BULL. AUSTRAL. MATH. SOC. 20F05, 20B30
VOL. 29(1984), 73-90.

SOME RESULTS ON QUOTIENTS OF TRIANGLE GROUPS

MARSTON D.E. CONDER

Given positive integers k,l,m, the (k,l,m) triangle group has presentation $\Delta(k,l,m) = \langle X,Y,Z \mid X^k=Y^l=Z^m=XYZ=1 \rangle$. This paper considers finite permutation representations of such groups. In particular it contains descriptions of graphical and computational techniques for handling them, leading to new results on minimal two-element generation of the finite alternating and symmetric groups and the group of Rubik's cube. Applications to the theory of regular maps and automorphisms of surfaces are also discussed.

1. Introduction

Suppose G is a group which can be generated by two elements, say x and y, such that x has order k and y has order l and their product xy has order m. Quite naturally we call (x,y) a (k,l,m)-generating pair for G. In such a case, the group G must be a quotient of the (k,l,m) *triangle group* $\Delta(k,l,m)$, that is, the abstract group with presentation

$$\Delta(k,l,m) = \langle X, Y, Z \mid X^k = Y^l = Z^m = XYZ = 1 \rangle .$$

Received 8 February 1984. The author wishes to warmly thank Graham Higman and Tom Tucker, for their inspiration and guidance, also Dave Teague for his assistance with implementation of the Schreier-Sims algorithm, and the University of Otago (Dunedin, New Zealand) for financial support in the form of a post-doctoral fellowship during 1981.

There is an obvious symmetry in this presentation; hence, for example, if (x,y) is a (k,l,m)-generating pair, then (z,y) is an (m,l,k)-generating pair, and so on. Indeed, $\Delta(k,l,m)$ is isomorphic to $\Delta(r,s,t)$ whenever (r,s,t) is a rearrangement of (k,l,m). Hence we normally assume that $k \leqslant l \leqslant m$.

The triangle groups are discussed in [5], [10] and [12]. We mention some of their important features below.

First, it is known that $\Delta(k,l,m)$ is finite precisely when $\frac{1}{k} + \frac{1}{l} + \frac{1}{m} > 1$. In that case the triangle groups are as follows:

$\Delta(1,m,m) \cong C_m$, the cyclic group of order m,

$\Delta(2,2,m) \cong D_m$, the dihedral group of order $2m$,

$\Delta(2,3,3) \cong A_4$, the tetrahedral group (of order 12),

$\Delta(2,3,4) \cong \Sigma_4$, the octahedral group (of order 24),

$\Delta(2,3,5) \cong A_5$, the icosahedral group (of order 60).

If $\frac{1}{k} + \frac{1}{l} + \frac{1}{m} = 1$, namely in the cases of $\Delta(2,3,6)$, $\Delta(2,4,4)$ and $\Delta(3,3,3)$, then the group is infinite but soluble: its commutator subgroup is a free Abelian group on two generators, and the associated factor-commutator group is cyclic of order m.

In this paper our interest centres on insoluble permutation groups, and therefore we consider mainly cases where $\frac{1}{k} + \frac{1}{l} + \frac{1}{m} < 1$. Each such triangle group is not just infinite and insoluble, but in fact *SQ-universal* (*cf.* [9]); that is, every countable group occurs as a subgroup of some quotient of $\Delta(k,l,m)$. In particular, these triangle groups are 'enormously large', possessing a wealth of interesting finite factor groups.

Suppose once again that the group G has a (k,l,m)-generating pair, say (x,y), and suppose further that G is a quotient of no triangle group $\Delta(r,s,t)$ with $\frac{1}{r} + \frac{1}{s} + \frac{1}{t} > \frac{1}{k} + \frac{1}{l} + \frac{1}{m}$. Then we shall say (x,y) is a *minimal generating pair* for G. In this sense, minimal means that the orders of the elements x, y and xy are as small as possible (subject to the condition that any two of these elements generate the group). Our definition is not quite the same as that adopted by McKay and Young

https://doi.org/10.1017/S0004972700001738 Published online by Cambridge University Press

(*cf.* [8]), because of the applications which we discuss shortly, however in many cases the two definitions give generating pairs which correspond to the same triangle group!

We can obviously rank the triangle groups $\Delta(k,l,m)$ in terms of descending value of the expression $\frac{1}{k} + \frac{1}{l} + \frac{1}{m}$. First come the finite and soluble ones, and these are followed by

$\Delta(2,3,7)$

$\Delta(2,3,8)$

$\Delta(2,4,5)$

$\Delta(2,3,9)$

$\Delta(2,3,10)$

$\Delta(2,3,11)$

$\Delta(2,3,12)$, $\Delta(2,4,6)$ and $\Delta(3,3,4)$

$\Delta(2,3,13)$

and so on.

