A Search for Analogues of the Mathieu Groups

By E. T. Parker and Paul J. Nikolai

I. Introduction. This paper describes a search for simple groups of a certain type using the UNIVAC Scientific Computer, Model 1103A.

Except for alternating and symmetric groups, the Mathieu groups of degrees 11, 12, 23, and 24 are the only known finite, quadruply transitive groups. These four groups, together with the Mathieu group of degree 22, are the only known abstract finite simple groups belonging to no known infinite system. (\[1\]) see “Mathieu groups” in index). The curious properties of these groups provide considerable motivation for a large-scale search by digital computer for analogous groups.

It can be noted that the degrees \( p = 11 \) and \( p = 23 \) are primes of the form \( p = 2q + 1 \), with \( q \) also a prime. The analogues to be considered are groups \( G \) with the following properties:

1) \( G \) is a transitive permutation group of degree \( p = 2q + 1 \), \( p \) and \( q \) primes;
2) \( G \) is a simple group, and not merely the group of order \( p \);
3) \( G \) is a proper subgroup of the alternating group of degree \( p \). Such groups have been studied by G. A. Miller [2] and first footnote thereof for earlier papers, and K. D. Fryer [3]. In these papers it is reported that no \( G \) exists for degrees 47, 59, and 83. Even for these fairly low degrees the computations are of such length that details were not published. For a fixed degree \( p = 2q + 1 \) the groups to be examined are relatively few. For each group tested, it was possible to construct a pair of generators in a form admirably suited to digital computation; this form is probably not in previous literature.

The program was run for all degrees \( p = 2q + 1 \), \( p \) and \( q \) primes, \( 23 < p < 1823 \). The values of \( p \) are 23, 47, 59, 83, 107, 167, 179, 227, 263, 347, 359, 383, 467, 479, 503, 563, 587, 719, 839, 863, 887, 983, 1019, 1187, 1283, 1307, 1319, 1367, 1439, 1487, 1523, 1619, and 1823. No \( G \) exists for any of these degrees, with the sole exception of the Mathieu group of degree 23. Degree 23, for which the facts are well known, yielded an invaluable check on the validity of the program. Inclusion of the next three degrees provided a check both on the program and on the tedious computations of earlier investigators.

In Section II are the arguments which lead to description of a pair of generators of a group to be tested, and to the criteria by which such a group may be rejected as the alternating group. In Section III the code for the UNIVAC Scientific Computer is described, with comments on running the program. In Section IV the results are summarized.

II. Mathematical arguments. As noted in the Introduction, the groups \( G \) under consideration have properties:

1) \( G \) is a transitive permutation group of degree \( p = 2q + 1 \geq 23 \), \( p \) and \( q \) primes;
2) \( G \) is simple, and not of order \( p \);
3) \( G \) is a proper subgroup of the alternating group of degree \( p \).

Received 27 September 1957. The program was written and run during the summer of 1956, while the authors were employed by Remington Rand UNIVAC, Division of Sperry Rand Corporation, St. Paul, Minnesota. The authors wish to express their thanks to Remington Rand UNIVAC for providing time on the UNIVAC Scientific Computer, model 1103A.
The alternating group of degree $p$ is disregarded as uninteresting in this search. Any group containing odd permutations has a normal subgroup of index 2, hence is composite if of order greater than 2. The group $G$ is required to be simple (property 2), and of order $> p > 23$ (properties 1 and 2). The motivation for demanding property 3 is established.

The group $G$, being transitive of degree $p$ (property 1), is of order divisible by $p$ ([4] p. 170, Corollary). Thus $G$ has a Sylow subgroup $P$ belonging to the prime $p$. This subgroup $P$ is of order $p$ only, hence cyclic. Were $P$ in the center of its normalizer in $G$, then the commutator subgroup $K$ of $G$ would be of order prime to $p$ ([4] p. 327, Theorem II). A transitive group $G$ of prime degree is primitive. The subgroup $K$ is a normal subgroup of $G$, hence either the identity or transitive on the $p$ letters ([4] p. 196, Theorem X). If $K$ is the identity, then $G$ is abelian and in turn of order $p$, which is ruled out by property 2. On the other hand, $K$ transitive on the $p$ letters implies that $K$ is of order divisible by $p$, conflicting with the assumption that $P$ is in the center of its normalizer. The only alternative is that $G$ has an element $b$ such that $b^{-1}Pb = P$, but $b^{-1}ab \neq a$, where $a$ is some non-identical element of $P$.

