Jñānābha, Vol. 14, 1984

A THEOREM OF G. A. MILLER ON THE ORDER OF THE PRODUCT OF TWO PERMUTATIONS. I

J. L. Brenner

10 Phillips Road

Palo Alto, California 94303, U. S. A.

and

R. C. Lyndon

Department of Mathematics, University of Michigan,

Ann Arbor, Michigan 48109, U S. A.

(Received: December 21, 1982)

ABSTRACT

We consider permutations A and B of a finite set of d elments such that A, B, and $C=AB$ have respective orders $a, b, c \geqslant 2$. G. A. Miller showed in 1900 that for $2 \leqslant a \leqslant b \leqslant c$, such permutations always exist with $d=c$, $c+1$, or $c+2$ according to the parities of a, b, c. If $s=max\ [s(a),\ s(b)\ \ s(c)]$, where $s(a)$ is the sum of the primary factors of a, then according to parities, $d \geqslant s$, $s+1$, $s+2$. We find an infinite class of triples a, b, c (with $a=2$) for which d must be larger than $s+2$ However, the cases $a=3$, 4, 5, 6, as well as other large families of cases, support the conjecture that, for $a \geqslant 3$, one can always choose $d \leqslant s+2$.

Introduction

We consider the following much studied question. Given three

The second author gratefully ackonwledges partial support from the National Science Foundation.

Part II of this work is scheduled to appear in *Indian J. Math.*, and Part **III** in *Pure Appl. Math. Sci.*

integers $a, b, c \geqslant 2$, what are the finite permutation groups G generated by two elements A and B of orders a and b, whose product $C=AB$ has order c ? G. A. Miller [25] refers to a remark of Burnside [11, *p.* 15]: "A relation of the form $S_p=S_qS_r$ between three operations of the group will not in general involve any necessary relation between the order of S_p and the orders of S_q and S_r."

This question has arisen in connection with finite simple groups. For example, when is the alternating group (or the symmetric group) of degree d generated by elements A and B, of orders a and b, such that $C=AB$ has order c ? (See Macbeath [23] for the case $a=2$, $b=3$, $c > 7$ and also Conder [14, 15] who treats the case $a=2$, $b=3$, $c \geqslant 7$.)

The same question arises in connection with a well known theorem, first conjectured by Fenchel [19], that every Fuchsian group G is virtually torsion free, that is, G contains a subgroup of finite index with no nontrivial element of finite order. Fenchel observed that the proof reduces easily to the case that G is a triangle group, $G= < A, B: A^a = B^b = (AB)^c = 1 >$, where it must be shown that G has a finite image in which the images of A, B, and $C=AB$ retain the orders a, b, and c. This case was proved by Fox [21] in 1952.

However, this result for triangle groups is contained in what appears to be the first paper on this subject, by G. A. Miller [25] in 1900, where it is shown that, for all $a, b, c \geqslant 2$, there exist permutations A and B of a finite set Ω such that A, B, and $C=AB$ have orders a, b, and c and that Ω has $d=m$, $m+1$, or $m+2$ elements, for m the maximum of a, b, c. Miller's proof, as well as the later proof of Fox, explicitly constructs permutations A and B with the required properties. Later proofs using matrices were given by Feuer [20] and by Mennicke [24]. In a second paper, Miller [26] showed that, for infinitely many d, A and B could be chosen as permutations of a set

Ω of d elements, such that the group G generated by A and B is transitive on Ω, thus obtaining infinitely many nonisomorphic groups G.

A proof of Fenchel's theorem by entirely different means appears to have been given first by Selberg [30]. It uses the well known fact that a Fuchsian group G contains only finitely many conjugacy classes of elements of finite order, and also the fact that G, viewed as a finitely generated matrix group over a field, is residually finite. From this it follows that there is a map from G onto a finite group in which the image of each element of finite order has the same order as the original; the kernel of this map is then a torsion free subgroup of finite index.