To find a minimal generating pair for a given finite group G, if indeed G is a 2-generator group, one may search down this list for the first triangle group which possesses G amongst its quotients. This is seldom an easy task! There are, however, several means of assistance, particularly in cases where G has a known faithful permutation representation. We outline some of these techniques in Section 2.

In the special case where one generator has order two, the quotients of the triangle groups have particular significance to the study of *regular maps* on surfaces (*cf.* [1], [5]). A finite group G is representable as the group of sense-preserving automorphisms of a regular map having l edges incident to each of its vertices and m edges bounding each of its faces, if and only if G is a quotient of $\Delta(2,l,m)$. When this happens, the genus g of the map (and of the associated orientable surface containing the map) is given by

$$2 - 2g = |G|\left(\frac{4-(l-2)(m-2)}{2lm}\right),$$

that is,

https://doi.org/10.1017/S0004972700001738 Published online by Cambridge University Press

$$g = 1 + \frac{1}{2}|G|\left(1 - \left(\frac{1}{2} + \frac{1}{l} + \frac{1}{m}\right)\right) .$$

One consequence of the latter formula is that any minimal $(2,l,m)$-generating pair will correspond to a regular map of smallest possible genus having the given group of sense-preserving automorphisms.

More generally, every triangle group is a *Fuchsian group*, and therefore a discrete subgroup of $PSL(2,\mathbb{R})$, the group of conformal homeomorphisms of the upper-half complex plane. It follows that any finite quotient G of $\Delta(k,l,m)$ is representable as the group of orientation-preserving automorphisms of a compact Riemann surface, whose genus g is given by

$$2 - 2g = |G|\left(2 - \left(1 - \frac{1}{k}\right) - \left(1 - \frac{1}{l}\right) - \left(1 - \frac{1}{m}\right)\right) ,$$

that is,

$$g = 1 + \frac{1}{2}|G|\left(1 - \left(\frac{1}{k} + \frac{1}{l} + \frac{1}{m}\right)\right) ,$$

being a consequence of the Riemann-Hurwitz equation (*cf.* [10]).

Following Tucker [12], we may define the *strong symmetric genus* $\sigma^0(G)$ of a finite group G to be the smallest genus of all such surfaces on which G acts as a group of orientation-preserving automorphisms. It is evident from the above formula that any minimal generating pair for G (if one exists) will provide an upper bound for $\sigma^0(G)$. But in fact Tucker proves much more than this - from his work we glean the following:

If G is a finite group with $\sigma^0(G) > 1$, then $|G| \leqslant 84(\sigma^0(G) - 1)$, and moreover, if $|G| > 12(\sigma^0(G) - 1)$ then G is a quotient of at least one triangle group $\Delta(k,l,m)$ with $\frac{1}{6} < \frac{1}{k} + \frac{1}{l} + \frac{1}{m} < 1$, and $\sigma^0(G)$ is correspondingly determined by the largest achievable value of $\frac{1}{k} + \frac{1}{l} + \frac{1}{m}$. In other words, if G has a minimal (k,l,m)-generating pair such that $\frac{1}{6} < \frac{1}{k} + \frac{1}{l} + \frac{1}{m} < 1$, then $\sigma^0(G)$ must equal

$$1 + \frac{1}{2}|G|\left(1 - \left(\frac{1}{k} + \frac{1}{l} + \frac{1}{m}\right)\right) .$$

We have been able to use this fact to determine the strong symmetric genus of each of the finite alternating and symmetric groups. Details are

https://doi.org/10.1017/S0004972700001738 Published online by Cambridge University Press

given in Section 3.

Consideration of orientation-reversing automorphisms of surfaces leads naturally to Tucker's definition of the (more general) *symmetric genus* of a group (*cf.* [12]). In a separate paper we announce the symmetric genus of the symmetric group Σ_n for all positive integers n.

Finally we mention the following application of minimal generating pairs. Given a finite group G, the smallest genus of all surfaces into which can be embedded the Cayley graph corresponding to some presentation for G is called simply the *genus* of the group (*cf.* [13]). Typically, the genus of a particular finite group is not easy to calculate, even if all its presentations are known. We can say, however, that if G is a quotient of the triangle group $\Delta(k,l,m)$, then at least one Cayley graph for G embeds into a surface of genus

$$1 + \frac{1}{2}|G|\left(1 - \left(\frac{1}{k} + \frac{1}{l} + \frac{1}{m}\right)\right) .$$

This result (*cf.* [12] or [13]) means that we can use minimal generating pairs in order to obtain a reasonable upper bound on the genus of some groups.

2. Machinery

In this section we describe some of the tools we have found useful in obtaining results about two-element generation of certain permutation groups.