It is expedient for computational purposes to identify the $p$ letters permuted by $G$ with the integers reduced modulo $p$. Without loss of generality a generator $a$ of $P$ may be chosen as $x \rightarrow x + 1$ (mod $p$). Being in the holomorph of $P$, $b$ is of the form $x \rightarrow tx$ (mod $p$), $t$ a fixed integer $\neq 0$ or 1 (mod $p$). Since $p - 1 = 2q$, $g$ an odd prime, $b$ is of order $q$, 2, or 2q. The element $b$ fixes only the zero residue class and permutes the remaining $2q$ letters in cycles of equal length. Hence the element $b$ of even order is an odd permutation, excluded by property 3. Accordingly $b$ is of order $q$. As the holomorph of $P$ has a unique subgroup of index 2, $b$ may be chosen as $x \rightarrow r^2x$ (mod $p$), $r$ a primitive root of $p$. Thus chosen, $b$ consists of two cycles, one permuting the quadratic residues of $p$, the other the quadratic non-residues.

The symmetric group of degree $2q + 1$, $q$ an odd prime, has its Sylow $q$-subgroups of order $q^2$, generated by two disjoint cycles of length $q$. If $G$ had as an element a single cycle of length $q$, then $G$ would be $p - q + 1 = q + 2$ times transitive ([4] p. 207, Theorem 1); noting that a transitive group of prime degree is primitive. In turn $G$ would contain the alternating group [5]. Thus $G$ has its Sylow $q$-subgroups of order $q$ only; let $Q$ denote the Sylow $q$-subgroup generated by $b$.

Assume that $Q$ is in the center of its normalizer. Then $K$ is of prime order to $q$. The normalizer in $G$ of $P$ is of order $pq$; hence the normalizer in $K$ of $P$ is of order only $p$. The second derived group of $G$ is then of order prime to $p$, thus the identity alone. The group $G$ must then be solvable ([4] p. 56), in conflict with property 2. Thus $G$ has an element $c$ such that $c^{-1}Qc = Q$, $c^{-1}bc \neq b$; then $c^{-1}bc = b^w$, $w \neq 0$, 1 (mod $q$). Two possibilities arise: either $c$ fixes set-wise the two cycles of $b$, or $c$ maps each cycle into the other. The search may with no real loss be restricted to minimal extensions of $\{a, b\}$, so that $c$ may be assumed to be of prime order. (Should a $G$ be found, it would then be of interest to drop the restriction that $c$ be of prime order, repeating the computations with $c'$ normalizing $Q$, $c$ a power of $c'$. This was not done, as no $G$ was found with $c$ of prime order.) Any element $c$ of prime order interchanging the two cycles of $b$ must be of order 2, consisting of $q$ transpositions;
such an element is not in the alternating group. Thus \( c \) may be chosen of prime
order, fixing set-wise the cycles of quadratic residues and quadratic non-residues
constituting \( b \), and transforming the cycles into like powers of themselves. Accord-
ingly \( c \) is of the form, \( (x^2 \rightarrow r x^{2k}) \cdot (-x^2 \rightarrow n x^{2k}) \) (mod \( p \)), where exponent \( k \) is
fixed, \( x \) ranges over all residues (mod \( p \)), \( r \) and \( n \) are a fixed quadratic residue and
non-residue of \( p \); \(-1\) is a quadratic non-residue of \( p \), since \( q \) is odd and in turn
\( p = 2q + 1 = 3 \) (mod 4). The holomorph of the group of order \( q \) has a unique
subgroup of order \( qh \), \( h \) any divisor of \( q - 1 \); thus \( \{b, c\} = \{b, c_1\} \), where \( c_1 \) is any
power of any conjugate of \( c \), provided that \( c \) and \( c_1 \) are of the same order. Thus it is
necessary to consider only those \( c \) of the form \( (x^2 \rightarrow r x^{2k}) \cdot (-x^2 \rightarrow -x^{2k}) \) (mod \( p \)).
This form of the generator \( c \) was referred to in the Introduction. Other mathe-
matically equivalent notations \([1, 3]\) would be very awkward to simulate on a
computer. A further observation reduces essentially to half the number of groups
to be examined. Note that \( y \rightarrow -y \) (mod \( p \)) transforms \( a \) into \( a^{-1} \) and \( \{b, c\} \) into
\( \{b, c^*\} \), where \( c \) and \( c^* \) are respectively \( (x^2 \rightarrow r x^{2k}) \cdot (-x^2 \rightarrow -x^{2k}) \) and
\( (x^2 \rightarrow r^{-1} x^{2k}) \cdot (-x^2 \rightarrow -x^{2k}) \) (mod \( p \)). The powers of 4 include all quadratic
residues of \( p \). Accordingly, for a given \( p \) and exponent \( k \), all groups to be examined
have \( c \) of the form \( (x^2 \rightarrow 4^i x^{2k}) \cdot (-x^2 \rightarrow -x^{2k}) \) (mod \( p \)), \( 0 \leq i \leq (p - 3)/4 \).
For each value of \( i \), the permutation \( c \) belonging to \( i + 1 \) is obtainable by multiply-
ing by 4 (mod \( p \)) the maps of all quadratic residues of \( p \) in the previous permu-
tation.

