6379

Bauer

(long)

Not on web

# SIMPLE GROUPS WITH 9, 10, and 11 CONJUGATE CLASSES

Thesis by

Christopher Allen Landauer

In Partial Fullfillment of the Requirements

For the Degree of

Doctor of Philosophy

California Institute of Technology

Pasadena, California

1973

(Submitted July 11, 1972)

Acknowledgment

The author wishes to acknowledge the invaluable assistance of his advisor D. B. Wales in planning and performing the research involved in this thesis. Thanks also go to M. Hall, Jr. and D Sibley for many helpful conversations on this and related topics. Special thanks go to the Department of Mathematics of the California Institute of Technology for providing a Teaching Assistanceship during the course of this research, and for providing the computer time without which this problem could not have been attempted.

Table of Contents

## Abstract

In this paper, we determine all simple groups with 9, 10 and 11 conjugate classes. The method we use is a modification of an old method of Landau: Suppose $G$ is a finite group with $n$ conjugate classes $K_1, K_2, \ldots, K_n$. Then the class equation for $G$ can be written in the following form :

$$1 = \sum_{i=1}^{n} |K_i| / |G| = \sum_{i=1}^{n} 1/m_i ,$$

where $m_i$ is the order of the centralizer of an element of $K_i$, and we choose the numbering so that $|G| = m_1 \geq m_2 \geq \cdots \geq m_n$. The method is to observe each solution and determine whether or not it corresponds to a simple group.

The main direction of this research was to develop tests that reduce the number of solutions computed. These tests deal primarily with the way various prime powers divide the $m_i$'s. These tests, together with a method for generating solutions to the class equation, were programmed by the author in FORTRAN for the IBM 370/155 at Caltech.

The computer time for the case $n = 9$ was 22 seconds, and for $n = 10$ it was about 7 minutes. For $n=11$, the numbers involved were occasionally too large for the computer to deal with, and after producing several new tests, the computing time was 8 hours.

The effect of the computer programs was to produce a few hundred solutions of the class equation that it could not eliminate. These were then examined by hand in order to eliminate the ones that do not correspond to simple groups. During the eliminations by hand, new tests were discovered that should be mechanized for higher values of n.

§1. Introduction.

All finite groups with $n \leq 8$ conjugate classes are known (see Annaveddar (1), Poland (1), Miller (1), Burnside (1), p. 462). In this paper we determine the finite simple groups with 9, 10, and 11 conjugate classes. We also recheck the simple groups with fewer than 9 conjugate classes. These are listed in a table at the end of §4.

We suppose that $G$ is a finite group with $n$ conjugate classes $K_1, \ldots, K_n$. We let $x_i \in K_i$ be a representative for the $i$th class and write $h_i = |K_i|$, $m_i = |G|/h_i = |C_G(x_i)|$ for $1 \leq i \leq n$. Then the class equation for $G$ reads:

$$|G| = \sum_i h_i = \sum_i |G|/m_i \text{ and then}$$

$$1 = \sum_{i=1}^{n} 1/m_i \tag{1.1}$$

Equation (1.1) is our basic starting point for this problem. We arrange the classes in order so that $|G| = m_1 \geq m_2 \geq \cdots \geq m_n$, whence $m_1$ is the least common multiple of the $m_i$'s. The main difficulty with this equation is that there are far more solutions that are not groups than solutions that are. Here we say a solution "is" a group if there exists a group with the specified centralizer sizes. There may be more than one such group. Annaveddar (1) says that for $n=8$ there are about 15,000 solutions, and only 15 groups.

The method we use for solving equation (1.1) was originally developed by Landau (1) in order to prove that the number of groups with $n$ conjugate classes is finite, and to establish some bound on the order of such groups. This method is easily programmed on a computer, using standard backtracking techniques. If we know $m_{i+1}, \ldots, m_n$, we can find some bounds on $m_i$ and we try each possible value. The number of tests this process requires is near the upper limit of what is presently feasible for a computer for 10 and 11 classes; for 12 classes it seems to be beyond the limit. Accordingly, the main results in this paper deal with ways to eliminate certain configurations before they are completed to solutions of equation (1.1). Here the assumption that $G$ is simple gives us further restrictions on these configurations. For example, no finite simple group with $n$ conjugate classes can have $m_n = m_{n-1} = m_{n-2} = 4$ (Poland (1)).

If $G$ is any non-abelian group, we have $m_n \geq 2$ and $m_1 > m_n$, so that $m_n \leq n - 1$. It will turn out that we may assume $5 \leq m_n \leq n-2$ for a simple group, since the simple groups with $2 \leq m_n \leq 4$ are all known. A computer is used to produce a relatively small list of solutions to equation (1.1) by the method described. These are then dealt with, again by computer, using many recent classification theorems about simple groups, and the results follow .

In particular, almost every possible group order is less than

one million for $n \leq 10$ so we can use the results of Hall (2), (4) to determine if the solution corresponds to a simple group.

Theorem: The simple groups with 9 conjugate classes are $L_2(8)$, $L_2(13)$, and $A_7$.

Theorem: The simple groups with 10 conjugate classes are $M_{11}$, $L_3(4)$.

Theorem: The simple groups with 11 conjugate classes are $L_2(17)$ and Sz (8).

The simple groups with fewer than 12 conjugate classes are tabulated elsewhere.

## § 2.1 Notation

All groups we consider will be finite.

$|S|$ The number of elements in the finite set S.

$\pi(a)$ The set of primes dividing the positive integer a.

$\pi'$ The set of primes not in $\pi$

$a_q$ The largest power of the prime q that divides the positive integer a; it is called the q-part of a.

$a_{q'}$ The largest divisor of the positive integer a that is relatively prime to the prime number q; it is called the q'-part of a.