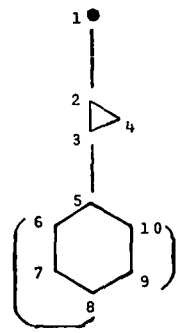
Most of our work hinges on the construction and analysis of *coset diagrams* for the appropriate triangle groups. Formally (*cf.* [5]), a coset diagram corresponding to a subgroup H of finite index in a finitely-generated group G, is a directed, edge-coloured graph, whose vertices are the (right) cosets of H in G and whose edges are defined as follows: we take a specific set of generators for G, and for each generator x and each vertex Hg, draw an edge of colour C_x from Hg to Hgx. This is of course a generalization of the Cayley colour graph corresponding to a (finite) presentation for G.

Now it is a well-known fact that every transitive permutation representation of a group corresponds naturally to one on the cosets of a subgroup (namely, the subgroup of elements fixing a particular point). Consequently any transitive permutation representation of a finitely-

generated group on a finite space can be depicted graphically by a coset diagram. Indeed, this can be done even without specific knowledge of the associated subgroup - one needs only the permutations induced by specific generators on the points of the space.

In the case of a triangle group $\Delta(2,l,m)$, we may simplify the coset diagram by removing some of its edges, directions and even the colours. If (x,y) is a $(2,l,m)$-generating pair, then we may represent the cycles of y by polygons (whose vertices are permuted, say, anticlockwise) or by heavy dots (indicating fixed points), and then draw lines to indicate the action of x (interchanging the points at the ends of each line).

For example, the triangle group $\Delta(2,6,14)$ has a transitive permutation representation on the space $\{1,2,3,4,5,6,7,8,9,10\}$, with the usual generators x and y acting as $(1,2)(3,5)(6,8)(9,10)$ and $(2,3,4)(5,6,7,8,9,10)$ respectively. The associated coset diagram may be drawn simply as below:



Once we have constructed such a diagram, it is quite easy to read off the permutation action of any particular word in the group generators, using a form of 'diagram chasing'. For example, in the above representation one can find that the element $xy^{-1}xy$ acts as $(1,2,3,10,7,9,5)(4,6,8)$, by following the 'path' corresponding to the word $xy^{-1}xy$ from each vertex in turn. This is much quicker than dealing with the permutations alone.

For a particular group, the construction and analysis of coset diagrams on a chosen number of vertices can be carried out by hand. This of course requires care and imagination. Alternatively, the work can be performed by a suitably programmed machine. In particular, there are a

couple of algorithms available which are ideally suited to each task. We outline them briefly:

The Lowindex algorithm

Given a presentation for a group G with a small (finite) number of generators and defining relations, it is possible to determine all subgroups - or just a representative from each conjugacy class of subgroups - of index less than some specified integer n. This algorithm (described in detail in [6], for example) first sets up a partial coset table, indicating the action of each generator of G on each numbered coset, in a way similar to the well-known Todd-Coxeter algorithm. Once a certain pre-set number of cosets have been defined, a branching process is begun. At each level of this process, the algorithm forces coincidences between pairs of cosets - equivalent to producing new generators for a subgroup - and updates the coset table accordingly. If the table becomes 'complete', with fewer than n cosets defined, then a new subgroup has been determined; otherwise the process jumps to the next level and examines all possible branches (new coincidences) there. A test can be included to check whether any current branch will lead only to conjugates of subgroups already found, in which case that branch is abandoned; otherwise the algorithm continues and outputs any new subgroups. Termination occurs when all possible branches (at the first level) have been exhausted.

From the complete coset table corresponding to any outputted subgroup, say H, it is a simple matter to obtain explicit generators for the subgroup H as words in the generators for G, together with those permutations induced by the generators of G on the cosets of H. Using the latter permutations, one can then draw the associated coset diagram (which, incidentally, will be the same for any subgroup from the same conjugacy class). In particular, this algorithm gives us a systematic method of enumeration of *all* coset diagrams for G on fewer than n vertices.

The Schreier-Sims algorithm

Given a small (finite) number of permutations on a small (finite) space, it is possible to determine the order of the group they generate. The algorithm we refer to was conceived by Charles Sims, and based on

Schreier's theorem for subgroup generators. It produces not only the order of the generated permutation group, but also a *base* and a *strong generating set* (as explained in [7] for example).

Roughly speaking, the base and strong generating set give an indication of the (multiple) transitivity and/or imprimitivity of the group generated by the given permutations, and are therefore helpful in the task of recognising the group itself.