A third approach lies in the observation that if a Fuchsian group G acts on the hyperbolic plane in the usual manner, with a fundamental region Δ, then the existence of a torsion free subgroup S (hence a surface group) of index d in G is equivalent to the existence of a union Σ of d translates $g\Delta$ of Δ such that Σ is a fundamental region for a surface group S. This approach has been followed by Edmonds, Ewing, and Kulkarni [16, 17, 18] who show that, under the obvious necessary conditions, a closed orientable surface can always be tessellated into d polygons, each with r sides and with prescribed vertex angles $\alpha_1,\ldots\alpha_r$. (Here the closure of a face is not required to be simply connected.) From this they deduce the following. Let G be a Fuchsian group with elliptic generators of orders $m_1,\ldots,m_r \geqslant 2$, and let m be the least common multiple of the m_i. In the special case that G has no parabolic generators, that m is even, and that $\Sigma m/m_i$ is odd, define $\delta=2$, and otherwise take $\delta=1$. Then G contains a torsion free subgroup of index $d \geqslant 1$ if and only if d is a multiple of $d_0=\delta m$. (They note that these subgroups need not be normal, and that the determination of the torsion-free normal subgroups of specified index appears to involve deep number theoretic questions.)

They obtain an interpretation of their results in terms of permutation groups. Given $m_1,\dots,m_r \geqslant 2$, where $r \geqslant 3$ and δ and d_0 are as before, the symmetric group of degree d_0 contains permutations $A_1,\dots,A_r$ such that each A_i is a product of d_0/m_i disjoint cycles of length m_i, that $A_1,\dots,A_r = 1$, and that the subgroup generated by $A_1,\dots,A_r$ is transitive.

In Part I of this paper we give a version of Miller's proof of his first result, in a pictorial (or geometric) form that we believe to be more perspicuous. This method, which has been much used elsewhere [4, 5, 6, 7, 13, 14, 15, 32, 33, 34, 35] lies in constructing of a "coset graph" for G, relative to the generators A and B.

In Parts II and III we present some results and a conjecture regarding the smallest possible degree $d=d\,(a,b,c)$ of a subgroup G of the symmetric group S_d that is generated by elements A and B such that $A,B,$ and AB have orders a, b, and c. It is easy to see that if the largest of a, b, c is prime power, then Miller's lower bound for d is best possible. But for general a, b, c one can do better. The least possible degree of a permutation of order $m \geqslant 2$ is $s(m)$, the sum of the factors in the primary decomposition of m as a product of powers of distinct primes. Clearly $d=d\,(a, b, c) \geqslant s=s(a, b, c)$, the maximum of $s(a)$, $s(b)$, $s(c)$; the same considerations as in Miller's argument show that, according to conditions of parity, one must have $d \geqslant s$, $d \geqslant s+1$, or $d \geqslant s+2$. One is tempted to conjecture that $d \leqslant s+2$, that is, that in all cases d is one of s, $s+1$, or $s+2$.

Suppose by symmetry that $s(a) \leqslant s(c) \leqslant s(b)$. We show that the extreme value $d = Max\,[a, b, c] + 2$ given by Miller is attained only if $b=2^r$ for some $r \geqslant 1$ and either $a=b=c$, or else a and c are both odd and $a, c < b$. Contrary to the tempting conjecture above, we show that when $a=2$ there are infinitely many values of b such that, for some c (which must in fact be a prime), $d > s+2$, but that these values of b have density 0. However, if a is 3,4 , 5, or 6, we can prove that $d \leqslant s+2$. This together with many other special cases, leads us to believe that $d \leqslant s+2$ whenever $a > 2$.

Although the pictorial interpretation used in Part I has guided our thinking in Parts II and III, we have not used it there.

PART I. MILLER'S THEOREM.

Let A and B be permutations of a finite set Ω. We define a 2-complex $K=K(A,B)$ as follows. The vertices (points, 0-cells)of K are the elements p of Ω.The 2-cells consist of edges joining distinct points p and q if and only if q is one of pA, pA^{-1}, pB, pB^{-1}. If $(p_1,\ldots,p_m)$, $m \geqslant 2$, is a nontrivial cycle of A [or of B], we adjoin as a 2-cell an *A-face* [or *B-face*], that is an m-gonal disc, oriented so that its boundary is the m-gon with vertices $p_1,\ldots,p_m$ in cyclic order. (If $m=2$, this choice of orientation is arbitrary.)