$C_G(A)$ The centralizer in G of the nonempty subset A of a group H containing G(H will be understood, and usually equal to G). If the context allows, we may omit the subscript or the parentheses. Thus: $CA, C(A), C_G A$ are all equivalent to $C_G(A)$.

A similar convention applies to the following notations:

$C_G(y)$ $C_G(\{y\})$.

$N_G(A)$ The normalizer in G of the nonempty subset A of a group H containing G.

$k_G(A)$ The conjugate class of the non-empty subset A of a group H containing G(i.e. the set $\{A^g \mid g \in G\}$).

$k_G(y)$ $k_G(\{y\})$

$G^{\#}$ The set of non-identity elements of the group G.

In addition, we need names for some known simple and non-simple groups. All the names are standard. The $q$ will always denote a prime power representing a finite field of order $q$.

The linear groups $L_n(q) = PSL(n,q)$, $SL(n,q)$, $GL(n,q)$, and $PGL(n,q)$, the unitary groups $U_n(q) = PSU(n,q)$ the alternating groups $A_n$, the Mathieu groups $M_{11}, M_{12}, M_{22}, M_{23}, M_{24}$, and the Suzuki groups $Sz(q)$.

Notation not explained here may be found in Gorenstein (1) or Huppert (1).

§ 2.2 Specific notation for this problem.

$G$ — A finite group.

$n$ — A fixed integer $\geq 2$, usually 9, 10, or 11, representing the number of conjugate classes of $G$.

$m_i$ — $|C_G(x_i)|$, ordered so that $m_1 \geq m_2 \geq \cdots \geq m_n$, and $m_i = m_{i+1} \Rightarrow$ the order of $x_i$ is $\leq$ the order of $x_{i+1}$.

$K_i$ — For $1 \leq i \leq n$, the ith conjugate class (in the ordering described above).

$h_i$ — $|K_i|$, for $1 \leq i \leq n$, the number of elements of the class $K_i$.

$x_i$ — An element of $K_i$, so that $K_i = k_G(x_i)$, and $m_i = |C_G(x_i)|$

$l_i$ — lcm $(m_i, m_{i+1}, \ldots, m_n)$ so that if we define $l_{n+1} = 1$, we have $l_i = \text{lcm}(m_i, l_{i+1})$ for $1 \leq i \leq n$.

$f_i$ $\quad$ $l_i(1 - \sum_{j=i}^{n} \frac{1}{m_j})$ so that $f_i/l_i + \sum_{j=i}^{n} 1/m_j = 1$,

and $f_i/l_i = \sum_{j=1}^{i-1} 1/m_j$. Thus this fraction $f_i/l_i$ tells us how big the $m_j$ must be for $j < i$.

§ 2.3 Assumed results.

We first list some relatively easy theorems that have grown up with this problem.

(2.1) Theorem (Burnside (1)).

If $m_n = 2 \neq |G|$, then $G$ has an abelian normal subgroup of order $2n-3$ and index 2.

(2.2) Theorem (Poland (1), Theorem 3.2)

If $m_n = n-1$, then $G$ is not simple (Poland actually gives a list of the groups here, but we are only interested in the fact that they are not simple).

(2.3) Theorem (Burnside (1)).

If $m_j = p$, a prime, for some $j$, then $p^2 \nmid |G|$. Moreover, $i \neq 1$ and $p \mid m_i \Rightarrow m_i = p$.

(2.4) Theorem (Miller (2)).

If $m_j = p$ for exactly $b$ values of $j \neq 1$, then $b \mid p-1$ and $G$ contains an element of order $(p-1)/b$.

Remark: If $b=p-1$ in the previous theorem, $G$ has a normal p-complement by a theorem of Burnside. We may therefore assume $b \leq (p-1)/2$.

(2.5) Theorem (Poland(1)).

If $m_j = pq$ for $j \neq 1$, and distinct primes $p, q$, then $pq \mid m_i$ for at least three values of $i \neq 1$.

Now we list some harder theorems about simple groups.

(2.6) Theorem (Feit & Thompson (1), see also Higman (1), and Suzuki (3)).

If $G$ is a non-abelian finite simple group with a self-centralizing element of order 3, then $G \cong L_2(5)$ or $G \cong L_2(7)$.

(2.7) Theorem (Suzuki (2), Proposition 8, page 268, see also last paragraph of introduction, page 255).

If a simple group $G$ has a self-centralizing element of order 4, then it has a dihedral Sylow 2-subgroup of order 8, and $G \cong A_6$, $A_7$, or $L_2(7)$.

(2.8) Theorem (For a discussion see Sims (1)).

The primitive permutation groups of degree $\leq 20$ are all known.

Remark: We may therefore assume that the maximal subgroups of $G$ have index more than 20.

(2.9) Theorem (Hall (2), and (4)).

The simple groups of order $< 43200$ are known.

The following result is a corollary of Theorem 3.1 of Hall (1) and the theorem of Brauer & Reynolds given below. It is discussed after Theorem 3.1 of Hall (1) and in Hall (2) page 142 & 149.

(2.10) Theorem.

If G is simple group with 1+rp Sylow p-subgroups, then $p^2 \mid |G|$ implies $r \geq p$ and $p^2 \nmid |G|$ implies $r \geq (p+3)/2$ or else one of the following occurs:

(a) $r = 1$ and $G \cong L_2(p)$.

(b) $r = (p-3)/2$ and $G \cong L_2(2^m)$ with $p = 2^m + 1$.

(2.11) Theorem (Brauer & Reynolds (1), see Hall (2), page 148). If G is a simple group with $p \mid |G|$, then $p^4 > |G|$ implies $p^2 \nmid |G|$. Furthermore, $p^3 > |G|$ implies $p > 3$ and one of the following occurs:

$G \cong L_2(p)$,

or

$G \cong L_2(2^m)$ with $p = 2^m + 1$.