For example, if we have a coset diagram corresponding to a subgroup H of low index in a finitely-presented group G (such as a triangle group), we can read off the permutations induced by the generators of G on the cosets of H, and attempt to identify the group they generate. Of course the latter group will be a finite quotient of G, corresponding to the normal subgroup $\bigcap_{g \in G} g^{-1}Hg$ of G (often called the *core* of H in G).

Consequently the Schreier-Sims algorithm can be used (together with the Lowindex algorithm) to help us determine those finite quotients of G which have transitive permutation representations of small degree.

The author of this paper has successfully implemented PASCAL versions of these algorithms (and others) on a microcomputer, but would like to point out that more sophisticated (and probably more efficient) packages are available - notably John Cannon's CAYLEY group system at the University of Sydney.

Finally we mention a result which has proved most useful in deciding that certain finite groups are *not* quotients of a given triangle group $\Delta(2,l,m)$. By putting a strong restriction on the possible cycle structures of the permutations induced by the group generators, it tells us that some coset diagrams cannot be constructed, or, if they can, then they must take a certain form.

THEOREM. *Suppose a and b are permutations of N points such that a has λ_u cycles of length u (for $1 \leqslant u \leqslant l$) and b has μ_v cycles of length v (for $1 \leqslant v \leqslant m$) and their product ab is an involution having k transpositions and $N-2k$ fixed points. If a and b generate a transitive group on these N points, then there exists a non-negative integer p such that*

https://doi.org/10.1017/S0004972700001738 Published online by Cambridge University Press

$$k = 2p - 2 + \sum_{1 \leqslant u \leqslant l} \lambda_u + \sum_{1 \leqslant v \leqslant m} \mu_v .$$

This is actually a special case of Theorem 2 from [10], for $N = \sum_{1 \leqslant u \leqslant l} \lambda_u u = \sum_{1 \leqslant v \leqslant m} \mu_v v$ and so on. The following proof, however, does not require the strength of the Riemann-Hurwitz equation.

Proof. (Due to Graham Higman.) Write ab as $t_1 t_2 \dots t_k$, the product of k disjoint transpositions, and let $s = \sum_{1 \leqslant u \leqslant l} \lambda_u$. We can arrange the transpositions such that $a^{-1} t_1 t_2 \dots t_i$ has $s - i$ cycles, for $1 \leqslant i \leqslant j$, where j is some integer less than both s and k, as postmultiplication by a transposition always increases or decreases the number of cycles by one. Indeed, let j be the largest integer for which this is possible. We claim that $j = s - 1$.

To see this, consider any orbit Λ of the permutation $a^{-1} t_1 t_2 \dots t_j$. This must be a union of orbits of a, and must also be fixed by each of the remaining transpositions $t_{j+1}, \dots, t_k$ (otherwise we can choose t_{j+1} such that $a^{-1} t_1 t_2 \dots t_j t_{j+1}$ has one cycle fewer than $a^{-1} t_1 t_2 \dots t_j$). Hence $\Lambda a = \Lambda$ and also $\Lambda b = \Lambda a^{-1} ab = \Lambda a^{-1} t_1 t_2 \dots t_k = \Lambda t_{j+1} \dots t_k = \Lambda$ so that Λ is an orbit for the group generated by a and b. By transitivity, Λ must have size N, hence $a^{-1} t_1 t_2 \dots t_j$ is a single N-cycle. In particular, $s - j = 1$.

Now when we postmultiply $a^{-1} t_1 t_2 \dots t_j$ by the remaining $k - s + 1$ transpositions $t_{j+1}, \dots, t_k$ in turn, some (say q) will increase the number of cycles by one, and others (say p) will decrease the number by one, so that $b = a^{-1} t_1 t_2 \dots t_k$ will have $1 + q - p$ cycles.

But this means

$$1 + q - p = \sum_{1 \leqslant v \leqslant m} \mu_v ,$$

and as we know on the other hand

$$q + p = k - s + 1 ,$$

we obtain (by subtraction)

https://doi.org/10.1017/S0004972700001738 Published online by Cambridge University Press

$$1 - 2p = \sum_{1 \leqslant v \leqslant m} \mu_v - k + \sum_{1 \leqslant u \leqslant l} \lambda_u - 1 ,$$

from which the desired equality follows.