For each prime divisor \( \lambda \) of \( q - 1 \) it is necessary to select only one value of \( k \)
yielding \( c \) of order \( \lambda \). Thus the number of groups to be examined for a given degree
\( \rho = 2q + 1 \) is \((\rho + 1)/4\) times the number of prime divisors of \( q - 1 \).

For a given \( \rho \) and \( k \), the \( c \) with \( i = 0 \) is of the simple form \( y \rightarrow y^k \) (mod \( p \)),
provided that \( k \) is odd, this condition being easily satisfied. As noted above, \( \rho = 3 \)
(mod 4). Further, \( q = 1 \) or 2 (mod 3), and \( q = 1 \) (mod 3) implies \( \rho = 0 \) (mod 3),
which is impossible for \( \rho \) a prime \( \geq 23 \). Hence \( q = 2 \) (mod 3) so that \( \rho = 2 \) (mod 3).
Thus \( \rho = 11 \) (mod 12). By quadratic reciprocity, \(-3\) is a quadratic non-residue
of \( p \). The multiplicative group of residues prime to \( p \) being cyclic of order \( 2q \), \(-3\) is
a primitive root of \( p \) Thus \( c \) with \( i = 0 \) is \((0 \rightarrow 0) \cdot [(p - 3)^i \rightarrow ((p - 3)^4)^i] \)
(mod \( p \)), \( 1 \leq j \leq p - 1 \). This observation made unnecessary the direct genera-
tion in the computer of large blocks of \( k \)-th powers.

Any of the groups \( \{a, b, c\} \) is generated by \( a \) and \( c \) alone. For \( \{a, c\} \) is transitive
on the \( p \) letters, the normalizer in \( G \) of \( P \) is of order \( \rho g \), and \( P \) is not in the center
of its normalizer in \( \{a, c\} \).

Each group \( \{a, c\} \) is simple ([3] Theorem 4.1), satisfying property 2. Thus
any \( \{a, c\} \) of the type considered is either the alternating group or a \( G \) having the
three properties.

Since \( \rho = 2 \) (mod 3), \( \rho - 2 \) is composite. Thus any group \( \{a, c\} \), with an
element consisting of a single cycle of length a prime \( \pi < \rho \), is the alternating group
of degree \( \rho \). The argument is given above for the special case \( \pi = q \).