Remark: If $p \mid |G|$ for a simple group G, then $2p(p+1) \leq |G|$ so if $|G| < (2p)(1+p(p+3)/2) = p(2 + p^2 + 3p) = p(p+1)(p+2)$, and G is simple, then G is an $L_2(q)$ for some q.

Now we list some hard theorems on numerical information about G.

(2.12) Theorem (Burnside (1), see also Gorenstein (1), page 131)

A group G with $|\pi(|G|)| \leq 2$ is solvable.

(2.13) Theorem (Thompson (1), see Gorenstein (1), page 259).

The order of a simple group is divisible by 12 or 320.

(2.14) Theorem (Thompson (1)).

If $G$ is a simple group with $|\pi(|G|)| = 3$, then the three primes are 2, 3, and one of 5, 7, 13, 17.

(2.15) Theorem (Wales (1), Brauer (2)).

If $|\pi(|G|)| = 3$ for a simple group $G$, then for $p \in \{5, 7, 13, 17\}$, $p^2 \nmid |G|$ implies $G$ is known.

Theorems (2.12) through (2.15) are used by the program after a configuration is completed and a tentative group order is known. As the application of such results to this problem is clear, they will not be mentioned further.

§ 3. Outline of the method used.

We build solutions $\{m_i \mid 1 \leq i \leq n\}$ to equation (1.1) by what amounts to a sophisticated trial and error method. If we have $m_n, m_{n-1}, \ldots, m_{j+1}, m_j$, we can find bounds on $m_{j-1}$ as discussed in § 4, and then try each possibility.

The major difficulty with applying a computer to this problem is the tremendous number of solutions to equation (1.1). The number of solutions is bounded by $2^{2^n}$ (Landau (1), see also Poland (1)). It is therefore not feasible to determine all the solutions first, and then examine which are simple groups.

Since we are assuming the solutions to represent the sizes of centralizers of elements in a simple group, we can apply many tests to the numbers to eliminate them as possible configurations. The main object is to recognize as early as possible when a sequence of numbers cannot be part of a solution for any simple group. We may cite in this regard an example mentioned before, that if $m_n = m_{n-1} = m_{n-2} = 4$, then no matter what values the remaining $m_i$'s have, we cannot have a simple group (Poland (1)).

There are three programs involved. Each acts as a filter on the set of solutions. The first program applies the easy tests and eliminates most of the configurations. The second applies harder tests and leaves a few cases remaining. The third applies test to a certain special case where the other methods break down.

The result is a short list of possible solutions that must be dealt with by hand. We will describe the programs and illustrate the methods that were most effective in eliminating configurations by hand.

The first program builds solutions and applies theorems (2.3), (2.4), and (2.5) in an attempt to eliminate configurations before they are completed to solutions. It may be noticed that these theorems are not very deep, but they still eliminate a significant percentage of the solutions to equation (1.1). We call a solution a basic solution if it satisfies Theorem (2.3) and the remark after Theorem (2.4). As an example of the effect of the first program, we mention the case $n = 11$. Out of 360,000 basic solutions, only about a thousand passed the tests this program applies.

The second program takes solutions to equation (1.1) which pass the first program's tests, and applies more sophisticated tests to eliminate the solution. This is the program that uses the deepest results from group theory. The majority of these concern the group order alone.

The third program is only used when some of the numbers get too large for our computer. When this situation arises, during the execution of the first program, it prints out information describing the problem. The third program reads this information and applies different tests to eliminate the case.

We describe the procedure used by the first program in more detail. We will consider a partial solution to equation (1.1) as a row of numbers $m_n, m_{n-1}, \ldots, m_j$, written on paper, with $m_n$ at the far left. We assume the paper to have n columns, labelled from n to 1 from left to right, with $m_i$ in the ith column. We view the operation of the program as "filling in the columns."

The program begins at the left, in column n, with a possible value for $m_n$ (we have bounds on $m_n$ from §4). Then Lemma (4.4) is used to find an upper bound for $m_{n-1}$, and the largest possible value for $m_{n-1}$ is written in column n-1.

The program can compute an upper bound for $m_{n-2}$ and continue. At each stage, the theorems are applied to determine if it is possible to complete the partial solution to form a solution of equation (1.1) corresponding to a simple group. We will describe later how each theorem is applied.

If it is possible to complete the solution (i.e., if the theorems are not contradicted), bounds on the next column are computed and the program tries the largest value for that column.

If one of the theorems is contradicted, the program backs up to the previous column (this is what gives the process the name "backtracking"), and tries the next possible value for that column. If there are no more possible values for that column, the program backtracks again and tries a different column.

There are two points at which this process breaks down. The first is when the program actually gets to a solution of equation (1.1), and the second is when it tries to backtrack out of column n, after it has tried all possible values for $m_n$.

When a solution passes all of the tests applied by the first program, it is printed (for the second program) and the program backtracks from column 1. This means that the next possible value for $m_2$ is chosen. Thus the output of the first program consists of a list of solutions to equation (1.1) that pass certain of the more basic tests.

When the program tries to backtrack from column n, it has tried all of the possible values for $m_n$, so the program is done.

Theorem (2.3) is tested two ways: first $m_i$ is examined to find out if it is a prime, and then the program finds out if it is divisible by a prime $p = m_j$, $j > i$. If $m_i$ is a prime, the prime must be remembered to test more $m_i$'s. If $m_i$ is divisible by a prime $p = m_j$ with $j > i$, then $p = m_i$ or else the configuration is not part of a solution representing a simple group, since it directly violates Theorem (2.3).