COROLLARY. *If* $\Delta(2,3,7)$ *has a transitive permutation representation of degree* N *, then*

$$\left[\frac{N}{2}\right] + 2\left[\frac{N}{3}\right] + 6\left[\frac{N}{7}\right] \geqslant 2N - 2 ,$$

and in fact there exist non-negative integers p, e, f, g *satisfying*

$$N = 84(p - 1) + 21e + 28f + 36g .$$

Proof. Take a and b such that $a^3 = b^7 = (ab)^2 = 1$, the group generated by a and b acting transitively on a set of N points. For the first part, notice

$$\sum_{1 \leqslant u \leqslant l} \lambda_u = \lambda_1 + \lambda_3 \geqslant \left(N - 3\left[\frac{N}{3}\right]\right) + \left[\frac{N}{3}\right] = N - 2\left[\frac{N}{3}\right]$$

and

$$\sum_{1 \leqslant v \leqslant m} \mu_v = \mu_1 + \mu_7 \geqslant \left(N - 7\left[\frac{N}{7}\right]\right) + \left[\frac{N}{7}\right] = N - 6\left[\frac{N}{7}\right]$$

while

$$k \leqslant \left[\frac{N}{2}\right] .$$

For the second part, let e, f and g denote the numbers of fixed points of ab, a and b respectively. The theorem tells us there is a non-negative integer p such that

$$\frac{1}{2}(N - e) = 2p - 2 + f + \frac{1}{3}(N - f) + g + \frac{1}{7}(N - g) ,$$

therefore

$$21(N - e) = 84p - 84 + 42f + 14(N - f) + 42g + 6(N - g) ,$$

which simplifies to the given formula. (These results were cited without proof in [2].)

https://doi.org/10.1017/S0004972700001738 Published online by Cambridge University Press

3. Alternating and symmetric groups

Some years ago Graham Higman discovered that for all sufficiently large integers n the alternating group A_n can be generated by elements x, y satisfying $x^2 = y^3 = (xy)^7 = 1$. He proved this by using a method for construction of transitive permutation representations of the triangle group $\Delta(2, 3, 7)$ of arbitrarily high degree, together with a clever argument based on a theorem of Jordan. The work was never properly published; however Professor Higman very kindly allowed the author of this paper to use it as the basis for a doctoral thesis; and consequently refinements and extensions of the theorem have appeared in print.

In [2] we showed how all but 64 of the finite alternating groups are quotients of $\Delta(2, 3, 7)$. Incidentally, there is an error in the statement of the theorem in Section 5 of [2] : the integer 139 is missing from the list (a) of those n which fail to satisfy the inequality $\left[\frac{n}{2}\right] + 2\left[\frac{n}{3}\right] + 6\left[\frac{n}{7}\right] \geqslant 2n - 2$. (In particular there is no coset diagram for $\Delta(2, 3, 7)$ on 139 vertices; hence A_{139} is not a Hurwitz group.)

We adapted Higman's methods in a sequel [3] to achieve the following generalization:

THEOREM. *Given any integer m greater than 6, all but finitely many alternating groups A_n occur as quotients of the triangle group $\Delta(2, 3, m)$. Moreover, if m is even, then all but finitely many symmetric groups Σ_n occur as well.*

An immediate consequence of these results is that we need look only at $\Delta(2, 3, 7)$ and $\Delta(2, 3, 8)$ to obtain minimal generating pairs for almost all alternating and symmetric groups.

In fact Σ_n has a $(2, 3, 8)$-generating pair for all integers n except for those in the range $1 \leqslant n \leqslant 17$ and for $n = 22, 23, 26$ and 29. We have proved this using the methods of [2] and [3], and our results match those obtained by machine computation. The exceptional cases are as follows:

(a) $n = 1, 2, 3, 4$: here Σ_n is a quotient of $\Delta(2, 3, 8)$, but of course Σ_n has no element of order 8;

https://doi.org/10.1017/S0004972700001738 Published online by Cambridge University Press

(b) n = 5, 7, 11, 23 : here $\Delta(2, 3, 8)$ has no transitive permutation representation on n points;

(c) n = 6, 8, 9, 10, 12, 13, 14, 15, 16, 17, 22, 26, 29 : here elements x, y satisfying $x^2 = y^3 = (xy)^8 = 1$ in Σ_n always generate a *proper*, often imprimitive subgroup of Σ_n.

Our computations have indicated also that A_n has a (2, 3, 8)-generating pair except when $3 \leqslant n \leqslant 9$ or n = 11, 12, 14, 15, 18, 19, 20, 21, 23, 24, 31, 35, 47. In particular, of the 64 alternating groups which are not quotients of $\Delta(2, 3, 7)$, all but 17 have a *minimal* (2, 3, 8)-generating pair.

It turns out that these remaining cases, together with the cases of the 21 exceptional symmetric groups above, can be dealt with almost entirely by examining the quotients of the triangle groups

$\Delta(2, 4, 5)$

$\Delta(2, 3, 9)$

$\Delta(2, 3, 10)$

$\Delta(2, 3, 11)$

$\Delta(2, 3, 12)$ and $\Delta(2, 4, 6)$.

We summarize the results in the following theorem.