Suppose conversely that a 2-complex K is given, together with a division of its 2-cells into A-faces and B-faces such that two A-faces [or two B-faces] are always disjoint, and with a specification of an orientation of each face. Then it is clear how to recover permutations A and B of the set Ω of vertices of K such that $K=K(A,B)$. We shall construct our permutations A and B in this way, by piecing together the complex $K=K(A,B)$.

In the complexes K considered below, all A-faces will have a vertices, and all B-faces will have b vertices, except there may occur one *A-digon* with two vertices if a is even, or one *B-digon* if b is even. Thus an A-face will be understood to have a vertices, and a B-face b vertices, unless otherwise noted. The complex K will always be connected. Moreover (after possible deletion of a single A–face) K will be simply connected, and embedded in the plane in such a way that all A–faces are oriented clockwise and all B–faces counterclockwise. In all cases $C=AB$ (which we interpret as A followed by B) will consist of a single cycle of length c, together with a possible fixed point (cycle of length 1) or, if c is even, a possible transposition (cycle of length 2).

We begin with a family of complexes K_n, for $n \geqslant 0$. For given a, b, and n, the complex K_n consists of n A–faces $A_1, \ldots, A_n$ and $n+1$ B–faces $B_0, \ldots, B_n$. Each A_i has one vertex in common with B_{i-1} and one with B_i, and the faces are otherwise disjoint. This is illustrated in Figure 0.

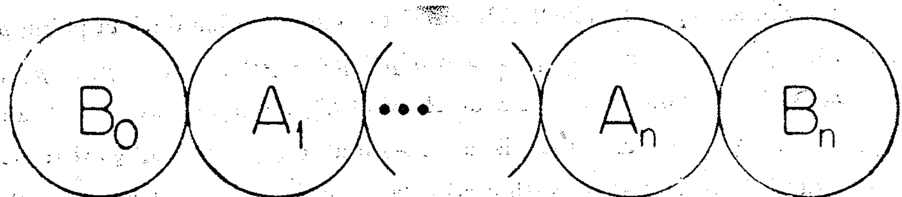

Figure 0.

Inspection shows that K_n has $c_n=b+nd$ vertices, where $d=a+b-2$, and that $C=AB$ consists of a single cycle of length $c=c_n$.

Except for K_0, in which A is trivial, each K_n exhibits A and B of orders a and b, with $C=AB$ of order c_n. For given a and b, we reach the remaining values $c \geqq b$ by attaching additional A–faces to B_0 and B_n, together possibly with one further A–digon or B–digon. The manner of attaching these additional faces is described in the following lemmas.

LEMMA 1. *Let P and Q be two cyclic permutations having in common only an odd number of vertices, which occur consecutively in P and Q. Then PQ is a single cycle.*

Proof. We may suppose that $P=(p_1,\ldots,p_k, r_1,\ldots,r_m)$ and $Q=(p_1,\ldots,p_k, s_1,\ldots,s_n)$ where k is odd. Then inspection shows that $PQ=(p_1, p_3,\ldots,p_k, r_1,\ldots,r_m, p_2, p_4,\ldots,p_{k-1}, s_1,\ldots,s_n)$.

This is illustrated in Figure 1. □

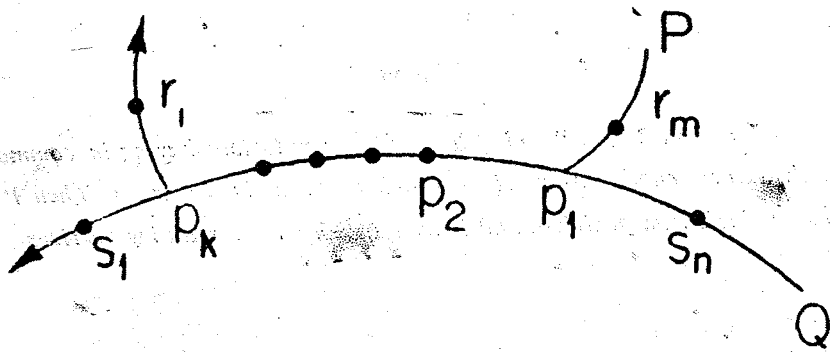

Figure 1.