For Theorem (2.4) to be applied, it is not sufficient to just remember which primes occur. Each prime must be counted also. If a prime p occurs more than $(p-1)/2$ times, the configuration may be eliminated (see the remark after Theorem (2.4)). When the program gets to a solution of equation (1.1), the number of times the

prime p occurs (called b in Theorem (2.4)) is checked to find out if it divides p-1 and if some centralizer is divisible by (p-1)/b. This is the only use this first program makes of the existence of an element of order (p-1)/b.

Similar recording is done for pairs of primes in accordance with Theorem (2.5). If an $m_i = pq$ for distinct primes p and q, then the centralizer it represents must be cyclic, so that elements of order p, q, and pq exist in G with pq dividing their centralizers. (This is, in fact, a proof of the theorem). This means that as the program determines each $m_i$, it keeps track of which prime pairs occur and how many times each pair occurs. These numbers are then tested when the configuration is completed to a solution.

Occasionally, during the backtracking, we recognize a situation that only arises due to the computer being used: when some $m_i$ is too large, we cannot trust the machine to do the arithmetic properly. Fortunately, this situation can be predicted and then dealt with by the special third program, which has to somehow avoid using the numbers. This program will be described after the second one. This situation is recognized when the lower bound on some $m_i$ is too large. For technical reasons, the bound we use is 32768. This case only happens for $m_4$, $m_3$, or $m_2$, when $n \leq 11$, but it gives possible group orders up to $10^{14}$. No simple groups with fewer than 12 conjugate classes occurred among solutions of equation (1.1) that produced this anomaly.

(3.1) Example.

We will illustrate the process by working the case $n = 5$. In order to avoid triviality, we restrict ourselves to using the easy theorems (2.1) through (2.5). We also allow a weak condition similar to (2.8), which says that a simple group has trivial center, so the index of the centralizer of a nontrivial element is at least 2. This means we may take $x = 2$ for Lemma (4.4) and we get: for $2 \leq i \leq 5$, $l_{i+1}/f_{i+1} < m_i \leq (i - 1/2)\, l_{i+1}/f_{i+1}$. We also use (2.1) and (2.2) to get $3 \leq m_5 \leq 5 - 2 = 3$, so $m_5 = 3$.

We write the columns as follows:

| | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|
| m | | | | | |
| f | | | | | |
| l | | | | | |
| u | | | | | |
| v | | | | | |

The integer at the top of each column is the subscript, and the letter at the left of each row is the variable. The variables m, f, and l are defined earlier (in § 2.2), and we repeat the definitions here: $m_i$ is the size of the $i$th centralizer, $l_i = \operatorname{lcm}\{m_i, m_{i+1}, \ldots, m_n\}$, and $f_i$ is chosen so that $f_i/l_i = 1 - \sum_{j=i}^{n} 1/m_j = \sum_{j=1}^{i-1} 1/m_j$. We also set

$v_i = l_{i+1}/f_{i+1}$ and $u_i = v_i(i - 1/2)$, so that for $i = 2,3,4$ we have

$v_i < m_i \leq u_i$ .

Since $m_5 = 3$, we get:

| | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|
| m | 3 | | | | |
| f | 2 | | | | |
| l | 3 | | | | |
| u | - | $5\frac{1}{4}$ | | | |
| v | - | $1\frac{1}{2}$ | | | |

According to the description, we choose the largest possible $m_4$, which is 5. This gives:

| | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|
| m | 3 | 5 | | | |
| f | 2 | 7 | | | |
| l | 3 | 15 | | | |
| u | - | $5\frac{1}{4}$ | 5.3 | | |
| v | - | $1\frac{1}{2}$ | 2.1 | | |

We try $m_3 = 5$ and compute $f_3$, $l_3$, $u_2$, $v_2$.

We get:

| | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|
| m | 3 | 5 | 5 | | |
| f | 2 | 7 | 4 | | |
| l | 3 | 15 | 15 | | |
| u | - | 5.25 | 5.3 | 5.6 | |
| v | - | 1.5 | 2.1 | 3.75 | |

Now $m_3 = 5$ implies $m_2 \geq 5$ and $u_2 = 5.6 \Rightarrow m_2 \leq 5$,

so $m_2 = 5$, but this contradicts (2.4). Thus the possibilities for $m_2$

are exhausted, so we backtrack to column 3 and change $m_3$. Since $m_4 = 5 \leq m_3$, we cannot reduce $m_3$, so we backtrack another column and reduce $m_4$. We get:

| | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|
| m | 3 | 4 | | | |
| f | 2 | 5 | | | |
| l | 3 | 12 | | | |
| u | - | $5\frac{1}{4}$ | 6 | | |
| v | - | $1\frac{1}{5}$ | 2.4 | | |

We first try $m_3 = 6$. This gives $f_3 = 3$, $l_3 = 12$. This gives the following configuration:

| | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|
| m | 3 | 4 | 6 | | |
| f | 2 | 5 | 3 | | |
| l | 3 | 12 | 12 | | |
| u | - | $5\frac{1}{4}$ | 6 | 6 | |
| v | - | $1\frac{1}{5}$ | 2.4 | 4 | |

We again try $m_2 = 6$, and get the solution (3, 4, 6, 6, 12) to equation (1.1). The prime pair $2 \cdot 3 = 6$ occurs only twice, so this solution contradicts (2.5). We therefore backtrack to column 2, and since $m_3 = m_2$, we cannot reduce $m_2$, so we backtrack to column 3. We reduce $m_3$, and we get:

| | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|
| m | 3 | 4 | 5 | | |
| f | 2 | 5 | 13 | | |
| l | 3 | 12 | 60 | | |
| u | - | $5\frac{1}{4}$ | 6 | 6.9 | |
| b | - | $1\frac{1}{5}$ | 2.4 | 4.9 | |