THEOREM. *Except for the cases listed below, every alternating group A_n has a minimal (2, 3, 7)-generating pair and every symmetric group Σ_n has a minimal (2, 3, 8)-generating pair.*

The exceptional values of n are:

(a) 25, 27, 30, 32, 33, 34, 38, 39, 40, 41, 44, 46, 48, 53, 54, 55, 59, 60, 61, 62, 67, 68, 69, 74, 75, 76, 82, 83, 89, 90, 95, 97, 103, 104, 110, 111, 118, 125, 131, 139, 146, 167, for here both A_n and Σ_n have minimal (2, 3, 8)-generating pairs;

(b) 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 22, 23, 24, 26, 29, 31, 47, for in these cases minimal generating pairs are obtainable for A_n and Σ_n from the triangle groups $\Delta(k, l, m)$ as given in the following list:

https://doi.org/10.1017/S0004972700001738 Published online by Cambridge University Press

n	A_n	Σ_n
1	$\Delta(1, 1, 1)$	$\Delta(1, 1, 1)$
2	$\Delta(1, 1, 1)$	$\Delta(1, 2, 2)$
3	$\Delta(1, 3, 3)$	$\Delta(2, 2, 3)$
4	$\Delta(2, 3, 3)$	$\Delta(2, 3, 4)$
5	$\Delta(2, 3, 5)$	$\Delta(2, 4, 5)$
6	$\Delta(2, 4, 5)$	$\Delta(2, 5, 6)$
7	$\Delta(2, 4, 7)$	$\Delta(2, 3, 10)$
8	$\Delta(2, 5, 7)$	$\Delta(2, 4, 7)$
9	$\Delta(2, 4, 6)$	$\Delta(2, 4, 6)$
10	$\Delta(2, 3, 8)$	$\Delta(2, 3, 10)$
11	$\Delta(2, 3, 11)$	$\Delta(2, 4, 5)$
12	$\Delta(2, 3, 11)$	$\Delta(2, 3, 12)$
13	$\Delta(2, 3, 8)$	$\Delta(2, 3, 12)$
14	$\Delta(2, 3, 12)$	$\Delta(2, 4, 6)$
15	$\Delta(2, 3, 7)$	$\Delta(2, 4, 5)$
16	$\Delta(2, 3, 8)$	$\Delta(2, 4, 5)$
17	$\Delta(2, 3, 8)$	$\Delta(2, 4, 6)$
18	$\Delta(2, 3, 9)$	$\Delta(2, 3, 8)$
19	$\Delta(2, 3, 9)$	$\Delta(2, 3, 8)$
20	$\Delta(2, 4, 5)$	$\Delta(2, 3, 8)$
22	$\Delta(2, 3, 7)$	$\Delta(2, 3, 10)$
23	$\Delta(2, 3, 11)$	$\Delta(2, 3, 10)$
24	$\Delta(2, 3, 10)$	$\Delta(2, 3, 8)$
26	$\Delta(2, 3, 8)$	$\Delta(2, 4, 5)$
29	$\Delta(2, 3, 7)$	$\Delta(2, 3, 12)$
31	$\Delta(2, 4, 5)$	$\Delta(2, 3, 8)$
47	$\Delta(2, 4, 5)$	$\Delta(2, 3, 8)$

https://doi.org/10.1017/S0004972700001738 Published online by Cambridge University Press

COROLLARY. *For all but 69 positive integers n, the strong symmetric genus of A_n is $\frac{n!}{168} + 1$ and that of Σ_n is $\frac{n!}{48} + 1$.*

The exceptional cases are given in the theorem, and for each n we can easily compute $\sigma^\circ(A_n)$ and $\sigma^\circ(\Sigma_n)$ using the earlier formula.

One should perhaps also notice that every A_n and Σ_n has a minimal $(2, l, m)$-generating pair for some l and m, that is, one of the minimal generators is always an involution. Hence in particular the theorem gives (indirectly) the regular maps of minimum genera with A_n and/or Σ_n as automorphism group.

4. The group of Rubik's cube

By the group of Rubik's cube we mean the group of 43, 252, 003, 274, 489, 856, 000 patterns achievable by natural manipulations of a standard six-coloured Rubik's cube. The structure of this group is quite well-known (*cf.* [11] for example). In particular, it may be viewed as an intransitive group of permutations on the 48 coloured labels of the edge and corner pieces of the cube, acting (imprimitively) on each of two orbits of size 24. One of these orbits corresponds naturally to the labels of the edge pieces: there are 12 blocks each of size 2, and the group acts on these as a split extension of an elementary Abelian 2-group of order 2^{11} by the symmetric group Σ_{12}. We will call the latter group the *edges group*. On the other orbit, with 8 blocks each of size 3, the cube group acts as a split extension of an elementary Abelian 3-group of order 3^7 by the symmetric group Σ_8. This group (of order $3^7.8!$) can be known as the *corners group*. The group of the cube is a subdirect product of these two imprimitive groups, that is, a subgroup of index two in the direct product of the edges group and the corners group. As such, it has order $\frac{1}{2}(2^{11}.12!\ 3^7.8!)$, which is the number stated above.