Lemma 2. *Let P and Q be cyclic permutations having in common only an even number of vertices, which occur as in Figure 2.Then PQ has a single fixed point, and is transitive on ther emaining vertices.*

Proof. If $P=(p_2, p_1, p_3, p_4,\ldots,p_k, r_1,\ldots,r_m)$, for k even, $Q=(p_1, p_2,\ldots,p_k, s_1,\ldots,s_n)$, then

$PQ=(p_2)\,(p_1, p_4, p_6,\ldots,p_k, r_1,\ldots,r_m, p_3, p_5,\ldots,p_{k-1}\; s_1,\ldots,s_n)$. □

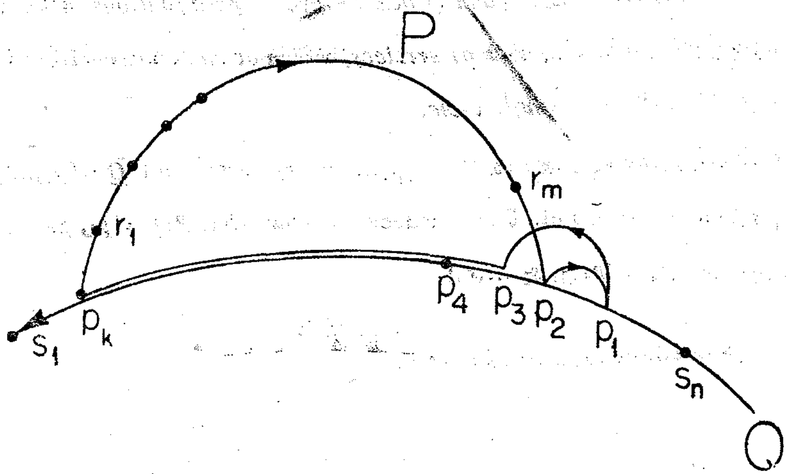

Figure 2.

Lemma 3. *Let P and Q be cyclic permutations having in common only an even number of vertices, which occur as in Figure 3. Then PQ has a single transposition, and is transitive on the remaining vertices.*

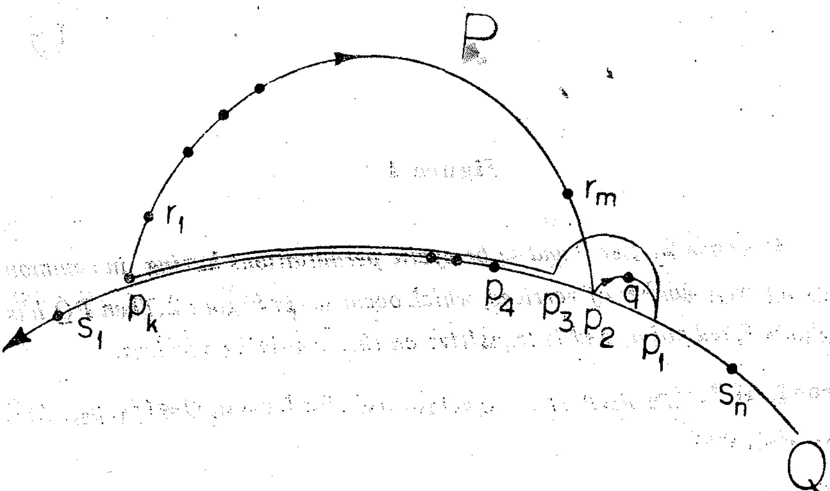

Figure 3.

Proof. If $P=(p_2, q, p_1, p_3, p_4, \dots, p_k, r_1, \dots, r_m)$, k even, and

$Q=(p_1, \dots, p_k, s_1, \dots, s_n)$, then

$PQ=(p_2, q)\ (p_1, p_4, p_6, \dots, p_k, r_1, \dots, r_m, p_3, p_5, \dots, p_{k-1}\ s_1, \dots, s_n)$. □

We need one more rather special lemma.