We try $m_2 = 6$, and this gives $f_2 = 3$, $l_2 = 60$, so this does not give a solution of (1.1). We backtrack and reduce $m_2$ to 5. This gives:

| | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|
| m | 3 | 4 | 5 | 5 | |
| f | 2 | 5 | 13 | 1 | |
| l | 3 | 12 | 60 | 60 | |

We have a solution (3, 4, 5, 5, 60) to equation (1.1), which we print, and then backtrack to column 2. Since $m_3 = m_2$, we backtrack to column 3 and reduce:

| | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|
| m | 3 | 4 | 4 | | |
| f | 2 | 5 | 2 | | |
| l | 3 | 12 | 12 | | |
| u | - | $5\frac{1}{4}$ | 6 | 9 | |
| v | - | $1\frac{1}{4}$ | 2.4 | 6 | |

Now $m_2 = 9$ contradicts (2.3) since $m_5 = 3$. Then $m_2 = 8$ gives:

| | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|
| m | 3 | 4 | 4 | 8 | |
| f | 2 | 5 | 2 | 1 | |
| l | 3 | 12 | 12 | 24 | |

We get a solution (3, 4 , 4, 8, 24), print it and continue. We backtrack to column 2, reduce $m_2$ to 7, and get:

| | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|
| m | 3 | 4 | 4 | 7 | |
| l | 3 | 12 | 12 | 84 | |

We do not get a solution here. We further reduce $m_2$ to 6, but this contradicts (2.3) again. We backtrack to column 3, find it can't be reduced, and backtrack again. We get $m_4 = m_5 = 3$, and by (2.4), this is impossible for a simple group. We must backtrack to column 4. Since $m_5 = m_4$, we cannot reduce $m_4$, so we backtrack again. We reduce $m_5$ to 2, and by (2.1), we may quit. This ends the first program, producing 2 solutions.

Since we are not allowing the program to use theorems (2.6) through (2.12), we assume that we must deal with the two solutions by hand.

We can use more complicated theorems to show that there is one simple group of order 60 given by the first solution, and that the second solution does not give a simple group. In fact, we can show it gives $S_4$.

We now describe the second program. It is given some solutions of equation (1.1), and wants to decide if the solutions represent simple groups or not. It is interesting to note that the easiest theorems to apply are the hardest to prove. For instance, theorems (2.12) through (2.15) are easy to apply, since we only need to factor the group order, but they definitely include the deepest theorems used here.

In order to make the testing faster here, we use the program to search for "new" simple groups rather than simple groups. For instance, if we get a group order of 20,160, we stop, because it is

known that there are just two non-isomorphic simple groups of that order, namely $A_8$ and $L_3(4)$. We use in this respect some very recent results. The two most basic -- these are also the two that eliminate the most configurations -- concern themselves solely with the group order and do not consider the other $m_i$'s. The first is a theorem of P. Fong (2, see also Fong (1), Hall (3)) and the second is a theorem of M. Hall, Jr. (4, see also Theorem (2.9)).

(3.2) Theorem. The simple groups whose order is not divisible by 64 are known.

(3.3) Theorem. If the order of a simple group is less than $10^6$, then either the group is known or else it has one of the following orders (there follows a short list of possible group orders, the smallest of which is 43200).

We used an earlier version of this program for $n \leq 10$, where we only assumed that the group order was divisible by 32 and that it was more than 20,000. The program returned only 3 numbers as possible group orders: 20,160, 40,320, and 87,360. The simple groups of order 20,160 are known. There are no simple groups of order 40,320, and we also easily eliminate $87,360 = 2^6 \cdot 3 \cdot 5 \cdot 7 \cdot 13$ as a possible group order with the techniques used by Hall (2).

So far, these tests have only considered the group order. The number of possibilities remaining is now small: for $n \leq 10$, there are about 100 more cases and for $n = 11$ there are about 400.

The program now performs a Sylow center test, determining some orders of elements. This test eliminates all of the remaining cases for $n \leq 10$ and reduces the number of cases for $n = 11$ to about 150.

Suppose that a prime $p$ has its highest power (i.e. $|G|_p$) dividing only one of the $m_i$'s with $i \neq 1$. The the corresponding class is easily seen to be the only class of elements that can be in the center of a Sylow p-subgroup of G. In particular, the elements in such a class must have order $p$. This eliminates a configuration, for instance, when two different primes have their highest powers occuring once only and for the same $m_i$.

This condition is checked for all primes dividing $|G|$. It sometimes occurs that we have a prime $p$ such that every $m_i$ for which $i \neq 1$ and $p | m_i$ is assigned to a prime different from $p$ by the above condition. Then no element is in the center of a Sylow p-subgroup of $G$ and therefore the configuration is eliminated.

The third program accepts as input a partial solution $\{m_i | n \geq i \geq r\}$ where $r = 3$, 4, or 5. Its purpose is to either eliminate the partial solution or compute $m_{r-1}$.

For $r = 5$, the program does nothing, since the cases it could eliminate have restrictive hypotheses that don't apply very often.

For $r = 4$, the third program can use Lemma (4.11) to eliminate some configurations.

For $r = 3$, the program uses lemmas (4.7) and (4.8) to produce a (usually short) list of possible values for $m_2$, together with factorizations of $m_2$ that give the group order $m_1$. The group order is printed when it isn't too large for the computer.

If the group order is not too large for the computer, the solution can be tested in the same way as the first and second programs test solutions. If the group order is too large, most of the tests can still be applied, but they take more time to compute, so not all of them are used.

The first program thus leaves two kinds of configurations. There are some solutions to (1.1) that pass the tests that the first program applies, and there are some partial solutions that pass some of those tests. The second and third programs deal with these two cases, respectively, reducing them to manageable proportions.

The last cases were eliminated by hand, using the techniques listed in the following lemmas. After these lemmas are some examples of the eliminations for $n = 11$.