The program was designed to construct the permutation \( c \) for each group, then
to decide whether any element \( a^i c \) (\( 1 \leq i \leq \rho - 1 \)) has any power consisting of
a single cycle of odd prime length \( \pi < \rho \). (\( \pi = 2 \) is ignored, since the alternating
group has no element with only one cycle of even length.) Either a group was re-
jected as alternating; or, when testing all $a'c$ failed to show the group alternating, an output of $c$ was provided.

III. Description of the Code for the UNIVAC Scientific Computer. For each prime value $p = 2q + 1$, $23 \leq p \leq 1823$, the value $q - 1$ was factored. Then for each prime divisor $\lambda$ of $q - 1$, an odd integer $k$ was found such that $k^\lambda \equiv 1 \pmod{q}$, $k \neq 1 \pmod{q}$. These $88$ $p$, $k$ pairs together with about 300 program instructions comprised the input.

The routines, with numerical designations, are described below for a given $p$, $k$ pair.

1. Generate and store the quadratic residues of $p$. Generate and store in addresses $y$, $1 \leq y \leq p - 1$, (high-speed magnetic core), the numbers $y^2 \pmod{p}$; store $p$ in address $p$. Addresses 1 to $p$ are thus loaded with $c$ ($i = 0$) for the first group of the block of $(p + 1)/4$ groups for the pair $p$, $k$. A copy of $c$ is also stored on the drum for possible output and for proceeding to the next group (Routine 5). Routine 2 is now entered.

2. Multiply the permutation in addresses 1 to $p$ by the permutation $a: x \rightarrow x + 1 \pmod{p}$. This routine is rapidly accomplished by using the Repeat instruction of UNIVAC Scientific to transmit the contents of address $y$ to address $y - 1$, $2 \leq y \leq p$. The initial contents of address 1 are then placed at address $y$. Addresses 1 to $p$, having been loaded with $a'c$, now contain $a^{i+1}c$, $0 \leq i \leq p - 2$. Proceed to Routine 3.

3. Count and store the lengths of cycles of the permutation stored in addresses 1 to $p$.
   The principal idea of this routine is the following: when an address has been accounted for in a cycle, the contents of this address are marked by a minus sign. Each cycle is traced through its course by proceeding from an address to the address indicated by the contents of the preceding. A sign test indicates the completion of a cycle. The next cycle is then begun at the first address whose constants are positive. The process necessarily terminates with the contents of addresses 1 to $p$ all negative. Routine 4 is entered next.

4. Test the set of cycle lengths to decide whether the group must be alternating.
   This routine makes use of the criterion developed near the end of Section 2. Reformulated for computation, the proposition is: If $a'c$ has a cycle of prime length $\pi < p$, and no other cycle of length divisible by $\pi$, then $\{a, c\}$ is the alternating group. $\pi = 2$ can be ignored, since the alternating group contains no element with only one cycle of even length.

A technique previously used by E. Lehmer ([6] p. 105) was employed to decide whether a given odd number is prime. Consecutive bits of the contents of consecutive addresses were loaded (as part of the program data) with one or zero according as consecutive odd numbers 1, 3, $\cdots$, 1823 are prime or composite. Having an odd number $Z$ to be tested, $1/2 (Z - 1)$ is divided by 36, the number of bits per word. The quotient then indicates the address and the remainder the bit in that address containing the information as to whether $Z$ is prime.

Each cycle length $L_i$ is checked as it is found by Routine 3. If $L_i$ is a prime such that $(p - 1)/2 < L_i < p$, enter alternative B described below. In this case
all other cycle lengths are $< p$, hence indivisible by $p$. If $L_i = p$, enter alternative $A$; the group cannot be rejected on this permutation.

If Routine 3 is completed without the group having been rejected, the cycle lengths are summed. If this sum were not $p$, the machine would stop. This error stop never occurred. Now for any prime cycle length $Z$ among the $L_i$, the product $\prod L_i \not\equiv 0 \pmod{Z^2}$ indicates rejection of the group, and alternative $B$ is entered. If the group is not rejected on any prime cycle length $Z$, enter Alternative $A$.

Alternative $A$: Return to Routine 2 except when all $a'c$, $1 \leq i \leq p - 1$, have been checked by $p - 1$ passes through routines 2, 3, and 4. If all $a'c$ have been tried, print a typewriter character indicating output, and punch a tape of the permutation $c$. Proceed to Routine 5.