Lemma 4. Suppose $m > 0$ is even and k is odd; suppose further that either $k = 1$ and $2 + m \leqslant c$ or that $2 + m + k \leqslant c$. Then there exist permutations A and B of a set Ω of c elements such that (i) A has order $a = mk$ and (ii) B and $C = AB$ have order c.

Proof. Let $\Omega = \{1, 2, \dots, c\}$. If $B = (1\ 2 \dots c)$ and $A_1 = (1\ 3)\ (2\ 4\ 5 \dots m + 2)$, then $C_1 = A_1B = (1\ 4\ 6 \dots m + 2, 3, 2, 5, 7, \dots m + 1, m + 3\ m + 4 \dots c)$. If $k = 1$, we take $A = A_1$ whence $C = C_1$. If $k > 1$ we take $A = A_1\ A_2$ where $A_2 = (m+3\ m+4 \dots m+k+2)$. By Lemma 1, $C = A_2C_1$ is a cycle of length c. □

We shall prove the following version of Miller's theorem.

Theorem 5. *Let a, b, c be integers, $2 \leqslant a \leqslant b \leqslant c$. Then there exist permutations A and B of a set Ω of $d \leqslant c + 2$ elements such that A, B, and $C=AB$ have orders a, b, and c. The set Ω can be taken with $d=c$ elements and hence with C a single cycle except in the following case,*

(1) *If $a = b = c = 6$, then the smallest value d_0 of $d = |\Omega|$ is $d_0 = 7 = c + 1$.*

(2) *If $a = b = c = 2^r$, $r > 1$, then the smallest value d_0 of d is $d_0 = c + 2$.*

(3) *If $a = 2^r$, $r > 1$, and $b = c = a + 1$, then $d_0 = c + 1$.*

(4) *If a, b are odd and c even, then, in certain cases (in fact, if and only if c is a power of 2), $d_0 = c + 2$.*

(5) *If a, c are odd and* $b = c - 1$, *then in certain cases (for example, if b is a power of 2)* $d_0 = c + 1$.

Proof. We first treat the case $b = c$. If $d = c$, then B and C must be single cycles of the same length $b = c$, whence B and C have the same parity and A must be an even permutation. If A is odd, we take A to be a single cycle of length a, together with fixed points, and attach this cycle to a c-cycle B in the manner of Lemma 1 to obtain a c-cycle $C = AB$.

We may now suppose that a is even, $a = 2^r k$, $r \geqslant 1$. k odd. Suppose first that $a = b = c = 6$. Now one of A, B, C, say A, must be an even permutation. Since A must contain one cycle of even length, it must contain two such, and A must also contain a cycle of order dividible by 3. This implies that $d \geqslant 7$. The value $d = 7$ can be realized by taking $\Omega = \{1, 2, \ldots, 6, p\}$, $A = (1\ 3)\ (2\ 4)\ (6\ 5\ p)$, $B = (1, 2\ \ldots\ 6)\ (p)$, whence $C = (1\ 4\ 3\ 2\ 5\ p)\ (6)$.

If $k = 3$ and $r \geqslant 2$, then $k + 2\,(k{-}1) \leqslant 2^r\ (k{-}1)$ whence $2 + 2^r + k \leqslant 2^r k = a \leqslant b = c$, and Lemma 4 applies to give $d = c$. If $k \geqslant 5$, then $k + 2 \leqslant 2\ (k - 1) \leqslant 2^r(k - 1)$, whence again $2 + 2^r + k \leqslant b = c$ and Lemma 4 again gives $d = c$.

Suppose now that $k = 1$, that is, $a = 2^r$. If $a + 2 \leqslant b = c$, then Lemma 4 again applies to give $d = c$. The cases remain that $b = c = a$ and that $b = c = a + 1$. If $a = b = c = 2^r$, then one of A, B, C must be an even permutation, hence must contain a 2^r–cycle together with another cycle of even length. This implies that $d \geqslant c+2$. To realize this value we take $\Omega = \{1, 2, \ldots, c, p, q\}$ with $A = (p\ 4\ q\ 3\ 5\ 6\ \ldots\ c)\ (1)\ (2)$, $B = (1\ 2\ \ldots\ c)\ (p)\ (q)$, whence