(3.4) Lemma. Suppose $m_i$ has $r$ different prime factors for some $i \neq 1$. Then we have at least $2r - 1$ different orders of non-trivial elements in $G$.

Proof: Write $m_i = \prod_{j=1}^{r} p_j^{a_j}$, with the $p_j$'s distinct primes and the $a_j$'s positive integers. Then some element of prime order

(Say $x_k$, $k \leq i$ since it may be chosen to be a power of $x_i$) has its centralizer divisible by $\prod_{j=1}^{r} p_j$. Say $x_k$ has order $p_1$. Then there are elements $y_j$ of order $p_j$ with $p_1 \mid\mid |Cy_j|$ for $j \neq 1$. We have therefore constructed $2(r-1)$ elements of order different from $p_1$ and so we have at least $2r-1$ elements of different orders. This is therefore a generalization of Theorem (2.5).

When we use this lemma, we will usually use the list of orders needed, and try to show that we have more necessary orders than classes to assign to them.

(3.5) Lemma. If $p^2 \mid\mid |G|$ and $p^2 \nmid |Cx|$, then $x$ does not have order $p$.

Proof: Let $x$ have order $p$, $x \in P$, a Sylow p-subgroup of $G$. If $x \in ZP$, then $P \leq Cx$, so $p^2 \mid\mid |Cx|$. If $x \notin ZP$, then $\langle x, ZP \rangle \leq Cx$ and $\langle x, ZP \rangle$ has order at least $p^2$.

For instance, if we assume $G$ is simple, then $4 \mid |G|$ so a centralizer of order $2p$ for an odd prime $p$ must correspond to an element of order $p$ or $2p$.

(3.6) Lemma. If a prime $p$ occurs $b \geq 1$ times, we must have $((p-1)/b) + b \leq n$.

Proof: If the prime $p$ occurs as an $m_i$, we have $p^2 \nmid |G|$ by

Theorem (2.3), and if it occurs b times, then there are b classes of p-elements , so if P is a Sylow p-group of G, $|NP/CP| = (p-1)/b$. Then a theorem of Brauer (1) implies that the principal p-block has $(p-1)/b + b$ ordinary irreducible characters, so $(p-1)/b + b \leq n$, since the number of ordinary irreducible characters in all of the blocks is n.

We can get more information here sometimes, when we can show $CP \neq P$, since then there is more than one p-block of defect 1. This limits the possible primes even further. However this is hard to show, since if $CP \neq P$, no $m_j = p$. We do know that for $1 \leq b \leq p - 1$, $\frac{p-1}{b} + b \geq 2\sqrt{p-1}$, so that we may assume $p \leq 1 + n^2/4$ for each prime that occurs to the first power.

We now list some examples for n = 11. In each case, we list several values $m_{11}, m_{10}, \ldots m_j$, $j \geq 3$, and show that this list of numbers is not the first part of the list of centralizer sizes for a new simple group.

The eliminations illustrated are configurations that the computer did not eliminate. The techniques used were developed during this research.

(3.7)

| $m_{11}$ | $m_{10}$ | $m_9$ | $m_8$ | $m_7$ | $m_6$ | $m_5$ | $m_4$ |
|---|---|---|---|---|---|---|---|
| 5 | 5 | 7 | 7 | 7 | 8 | 32 | 66 |

Here we use Lemma(3.4) with $i = 4$, $r = 3$. No $m_i$ with $i \geq 5$ has two primes dividing it, so the $2r - 1 = 5$ classes implied by the lemma must occur among the three classes $K_4$, $K_3$, and $K_2$, which is not possible.

(3.8)

| $m_{11}$ | $m_{10}$ | $m_9$ | $m_8$ | $m_7$ | $m_6$ | $m_5$ |
|---|---|---|---|---|---|---|
| 5 | 5 | 7 | 7 | 8 | 9 | 13 |

Now we compute $f_5/l_5 = 41/32760$ (see §2.2 for notation), so Lemma (4.4) implies $m_4$ cannot be 13. Therefore Lemma (3.6) with b=1 gives $13 \leq 11$, a contradicition.

(3.9)

| $m_{11}$ | $m_{10}$ | $m_9$ | $m_8$ | $m_7$ | $m_6$ | $m_5$ |
|---|---|---|---|---|---|---|
| 5 | 5 | 7 | 7 | 9 | 9 | 11 |

Here $f_5/l_5 = 4/3465$ so $m_4$ cannot be 11 by Lemma (4.4). Thus we have by Theorem(2.4) an element $x$ of order 10, and since $5 \mid |Cx|$ and $5 \nmid |Cx|$, we contradict Theorem (2.3).

(3.10)

| $m_{11}$ | $m_{10}$ | $m_9$ | $m_8$ | $m_7$ | $m_6$ | $m_5$ | $m_4$ |
|---|---|---|---|---|---|---|---|
| 6 | 6 | 6 | 6 | 7 | 12 | 18 | 20 |

Now $9 \mid m_5 \mid\mid G \mid$ so the centralizers of order 6 must be centralizers of elements of order 6, so $x_{11}$, $x_{10}$, $x_9$, $x_8$ have order 6 by Lemma(3.5). Since we have $5 \mid m_4$, we have $x_4$ of order 10 (it can't have order 20 since that would require $x_3, x_2$ to have

orders 10, 5, 4, and 2 with 5 dividing the centralizers). Since we need elements of order 5 and 2 with 20 dividing the centralizer, $x_2$ and $x_3$ have orders 2 and 5 or 5 and 2, respectively. Thus $x_5$ can't have order 9 or 18 or 6, since each requires an element of order 3 with 18 dividing the centralizer. For example, if $x_5$ has order 6, $x_5^2$ has order 3 and $Cx_5 \subseteq Cx_5^2$. Therefore $x_5$ has order 3.