This view was adopted in [4], where we showed that the group of the cube can be generated by elements x and y satisfying $x^2 = y^4 = (xy)^{1260} = 1$, with the orders 2 and 4 of the generators being 'minimal' in a certain sense. Well, we can now state that the group of Rubik's cube has a (2, 4, 12)-generating pair, which is minimal in the sense described earlier (*cf.* Introduction).

https://doi.org/10.1017/S0004972700001738 Published online by Cambridge University Press

The proof of these claims goes as follows.

First we label the coloured stickers on the edge and corner pieces as 1, 2, ..., 48 in any way such that the blocks of imprimitivity are of the form:

Corner blocks $\{m,\ m+8,\ m+16\}$ for $1 \leqslant m \leqslant 8$,

Edge blocks $\{m,\ m+12\}$ for $25 \leqslant m \leqslant 36$,

with the added condition that the corner pieces are labelled according to a consistent (say clockwise) orientation.

Now consider the following pair of permutations:

x = (1, 20)(2, 5)(3, 14)(4, 9)(6, 19)(10, 13)(11, 22)(12, 17)
(18, 21)(25, 26)(27, 31)(28, 30)(29,35)(32, 33)(37, 38)
(39, 43)(40, 42)(41, 47)(44, 45);

y = (1, 2, 3, 4)(5, 6, 7, 8)(9, 10, 11, 12)(13, 14, 15, 16)
(17, 18, 19, 20)(21, 22, 23, 24)(26, 27, 28, 29)(30, 42)
(31, 32, 43, 44)(33, 34, 45, 46)(35, 48, 47, 36)(38, 39, 40, 41).

One may observe immediately that these permutations satisfy the relations $x^2 = y^4 = 1$, and a little further investigation yields $(xy)^{12} = 1$. (Indeed, the reader may wish to draw the associated coset diagrams in order to verify these and other details.)

Also it is not difficult to show that both x and y are achievable by natural manipulations of the cube. For example, one could dismantle the cube and reassemble it into the state prescribed by the action of the appropriate permutation, and then use one's favourite algorithm to return the cube to its original state! In particular x and y may be taken as elements of the group of Rubik's cube.

The subgroup generated by x and y is transitive on $\{1, 2, \ldots, 24\}$ and also on $\{25, 26, \ldots, 48\}$, and of course acts imprimitively on each of these two orbits.

The commutator $xyxy^{-1}$ is the permutation (1, 11, 22, 20, 8)
(2, 18, 10)(3, 14, 12, 24, 17)(4, 16, 9, 19, 6)(5, 13, 21)
(25, 44, 45, 26, 29, 35)(27, 46, 31, 42, 48, 40)(28, 39, 34, 43, 30, 36)
(32, 33, 38, 41, 47, 37).

Now $(xyxy^{-1})^6$ acts as a 5-cycle on the corner blocks, fixing all

https://doi.org/10.1017/S0004972700001738 Published online by Cambridge University Press

the other labels, so the group $\langle x, y \rangle$ generated by x and y must act primitively on the corner blocks, and indeed it acts as Σ_8, by a theorem of Jordan (*cf.* Theorem 13.10 of [14]). On the other hand, $(xyxy^{-1})^5$ 'twists' the corner blocks $\{2, 10, 18\}$ and $\{5, 13, 21\}$ in opposite directions, and multiple transitivity of $\langle x, y \rangle$ gives all such twists of corner blocks. Consequently $\langle x, y \rangle$ acts in exactly the same way as the corners group, inducing $3^7.8!$ permutations on the labels 1, 2, ..., 24.

Similarly $(xyxyxy^{-1}xy^{-1})^{15}$ acts as a 7-cycle on the edge blocks, fixing all the other labels, so $\langle x, y \rangle$ acts as Σ_{12} on the edge blocks; and as $(y^2(xyxyxy^2xy^{-1})^{28})^2$ 'flips' the two edge blocks $\{27, 39\}$ and $\{29, 41\}$, we obtain all possible rearrangements of the edge labels. Hence $\langle x, y \rangle$ acts in the same way as the edges group on the orbit $\{25, 26, \ldots, 48\}$.

It now follows easily that $\langle x, y \rangle$ is a subdirect product of the edges group and corners group, of order $\frac{1}{2}(3^7.8! \; 2^{11}.12!)$ since both x and y induce *even* permutations on the 20 blocks of imprimitivity. That is, x and y generate the group of Rubik's cube.