$$C = (1\ 2\ 3\ 6\ 8\ \ldots\ c\ p\ 5\ 7\ \ldots\ c{-}1)\ (q\ 4).$$

If $a = 2^r$ and $b = c = a + 1$, then B and C are even permutations, whence A must be even, with a cycle of length 2^r and another cycle of even length. This implies that $d \geqslant a + 2 = c + 1$. To realize this value we take $\Omega = \{1, 2, \ldots, c, p\}$ with $A = (1\ p)\ (3\ 2\ 4\ 5 \ldots c)$, $B = (1\ 2\ \ldots\ c)\ (p)$, whence $C = (1\ p\ 2\ 5\ 7\ \ldots\ c\ 4\ 6\ \ldots\ c - 1)\ (3)$.

This completes the proof of the theorem in the case $b = c$.

We assume henceforth that $2 \leqslant a \leqslant b < c$. We turn next to the exceptional cases (4) and (5).

Let a, b be odd and c even. Then A and B are even permutations whence C must be even. Thus C cannot be a single cycle of even length c. If c is a power of 2, this implies that $d \geqslant c + 2$. We establish below that the value $d = c + 2$ can always be attained when a, b are odd and c is even.

Let a, c be odd and b even. Then B must be even and cannot consist of a single cycle of length b. If b is a power of 2, then $d \geqslant b + 2$, which, in case $c = b + 1$, implies that $d \geqslant c + 1$. To show that, for a odd, b even, and $c = b + 1$, the value $d = c + 1$ can be realized, we take A to consist of a single a–cycle (together with fixed points). We attach a b–cycle B_1 to A along a–2 consecutive points; by Lemma 1, $C_1 = AB_1$ is a single cycle of length $b+2 = c+1$. We now attach a 2–cycle B_2 to A along its two remaining points, and take $B = B_1B_2$. Then $C = AB = AB_1B_2$ consists of a single c–cycle together with one fixed point.

To complete the proof of the theorem we suppose a and b given, and start with the complexes K_n, which yield for c all values $c = c_n$. We proceed, according to the parities of a and b, by attaching new faces to the K_n to obtain complexes K yielding the remaining values of $c \geqslant b$. We have already disposed of the case $b = c$, and of case (5) (where a is odd, b is even, and $c = b + 1$). Thus we may suppose that $c > b$. In case (4), we must show that K has $d = c + 2$ vertices. In cases (1), (2), (3) we must show that K has $d = c$ vertices.

Case I: *a odd.* We shall attach h A–faces, for some h to be specified later, each to B_0 or to B_n at a single vertex, and we attach a further A–face P to B_0, as in Lemma 1, along an arc containing some odd number k of vertices. We require that

(1) $1 \leqslant k \leqslant k^* = a - 2$, k *odd.*

To be able to attach h–faces at a single point, in the worst case where $n = 0$ and $B_0 = B_n$, and where $k = k^*$, we must have $h + k^* \leqslant b$. Thus we must require that

(2) $0 \leqslant h \leqslant h^* = \delta + 2$ *where* $\delta = b - a \geqslant 0$.

By Lemma 1, C is transitive, whence $c = |\,\Omega\,| = c_n + \Delta$, where

(3) $\Delta = h\,(a - 1) + (a - k)$, *even.*

All values of h, k satisfying (1) and (2) are possible, giving all values of Δ in the range

(4) $h\,(a - 1) + 2 \leqslant \Delta \leqslant (h + 1)\,(a - 1)$, Δ even.

The largest value of Δ is $\Delta^* = (h^* + 1)\,(a - 1) = (\delta + 3)\,(a - 1)$, and $\nabla = \Delta^* - d = (\delta+3)\,(a-1) - 2(a-1) = (\delta+1)\,(a-1) - \delta > \delta\,(a - 1) - \delta = \delta\,(a - 2) \geqslant 0$. Thus, as h and k range over the admissible values, $c = c_n + \Delta$ assumes all values such that

(5) $c_n + 2 \leqslant c \leqslant c_{n+1} + 2$, $c \equiv c_n$ (*modulo* 2).