We claim $x_6$ has order 2. Order 12 is out since it requires an element of order 4 with 12 dividing the centralizer. Order 6 is out since it implies 12 divides the centralizer of an element of order 3. Order 3 is out by Lemma(3.5) since $9 \mid |G|$. Order 4 is out since if 3 divides the centralizer of an element of order 4, there is an element of order 12.

The orders of the elements of G are now known:

| $x_{11}$ | $x_{10}$ | $x_9$ | $x_8$ | $x_7$ | $x_6$ | $x_5$ | $x_4$ | $x_3$ and $x_2$ |
|---|---|---|---|---|---|---|---|---|
| 6 | 6 | 6 | 6 | 7 | 2 | 3 | 10 | 2 and 5 or 5 and 2. |

There are no elements of order 4 in G, so a Sylow 2-group P is elementary abelian. Since $x_6$ has order 2, $P \subseteq C(x_6)$, so $|P| = 4$, and $CP \cong P \times Z_3$.

Since not all involutions are conjugate, $NP/CP$ has order 1, and so $NP = CP$. Burnside's theorem implies G has a normal 2-complement.

(3.11)

| $m_{11}$ | $m_{10}$ | $m_9$ | $m_8$ | $m_7$ | $m_6$ | $m_5$ |
|---|---|---|---|---|---|---|
| 5 | 5 | 7 | 7 | 7 | 8 | 52 |

We know $x_5$ has order 2, 4, 13, 26 or 52. If 2 or 4, then there must be an element $y$ of order 26 or 52 whose 13th power is $x_5$, so $Cy \subseteq Cx_5$, which is clearly impossible. If $x_5$ has order 13, there is an element $y$ of order 26 or 52 with $y^2$ or $y^4$ conjugate to $x_5$. Again $Cy \subseteq Cx_5$, which is impossible. Therefore $x_5$ has order 26 or 52. If it has order 52, we need elements of orders 26, 13, 4, and 2 with 52 dividing their centralizers, so these four orders must occur in the three classes $K_4, K_3$, and $K_2$, a contradiction.

We have then that $x_5$ has order 26, so that among $\{x_4, x_3, x_2\}$ there are elements of orders 13 and 2 with 52 dividing the centralizers.

We compute $f_5/l_5 = 99/3640$, so using Lemma (4.4), we get $m_4 \leq 112$. Now using $m_4 \geq 52$, we have $f_4/l_4 \geq 29/3640$, so $m_3 \leq 260$.

If a prime $p \mid |G|$ with $p \notin \{2, 5, 7, 13\}$, then we have $p$ divides exactly one of $m_2, m_3, m_4$ since two of the orders are known. We then have that the corresponding $m_i$ must be a power of $p$.

If $13^2 \nmid |G|$, then the group $C(x_5)$ contains a Sylow

13-subgroup P of G, so that CP contains $x_5$. Therefore CP > P, so there are at least two 13-blocks of defect 1(Brauer (1) ). Since any 13-block of G of defect 1 has at least 7 characters, we have at least 14 characters here, contradicting n = 11. Therefore $13^2 \mid |G|$.

Since there is only one class of elements of order 13, and since an element of order 13 has a centralizer whose order is divisible by 4, we have that the centralizer of an element of order 13 has order at least $4 \cdot 13^2 = 676 > 260$. Therefore, we must have $x_2$ of order 13, so $x_3$ or $x_4$ has order 2, with 13 dividing the order of $Cx_3$ or $Cx_4$. By Theorem (3.4), there is an element of order 2 with 64 dividing the centralizer order. Since $13 \cdot 64 > 260$, we cannot have the same class for these 2-elements, so $x_3$ and $x_4$ both have order 2, with 26 dividing one centralizer order and 64 the other.

Therefore $|G| = 2^a \cdot 5 \cdot 7 \cdot 13^b$, with $a \geq 6$, $b \geq 2$, since no other prime can occur in $|G|$.

The multiples of 64 that are less than 260 are 64, 128, 192, and 256. Since $3 \nmid |G|$, no centralizer can have order 192, so one centralizer (either $C(x_3)$ or $C(x_4)$) has order $2^a$, with $6 \leq a \leq 8$.

Similarly, for 26 we want a multiple of 26 between 52 and 260 with no primes except 2, 13. The only possibilities are 52, 104, 208,

so this centralizer has order $2^s \cdot 13$, $2 \leq s \leq 4$.

Now $m_2 = 2^r \cdot 13^b$ for some $r \geq 1$, since no other prime can occur. We have $a \geq r \geq 1$, since a Sylow 2-subgroup of $C(x_2)$ is contained in a Sylow 2-subgroup of G. Then since $f_5/l_5 = 99/3640$, we have :

$$99/13 \cdot 35 \cdot 8 = 1/2^a + 1/2^s \cdot 13 + 1/2^r \cdot 13^b + 1/|G|$$

If we multiply the above equation by $|G|$, we get :

$$99 \cdot 2^{a-3} \cdot 13^{b-1} = 5 \cdot 7 \cdot 13^b + 2^{a-s} \cdot 5 \cdot 7 \cdot 13^{b-1} + 2^{a-r} \cdot 5 \cdot 7 + 1$$

Now taking residues modulo 13, we have (recall $b \geq 2$) :

$$0 \equiv 2^{a-r} \cdot 35 + 1 \pmod{13}$$

$$4 \cdot 2^{a-r} \equiv 1 \equiv 40 \pmod{13}$$

$$2^{a-r} \equiv 10 \equiv 1024 \pmod{13}$$

$$a - r \equiv 10 \pmod{12}.$$

But $8 \geq a \geq r \geq 1$ implies $7 \geq a - r \geq 0$, so this configuration is eliminated.

The last two examples illustrate the application of Lemma (4.8) to these problems.