Alternative $B$: Print a typewriter character indicating rejection of the group as alternating. Proceed to Routine 5.

5. *Generate $c$ for the next group in the block of $(p + 1)/4$ groups for this $p$, $k$ pair.*

Multiply the contents of each address $y$ of $c$, $1 \leq y \leq p$ which is a quadratic residue of $p$ by $4 \pmod{p}$. Write this new $c$ over the old one; enter Routine 2 as before.

The program was run for 15,924 groups, requiring somewhat less than 6½ hours on the UNIVAC Scientific computer; that is, an average of about 1.5 seconds was consumed per group. For the groups of high degree, the typewriter indication of rejection of a group as alternating was nearly rhythmic. Some calculation of instruction times made it clear that most groups of high degree were rejected on $ac$, the first permutation tested.

IV. Results. It was demonstrated by the program that for $p = 2q + 1$, $p$ and $q$ primes, $23 \leq p \leq 1823$, the only $G$ of the type sought is the Mathieu group of degree 23. An output tape was prepared for exactly one other group, namely $p = 47$, with $c$ the initial permutation $x \rightarrow x^{45} \pmod{47}$. This occurred through no program or machine error. In this isolated case all $a'c$ fail to satisfy the criterion for rejection. Longhand multiplication of a few permutations showed the group to be alternating. Actually it is a bit surprising that all but one group were rejected by this criterion.

The authors somewhat expected to construct at least one $G$ with this program. It seemed plausible that the $G$ might be quadruply transitive. Instead, the Mathieu groups remain isolated more than before. The results of the program yield good evidence for the conjecture: An unsolvable transitive group of degree $p = 2q + 1$, $p$ and $q$ primes, is alternating or symmetric, except for $p = 7, 11, and 23$. (There is exactly one exception for each of 7 and 23, and two for 11.)

*ADDED IN PROOF.* Paul J. Nikolai, currently with Wright Air Development Center, Wright-Patterson AFB, Ohio, has obtained computer time to continue the problem. The machine used is an 1103A with 12,288 words of core storage. The large storage capacity rendered unnecessary several time-consuming instructions of the earlier code. In addition, the authors improved the logical organization of the program. The result was a speed better than twice that reported above. As for degrees $23 < p \leq 1823$, all groups generated were rejected as alternating. The further degrees run are $p = 1907, 2027, 2039, 2063, 2099, 2207, 2447, 2459,$
On the Accuracy of Implicit Difference Approximations to the Equation of Heat Flow

By Wolfgang Wasow

1. Introduction. Implicit finite difference methods are gaining favor in the numerical solution of initial value problems for partial differential equations, because their computational stability is comparatively insensitive to the mesh ratios. The difference equation problems of importance in the applications are mostly too complicated to permit a theoretical analysis of their approximating qualities. It is a reasonable working hypothesis that the properties of the simplest linear difference equations with constant coefficients are indicative of the situation to be expected in many more involved problems.

The present paper is devoted to a study of the convergence, the stability and the truncation error of implicit difference approximations to the initial value problem defined by the differential equation

\[ L[u] = u_t - u_{xx} = 0, \quad 0 < x < \pi, \quad 0 < t \leq T, \]

where the subscripts indicate partial differentiations, and the subsidiary conditions

\[ u(x, 0) = f(x), \quad u(0, t) = u(\pi, t) = 0, \]

in which \( f(x) \) is a given function. The approximating difference equation to be considered is

\[ L_a[\tilde{u}] \equiv k^{-1}\{ U(x, t + k) - U(x, t) \} - sh^{-2}\{ U(x + h, t + k) - 2U(x, t + k) + U(x - h, t + k) \} - (1 - s)h^{-2}\{ U(x + h, t) - 2U(x, t) + U(x - h, t) \} = 0, \quad 0 < x < \pi, \quad 0 < t \leq T. \]

Received 1 May 1957. Sponsored by the United States Army under Contract No. DA-11-022-ORD-2059.