Subcase I.1: *b even.* Attaching a single B–digon at a single vertex to an A–face increases Δ by $+1$. Thus we obtain all values $c > b + 1$ without the restriction that $c \equiv c_n$ (modulo 2). The case $c = b + l$ is case (5), already treated.

Subcase I.2: *b odd*. Here d is even. Since $c_0 = b$ is odd, all c_n are odd, whence the values of $c = c_n + \Delta$ for even Δ are precisely the odd numbers c for $c \geqslant b$. To obtain the even numbers c, for $c > b$, we modify the constrution, now attaching P as in Lemma 3. Conditions (1) and (2) are now replaced by

(1′) $2 \leqslant k \leqslant k^* = a - 1$, *k even*,

(2′) $0 \leqslant h \leqslant h^* = \delta + 1$.

By Lemma 3, C now consists of a 2–cycle together with a disjoint cycle of length $c = d - 2$. Thus $c = c_n + \Delta$ where

(3′) $\Delta = h\,(a - 1) + (a - k) - 2$, Δ *odd*.

We obtain all Δ in the range

(4′) $h\,(a - 1) - 1 \leqslant \Delta \leqslant (h + 1)\,(a - 1) - 3$, Δ *odd*.

For $n \geqslant 0$, since c_n is odd, this yields all $c = c_n + \Delta$ for

(5′) $c_n - 1 \leqslant c \leqslant c_{n+1} - 3$, *c even*.

This gives all even values of c for $c \geqslant b$.

Case II: *a even*. We attach new A–faces as in Case I. We now have

(1″) $1 \leqslant k \leqslant k^* = a - 1$, *odd*,

(2″) $0 \leqslant h \leqslant h^* = \delta + 1$, (3″) $\Delta = h\,(a-1) + (a-k)$, $\Delta \equiv h+1$ (*modulo* 2),

(4″) $h\,(a-1) + 1 \leqslant \Delta \leqslant (h+1)\,(a-1)$, $\Delta \equiv h+1$ (*mod*) 2).

Now $\nabla = (h^*+1)\,(a-1) - d = (\delta+2)\,(a-1) - 2\,(a-1) - \delta$
$= \delta\,(a-1) - \delta = \delta\,(a-2) \geqslant 0$.

Subcase II.1: *b even.* Attaching a single B–digon at a single vertex increases Δ by $+1$, thus removing the restriction $\Delta \equiv h+1$ and yielding all $c \geqslant b+1$.

Subcase II. 2: *b odd.* This case, with $c > b$, is treated as above, now attaching a single A–digon to B_0 or B_n at a single vertex. There is room to do this except possibly in the case that $n = 0$, hence $B_0 = B_n$, and that $h + k = b$. In this case we must have $k = k^*$ and $h = h^*$, hence $\Delta = h^*\,(a-1) + (a-k^*) = (\delta+1)\,(a-1) + 1$. The missing value, $c = c_0 + \Delta + 1$, can be obtained from some c_n, for $n \geqslant 1$, provided that $c \geqslant c_1$, that is, provided that $\Delta + 1 \geqslant d$, or that $(\delta + 1)\,(a - 1) + 2 \geqslant 2\,(a - 1) + \delta$. This condition is equivalent to $(\delta - 1)\,(a - 1) \geqslant \delta - 2$, which holds since $(\delta - 1)\,(a - 1) \geqslant \delta - 1$.

This campletes the proof of Miller's theorem.

REFERENCES

[1] G. Boccara, Cycles comme produit de deux permutations de classes donnèes, *Discrete Math.* **38** (1982), 129–142.

[2] J. L. Brenner, Problem E 1118, *Amer. Math. Monthly* **62** (1955), 43.

[3] J. L. Brenner, Covering theorems for finite nonabelian simple groups. IX. How the square of a class with two nontrivial orbits in S_M covers A_n, *Ars Combinatoria* **4** (1977), 151–176.

[4] J. L. Brenner and R. C. Lyndon, Nonparabolic subgroups of the modular group, *J. Algebra* **77** (1982), 311–322.