We now proceed to justify our claim that this generating pair (x, y) is minimal.

First, as we pointed out in [4], the symmetric group Σ_8 cannot be generated by elements u, v which satisfy either $u^2 = v^3 = 1$ or $u^3 = v^3 = 1$. Well, neither can it have a (k, l, m)-generating pair for $(k, l, m) = (2, 4, 6), (2, 4, 9), (2, 4, 11), (2, 5, 5), (2, 5, 6)$ nor $(2, 5, 7)$. This leaves just the possibilities $(2, 4, 7), (2, 4, 8)$ and $(2, 4, 10)$, if we seek a (k, l, m)-generating pair with

$$\frac{1}{k} + \frac{1}{l} + \frac{1}{m} > \frac{1}{2} + \frac{1}{4} + \frac{1}{12} = \frac{5}{6} \; .$$

The symmetric group Σ_{12} has no $(2, 4, 7)$-generating pair; it can, however, be generated by elements u, v satisfying $u^2 = v^4 = (uv)^m = 1$ where $m = 8$ or 10. Also Σ_8 can be generated in this way. But it is impossible to generate the corners group (of order $3^7.8!$) by such elements, for neither $\Delta(2, 4, 8)$ nor $\Delta(2, 4, 10)$ has a transitive permutation representation of degree 24 with 8 blocks of imprimitivity (each of size 3).

Hence $(2, 4, 12)$ is the best possible.

https://doi.org/10.1017/S0004972700001738 Published online by Cambridge University Press

In fact the pair (x,y) of permutations given above leads to a sort of 'minimal presentation' for the group of Rubik's cube. These elements also satisfy the relations

$$\begin{aligned} 1 &= (xy^2)^8 \\ &= (xyxy^2)^{12} \\ &= (xyxy^{-1})^{30} \\ &= (xyxyxy^2)^{36} \\ &= (xyxyxy^{-1})^{36} \\ &= (xyxy^2xy^2)^{60} \\ &= (xyxy^2xy^{-1})^{24} \end{aligned}$$

and so forth.

The resulting presentation (obtained by continuing until enough relations are found in order to *define* the group) is minimal in the sense that if we write x, y, xy, xy^2, $xyxy^2$ (and so on) as a sequence of words of increasing length, then the order of each word is as small as possible subject to the condition that x and y generate the group and subject to the relations corresponding to the orders of all earlier words in the sequence. We do not, however, know how many of these relations must be included in order to obtain a defining presentation for the group. That seems to be an open problem.

References

[1] N. L. Biggs and A. T. White, *Permutation Groups and Combinatorial Structures*, London Math. Soc. Lecture Note Series, No. 33 (Cambridge University Press, 1979).

[2] M. D. E. Conder, "Generators for alternating and symmetric groups", *J. London Math. Soc. (2)*, 22 (1980), 75-86.

[3] M. D. E. Conder, "More on generators for alternating and symmetric groups", *Quart. J. Math. Oxford Ser. 2*, 32 (1981), 137-163.

[4] M. D. E. Conder, "On the group of Rubik's 'magic' cube", *Bull. Inst. Math. Appl.*, 17 (1981), 241-243.

[5] H. S. M. Coxeter and W. O. J. Moser, *Generators and Relations for Discrete Groups*, 4th ed. (Springer-Verlag, 1980).

[6] A. Dietze and M. Schaps, "Determining subgroups of a given finite index in a finitely-presented group", *Canadian J. Math.* 26 (1974), 769-782.

[7] J. S. Leon, "On an algorithm for finding a base and strong generating set for a group given by generating permutations", *Math. Comp.* 35 (1980), 941-974.

[8] J. McKay and K-c. Young, "The non Abelian groups G, $|G| < 10^6$ - minimal generating pairs", *Math. Comp.* 33 (1979), 812-814 (plus microfiche supplement).

[9] P. M. Neumann, "The SQ-universality of some finitely presented groups", *J. Austral. Math. Soc.* 16 (1973), 1-6.

[10] D. Singerman, "Subgroups of Fuchsian groups and finite permutation groups", *Bull. London Math. Soc.* 2 (1970), 319-323.

[11] D. Singmaster, *Notes on Rubik's 'Magic Cube'* (Polytechnic of the South Bank, London, 1980).

[12] T. W. Tucker, "Finite groups acting on surfaces and the genus of a group", *J. Combin. Theory Ser. B*, 34 (1983), 82-98.

[13] A. T. White, "On the genus of a group", *Trans. Amer. Math. Soc.* 173 (1972), 203-214.

[14] H. Wielandt, *Finite Permutation Groups* (Academic Press, 1964).

Department of Mathematics and Statistics,
University of Auckland,
Private Bag,
Auckland,
New Zealand.