Since each of these cells has only finitely many symmetries it follows that H must be a finite group. In the case of the 6 hyperplanes in \mathbb{R}^3 the group H is bigger than the group obtained in the previous section. The group H would be the semidirect product of the "supergroup" ([15], [17]) by the group of order 24 of symmetries of a cube. The group in the previous section is a quotient of the supergroup by an abelian group that corresponds to taking the rotation of the center pieces into account in describing a configuration. The semidirect product with the symmetry group of the cube corresponds to taking into account the position of the cube in space.

One general strategy for describing H that works in many cases is to judiciously choose a finite set of points in \mathbb{R}^n (analogous to facelets) on which H acts faithfully. One can then hope to partition the points into their H -orbits and then apply the ideas of section 1. In all cases that we have considered the groups are essentially subgroups of wreath products when acting on the various orbits, and the canonical character plays a prominent role.

5. The n-cube. In order to focus on an interesting case in which we can completely describe the group H we will devote the rest of this paper to the n -dimensional generalization of the Magic Cube. This section contains some preliminary results on the group of symmetries of the n -cube.

Let $C_n = \{(x_i) \in \mathbb{R}^n : -1 \leq x_i \leq 1 \text{ for all } i\}$ be the n -cube centered at the origin in n -space. Let $E(C_n)$ denote the group of symmetries of C_n - the group of rigid motions g of \mathbb{R}^n such that $g(C_n) = C_n$. From the first section we know that $E(C_n) \cong \pm 1 \wr S_n$. The matrices of the orthogonal transformations in $E(C_n)$ are monomial matrices whose nonzero entries are ± 1 .

There are 4 homomorphisms from $E(C_n)$ to $\{\pm 1\}$: the trivial map, the determinant mapping $\det(g)$, the canonical character $\chi(g)$ of the wreath product, and the map taking g to $\text{sgn}(\bar{g})$ where $\bar{g} \in S_n$ is the underlying permutation. The product of any two of the nontrivial characters is equal to the third. By using the semidirect product representation of the wreath product it can be checked that the commutator subgroup $(\{\pm 1\} \wr S_n)'$ is the group of matrices with an even number of -1 's and whose underlying permutation is even. Since this group is of index 4 it follows that the 4 maps above are the only one-dimensional characters of $E(C_n)$ (i.e. the only homomorphisms $E(C_n) \rightarrow \mathbb{C}^*$).

If $0 \leq d \leq n$ then a d -dimensional face of C_n is a set of vectors which have $n-d$ fixed components each having the value 1 or -1 , and d components that range over all values between -1 and 1. Since there are $\binom{n}{d}$ ways to partition the coordinates into two classes and 2^{n-d} ways to choose the values of the fixed coordinates it follows that there are

$$N_d = \binom{n}{d} 2^{n-d}$$

d -dimensional faces of C_n .

Matrix multiplication show that

$$\begin{aligned} a(\underline{+e}_1) &= \overline{+e}_1, & a(\underline{+e}_2) &= \underline{+e}_2 \\ b(\underline{+e}_1) &= \underline{+e}_2, & b(\underline{+e}_2) &= \underline{+e}_1. \end{aligned}$$

Hence a induces an odd permutation on the midpoint vectors (and hence on the faces) and b induces an even permutation. Since the canonical character is the product of the nonzero entries of a matrix, $\chi(a) = -1$ and $\chi(b) = 1$. Thus $\text{sgn}(g_{n-1}) = \chi(g)$ and the second statement of the proposition is proved.

Now consider $d = n-2$. The midpoint vectors are the vectors $e_{ij}(x,y)$ which have i -th coordinate equal to $x \in \{\underline{+1}\}$ and j -th coordinate equal to $y \in \{\underline{+1}\}$. We take $i < j$; there are $4\binom{n}{2} = N_{n-2}$ such vectors. On the 4 vectors $e_{12}(\underline{+1},\underline{+1})$ it is easy to check that a induces an even permutation and b induces an odd permutation. On the rest of the vectors it is easy to pair up transpositions; for instance a transposes $e_{13}(1,1)$ and $e_{13}(-1,1)$ and it transposes $e_{13}(1,-1)$ and $e_{13}(-1,-1)$. Hence $\text{sgn}(a_{n-2}) = 1$ and $\text{sgn}(b_{n-2}) = -1$. Since the character $\text{sgn}(\overline{g})$ has the same property the third assertion of the proposition is proved.

Finally, consider $d < n-2$. The midpoint vectors all have more than 2 nonzero coordinates. It is easy to see that if a or b transpose two vectors u and v then they also transpose the vectors u' and v' where the signs of (say) the 3-rd components of u and u' (resp. v and v') are opposite. Hence a and b give an even number of transpositions and the proposition is proved.