[5] J. L. Brenner and R. C. Lyndon, Permutations and cubic graphs, *Pacific J. Math.*

104 (1983), 285–315

[6] J. L. Brenner and R. C. Lyndon, Maximal nonparabolic subgroups of the modular group. *Math. Ann.* **263** (1983) 1–11.

[7] J. L. Brenner and R. C. Lyndon, The orbits of the product of two permutations, *European J. Combinatorics* **4** (1983) (To appear).

[8] J. L. Brenner and R. C. Lyndon, Infinite Eulerian graphs, *Discrete Math.* **46** (1983) (To appear)

[9] J. L. Brenner, M. Randall and J. Riddell, Covering theorems for finite nonabelian simple groups. I, *Colloq. Math.* **32** (1974), 39–48.

[10] J. L. Brenner and J. Riddell, Noncanonical factorization of a permutation, *Amer. Math. Monthly* **84** (1977), 39–40,

[11] W. Burnside, Theory of Groups of Finite Order. Dover, New York, 1955.

[12] M. Cohn and A. Lempel, Cycle decomposition by disjoint transpositions. *J. Combinatorial Theory* **A13** (1972), 83–89.

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

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

[15] R. Cori, Un code pour les graphes planaires et ses applications, *Astérisque, Soc. Math. France* **27** (1975)

[16] A. L. Edmonds, J. H. Ewing and R. S. Kulkarni, Torsion free subgroups of Fuchsian groups and tessellations of surfaces, *Bull. Amer. Math. Soc.* **6** (1982), 456–458.

[17] A. L. Edmonds, J. H. Ewing and R. S. Kulkarni, Regular tessellations of surfaces and $(p, q, 2)$ triangle groups. *Ann. of Math.*

[18] A. L. Edmonds, J. H. Ewing and R. S. Kulkarni, Torsion free subgroups of Fuchsian groups and tessellations of surfaces. *Inventiones Math.* (To appear).

[19] W. Fenchel, Bemarkingen om endelige grupper af abbildungsklasser, *Mat. Tidssk.* **B** (1950), 90–95.

[20] R. D. Feuer, Torsion–free subgroups of triangle groups. *Proc. Amer. Math. Soc.* **30** (1971), 235–240.

[21] R. H. Fox, On Fenchel's conjecture about *F*-groups. *Mat. Tidssk.* **B** (1952), 61–65.

[22] R. S. Kulkarni, Normal subgroups of fuchsian groups. (To appear).

[23] A. M. Macbeath, *Fuchsian Groups*, Queen's College, Dundee, 1961.

[24] J. L. Mennicke. Eine Bemerkung über Fuchssche Gruppen, *Inventiones Math.* **2** (1967), 301–305; corrigendum, *ibid.* **6** (1968), 106.

[25] G. A. Miller, On the product of two substitutions. *Amer. J. Math.* **22** (1900), 185–190.

[26] G. A. Miller, Groups defined by the orders of two generators and the order of their product, *Amer. J. Math.* 24 (1902), 96–100.

[27] G. Moran, Chords in a circle and linear algebra over GF (2). Preprint.

[28] H. E. Richert, Über Zerfällungen in ungleiche Primzahlen. *Math. Zeitschr.* **52** (1950), 342–343.

[29] J. Riddell, Partitions into distinct small primes. *Acta Arithmetica* **41** (1982), 71–84.

[30] A. Selberg, On discontinuous groups in higher dimensional symmetric spaces, *Colloq. Function Theory*, Bombay. 1960. 147–164.

[31] W. Sierpiński, *Elementary Theory of Numbers*, Warsaw, 1964. (Page 144, Theorem 12).

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

[33] W. W. Stothers, Subgroups of the modular group, *Proc. Cambridge Philos. Soc.* **75** (1974), 139–153.

[34] W. W. Stothers, Subgroups of the (2, 3, 7) triangle group, *Manuscripta Math.* **20** (1977), 323–334.

[35] W. W. Stothers, Diagrams associated with subgroups of Fuchsian groups, *Glasgow Math. J.* **20** (1979), 103–114.

[36] R. G. Burns and D. Solitar, Indices of torsion-free subgroups of Fuchsian groups. (To appear).