6. The group of the n -cube. As above let C_n be the n -cube and X_d the set of d -dimensional faces (called d -faces for short) of C_n . When convenient we will identify d -faces with their midpoint

vectors. An $n-1$ -face is called a facet; the midpoint vector of a facet is of the form $\frac{1}{2}e_i$. If y is a facet and x is a d -face then $x \subset y$ is equivalent to saying that the midpoint vector of y can be obtained from the midpoint vector of x by setting all but one of the coordinates equal to 0.

As in the 3-dimensional case we want to construct a transformation group on \mathbb{R}^n arising from $2n$ hyperplanes, each orthogonal to a standard basis vector. This arrangement of hyperplanes divides C_n into 3^n subcubes. Each "side" of C_n consists of 3^{n-1} subcubes; the generators of our group will move these 3^{n-1} cubes as a block by a symmetry that is determined by an $n-1$ -dimensional orientation-preserving symmetry of the corresponding facet. In order to have the group follow as closely as possible along the lines of the 3-cube we will ignore the movements of the facets; this corresponds to taking a quotient of the group defined in the previous section.

For $0 \leq d < n-1$ let

$$Y_d = \{(y,x) : y \text{ is a facet, } x \text{ is a } d\text{-face, } x \subset y\}.$$

We will call the elements of Y_d the d -facelets. Let $Y = \bigcup_{d=0}^{n-2} Y_d$.

For $0 < d < n-1$ let G_d be the maximal permutation group on Y that preserves the equivalence relation "has the same second component". For $d = 0$ we orient the n 0-facelets with a given 0-face (vertex) x as second component by saying that a numbering of the facelets (y_i, x) is positive if the determinant of the matrix whose columns are the y_i in order is equal to +1. G_0 is the maximal subgroup of $\text{Sym}(Y_0)$ that preserves the relation "has the same second component" and induces a orientation-preserving mappings on the facelets lying over a given vertex.

These definitions are the exact analogue of the corresponding definitions for the 3-cube. Indeed, each facelet on the Magic Cube resides on a given 0-face (corner) or 1-face (edge) of the cube and it has a color corresponding to one of the 6 facets. On the n -cube there are $2n$ facets (colors).

In the case of the 3-cube the generating moves are the cyclic groups of order 4 generated by quarter turns around the coordinate axes. These symmetries are extensions to \mathbb{R}^3 of the orientation-preserving symmetries of the sides (which are 2-cubes). For each facet y of C_n let E_y denote the group of orientation-preserving rigid motions of the facet y . Since the facets of the n -cube C_n are $n-1$ -cubes it follows that $E_y = E(C_{n-1})^0$, where $E(C_{n-1})^0$ denotes the subgroup of index 2 of orientation-preserving symmetries (whose determinant is equal to 1). A rigid motion g of the hyperplane spanned by y extends in a unique way to an orientation-preserving rigid motion, which we will also denote g , of \mathbb{R}^n . Any vector normal to the hyperplane is fixed.

For each facet y_0 the group E_{y_0} acts in a natural way on the collection of all facelets: if $g \in E_{y_0}$ then define $\tilde{g} \in \text{Sym}(Y)$ by

$$\tilde{g}(y, x) = \begin{cases} (gy, gx) & \text{if } x \subset y_0 \\ (y, x) & \text{otherwise.} \end{cases}$$

In concrete terms we can write (the midpoint vectors of) y and x and let a matrix g act on them by matrix multiplication; the matrix g is obtained from an $n-1$ by $n-1$ monomial matrix in $E(C_{n-1})$ by adding an i -th row and i -th column equal to e_i if $y = \pm e_i$. A little thought should persuade you that this is the exact generalization of the generating moves on the usual 3-cube.

Let H be the subgroup of $\text{Sym}(Y)$ that is generated by the \tilde{g} as g ranges over all E_y where y is one of the $2n$ facets. The

group H is contained in the group $G = \prod_{d=0}^{n-2} G_d$ of all "configurations" (in the case of orientations on the vertices X_0 this will be spelled out in detail in the course of the next theorem). Our central goal is to describe H explicitly as a subgroup of G .

Each d -face x is contained in $n-d$ different facets y . Hence there are $n-d$ facelets whose second component is x . We can choose a numbering $Y_d \approx X_d \times \overline{n-d}$ and find that for $d > 0$ $G_d \approx S_{n-d} \sim \text{Sym}(X_d)$ and that $G_0 \approx A_n \sim \text{Sym}(X_0)$. We let χ_d denote the corresponding canonical character. For each $g_d \in G_d$ we let \bar{g}_d denote the underlying permutation in $\text{Sym}(X_d)$.

The "reachable configurations" satisfy constraints described in the following theorem.

Theorem 4: Let $g = (g_d) \in G = \prod_{d=0}^{n-2} G_d$. If g is in H then

$$\text{sgn}(\bar{g}_{n-2}) = \text{sgn}(\bar{g}_{n-3})$$

$$\text{sgn}(\bar{g}_d) = 1 \quad \text{for } 0 \leq d < n-3$$

$$\chi_d(g_d) = 1 \quad \text{for } 0 \leq d < n-1 .$$

Remark: For $n = 3$ these are exactly the constraints in section 2.

For $n = 4$ they can also be found in [7].

Proof: It suffices to verify these conditions for the generators g . Fix a facet y_0 and let g be a symmetry in E_{y_0} . Let g_d denote the projection of g onto G_d .

The group $E_{y_0} = E(C_n)^0$ of orientation-preserving symmetries of the $n-1$ -cube is the kernel of the character $\det()$. By

Proposition 3 the character $\text{sgn}(\bar{g})$ is equal to the canonical character $\chi(g)$ on the kernel of $\det(g)$. The parity of \bar{g}_d on the d -faces X_d is determined by that result (since g_d fixes the d -faces not contained in y_0 and y_0 is an $n-1$ -cube):

$$\text{sgn}(\bar{g}_{n-2}) = \text{sgn}(\bar{g}_{n-3}) = \chi(g)$$

$$\text{sgn}(\bar{g}_d) = 1 \quad \text{for } 0 < d < n-3$$

This proves the first two constraints.

Suppose that $d > 0$. For each d -face x let $[x]$ denote the set of facelets whose second component is x ; choose numberings $f_x: [x] \rightarrow \bar{n-d}$ for each x . The value of the canonical character χ_d on g_d is the class of

$$\prod_{x \in X_d} f_{sx} \circ g_d \circ f_x^{-1}$$

in $\{\pm 1\} = S_{n-d}/A_{n-d}$, where $s = \bar{g}_d \in \text{Sym}(X_d)$.

By the definition of g we can ignore terms in the above product corresponding to d -faces x that are not contained in y_0 . If x is a d -face in y_0 let x' denote the "antipodal" face in y_0 ; its midpoint vector is obtained from the midpoint vector of x by negating all components except the i -th if (the midpoint vector of) y is $\pm e_i$. By Proposition 1 we are free to choose the numberings as we wish. Choose the numbering at x to be the "same" as at x' : $f_x(y, x) = f_{x'}(y', x')$. Since g_d is induced by a linear map we have $g_d(y)' = g_d(y')$. It follows that the term at x in the above product is the same as the term at x' . Hence $\chi_d(g_d) = 1$ as claimed.

For $d = 0$ the canonical character is automatically trivial for $n > 4$. For $n = 3$ and $n = 4$ the groups E_{y_0} are generated by

elements of order 4 and the image of the canonical character is in a group of order 3 since $A_3/A_3' \cong A_4/A_4' \cong A_3$. Hence $\chi_0(g_0) = 1$ and the theorem is proved.

Remark: The order of the subgroup of G that satisfies these constraints is

$$\frac{1}{2^{2n-4} 2^{N_0} [A_n : A_n']} \prod_{d=0}^{n-2} N_d! (n-d)!^{N_d} .$$

For $n = 4$ this is roughly 1.8×10^{120} . If Ideal Toy ever gets around to marketing this puzzle perhaps it will contain "at least one trillion positions."

Finally, we must prove that H is actually equal to the subgroup of G satisfying these constraints.

Theorem 5: The group H corresponding to "reachable configurations" is

$$H = \{(g_d) \in G : \text{sgn}(\bar{g}_{n-2}) = \text{sgn}(\bar{g}_{n-3}), \text{sgn}(\bar{g}_d) = 1 \text{ for } d < n-3, \\ \chi_d(g_d) = 1 \text{ for } 0 \leq d < n-1 .$$

The index of H in G is $2^{2n-4} [A_n : A_n']$.

Proof: For each d let H_d denote the projection of H onto G_d . We will follow the pattern of the $n = 3$ case and first prove that the projection of H_d onto $\text{Sym}(X_d)$ is as big as claimed, then prove that H_d is as big as claimed, and finally prove that H is as big a subgroup of H_d as claimed.

References

1. M. R. Black and Herbert Taylor, *Unscrambling the Cube*, Zephyr Engineering Design, 1980.
2. Pierre Cartier, *Les arrangements d'hyperplanes*, Séminaire Bourbaki 1980/81.
3. Marston Conder, *On the group of Rubik's 'Magic' Cube*, preprint.
4. J. H. Conway, E. R. Berlekamp, and R. K. Guy, *Winning Ways*, Academic Press, 1981.
5. P. Diaconis, R. L. Graham, W. M. Kantor, *The Mathematics of Perfect Shuffles*, in preparation.
6. Marshall Hall, *Group Theory*, Macmillan, 1968.
7. T. R. Keane and H. J. Kamack, *The Rubik Tesseract*, preprint.
8. B. Jackson (a. k. a. 3DJ), *A Cube Dictionary*, preprint.
9. B. Jackson and J. Buhler, *So you want to solve the Magic Cube?*, preprint.
10. R. Levenston and D. E. Taylor, *The theorem of Margraff on primitive permutations groups which contain a cycle*, Bull. Aust. Math. Soc. v. 15 (1976), p. 125-128.
11. J. Nourse, *The Simple Solution to Rubik's Cube*, Bantam Books, 1981.
12. Oystein Ore, *The Theory of Monomial Groups*, Trans. Amer. Math. Soc., v. 51 (1942), p. 15-64.
13. C. A. Rowley, *The Group of the Hungarian Magic Cube*, preprint.
14. Claude Shannon, *A Rubric on Rubik's Cube*, preprint.
15. David Singmaster, *Notes on Rubik's Magic Cube*, Enslow Publishers, 1981.
16. David Singmaster, *Magic Graphs and Magic Polyhedra*, preprint.
17. David Singmaster and Alexander Fry, *Handbook of Cubik Math*, Enslow Publishers, 1982.

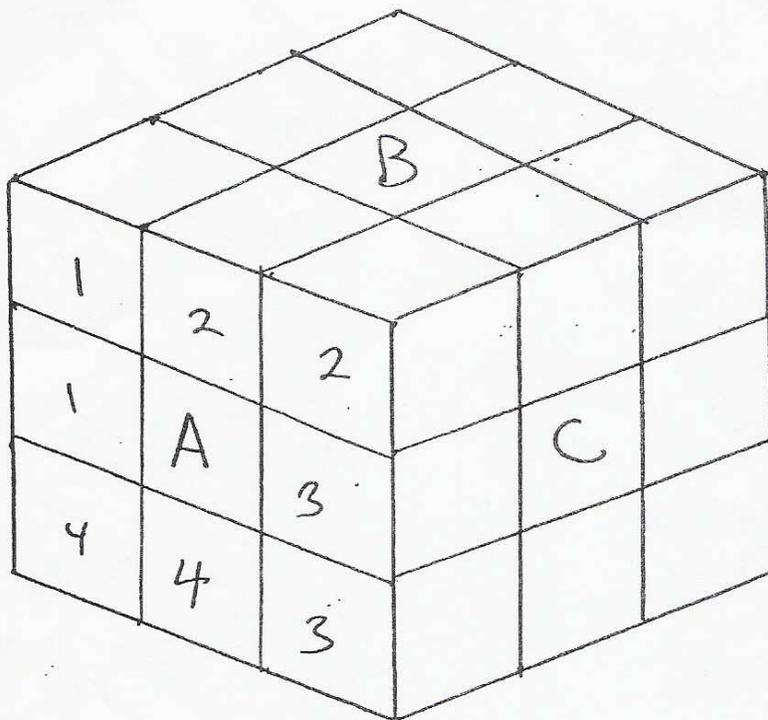
18. John Thompson, Rational functions associated to presentations of finite groups, *J. Algebra* 71 (1981), p. 481-489.
19. T. Zaslavsky, Facing up to arrangements: face-count formulas for partitions of space by hyperplanes, *Memoirs Amer. Math. Soc.* 154 (1975).

Some additional references that will be added:

Wielandt's book

an article by W. Kantor in *J. Algebra* 1969 p. 471 on "Jordan groups" (= primitive permutation groups with subgroups that fix a set point-wise and act transitively on the complement)

DIAGRAM 1



Let A^+ (resp. A^-) denote a 90° clockwise (resp. counterclockwise) turn of the face A in the diagram; similarly for B and C.
 Let $[x,y] = xyx^{-1}y^{-1}$ denote the usual commutator.

MASTER PROCESS: $M = A^- [B^+, C^-] [A^+, C^+]$.

We follow our conventions of reading from right to left. In the more usual (in the cube literature) left to right notation of Singmaster (with $A = F =$ front, $B = U =$ up, $C = R =$ right) this process is

$$M = R^- F^- R F R U^- R^- U F^- .$$

In the corner configuration group $A_3 \sim S_8$ the process M gives an element (f,s) where s is the permutation (12) with the numbering of the cubelets given in the diagram and $f: \mathbb{8} \rightarrow A_3$ is a specific "twist" function. The square of M is $(g,1)$ where g is the twist function whose value at corners 1, 2, and 4 is a specific 3-cycle, and whose value at the other corners is the identity. In the edge configuration group $S_2 \sim S_{12}$ the process M gives (f,s) where $s = (1$. The square of M gives $(g,1)$ where g is nontrivial only at edges 1 and 4.