(3.12)

| $m_{11}$ | $m_{10}$ | $m_9$ | $m_8$ | $m_7$ | $m_6$ | $m_5$ | $m_4$ | $m_3$ |
|---|---|---|---|---|---|---|---|---|
| 6 | 6 | 6 | 6 | 10 | 10 | 10 | 32 | 486 |

Here $l_3 = 38880 = 2^5 \cdot 3^5 \cdot 5$. Since $486 = 2 \cdot 3^5$ divides $|G|$, the sixes must correspond to elements of order 6 by Lemma (3.5). Since we assume $64 \mid |G|$ by (3.2), and since $64 \nmid l_3$, we have $64 \mid m_2$ and $x_2$ has order 2. Therefore $m_3$ must be the centralizer of a central element in a Sylow 3-group, so $x_3$ has order 3. Now the sixes imply that there is an element of order 2 with 3 dividing the centralizer, so $3 \mid m_2$.

Now $\{x_7, x_6, x_5\}$ must have orders 5 and 10, so we may assume $x_7$ has order 10 and $x_5$ has order 5. Then $x_6$ has order 5 or 10. If $x_6$ has order 5, then all elements of order 10 are conjugate to $x_7$, so all elements of order 5 are conjugate to $x_7^2$. This contradicts the fact that here we have two classes of elements of order 5. Therefore $x_6$ has order 10 and $5^2 \nmid m_2$.

We take Lemma (4.8) with $p = 2$, $m_2 = 2^{a+b} c$, $l_3 = 2^b(2^a - 1) c$, $c$ is odd and $b=5$. Since $15 \mid m_2$, $15 \mid c$, so $2^a - 1 \mid 3^4$. Therefore $2^a - 1 = 3$, $a = 2$, $c = 5 \cdot 3^4$, or $2^a - 1 = 1$, $a = 1$, $c = 5 \cdot 3^5$, which gives $m_2 = 2^7 \cdot 5 \cdot 3^4$ or $2^6 \cdot 5 \cdot 3^5$. Then

$$|G| = 2^7 \cdot 5 \cdot 3^5 = 155,520 < 10^6, \quad 2^6 \cdot 3^5 \cdot 5 = 77,760 < 10^6,$$

and both of these orders are not on the list of Theorem (3.3).

A nice alternative to this elimination uses the results of Brauer (2) on simple groups of order $2^a 3^b 5$. For the configuration

above, we have one class of elements of order 5, so there is an element of order 4 normalizing a Sylow 5-group. This must be conjugate to $x_4$. Note that we can now say that G has two 5-blocks of defect 1. Since $m_2$ cannot have a prime divisor other than 2, 3, 5, we have $|G| = 2^a 3^b 5$ with $a \geq 6$, $b \geq 5$. There is no such simple group.

(3.13)

| $m_{11}$ | $m_{10}$ | $m_9$ | $m_8$ | $m_7$ | $m_6$ | $m_5$ | $m_4$ | $m_3$ |
|---|---|---|---|---|---|---|---|---|
| 6 | 6 | 6 | 6 | 8 | 8 | 14 | 96 | 686 |

Here $l_3 = 32928 = 2^5 \cdot 3 \cdot 7^3$. Now since $m_3 = 686 = 2 \cdot 7^3$, $x_5$ must be an element of order 14. We again assume $64 \mid |G|$ by Theorem (3.2), and since $64 \nmid l_3$, we have $64 \mid m_2$ and $x_2$ has order 2. Then $x_3$ has order 7, and so $7 \mid m_2$ by Theorem (2.5).

To apply Lemma (4.8), we have p=2 again, and $l_3 = 2^5 \cdot 3 \cdot 7^3 = 2^b(2^a - 1)c$, c odd, and $m_2 = 2^{a+b}c$. Since $7 \mid m_2$, $7 \mid c$. Therefore, $2^a - 1 \mid 3 \cdot 7^2$. There are three solution to this condition: a = 1, 2, and 3. These give $2^a - 1 \mid 21$, so $7^2 \mid c$. Therefore, since $c \mid m_2$, $x_2$ of order 2 commutes with a 7-subgroup of G of order 49. Since there is only one class of 7-elements in G, all have order 7, so this group of order 49 is elementary abelian. But now we have an abelian group of order 98, so there is an element of order 14 with a centralizer divisible by 98, which is not possible. Thus this configuration is eliminated.

§ 4. Bounds

We have seen that for a finite simple group, we have $2 < m_n < n-1$ (Theorem (2.1) and (2.2)). We will show that we may assume $4 < m_n < n-1$. This gives a bound for $m_n$ as required by the algorithm of the first of the three computer programs. We will also derive bounds for each $m_i$ in terms of $m_{i+1}, \ldots, m_{n-1}, m_n$ for $2 \leq i \leq n-1$.

(4.1) Lemma. If G is a finite simple group with n conjugate classes, and if $m_n \leq 4$, then G is known.

Remark: The program uses this result by assuming $5 \leq m_n \leq n-2$ (see Theorem (2.2)).

Proof: We will show that if $m_n = 3$, there is a self-centralizing 3-element, and all such groups are classified (Feit and Thompson(1)). If $m_n = 4$, then the possible Sylow 2-subgroups are found, and the simple groups for each type of Sylow 2-group have been classified.

If some $m_j = 3$, then G has a centralizer of order 3, so G has a self-centralizing Sylow 3-group of order 3 by Theorem (2.3). Then Theorem (2.6) implies G is isomorphic to $L_2(5)$ with 5 classes, or $L_2(7)$ with 6 classes.

If some $m_j = 4$, we have $m_j = |C(x_j)|$, where $x_j \in G$. Let P be a Sylow 2-subgroup of G containing $x_j$. Then $C_P(x_j)$ has order 4 also. Now by a theorem in Huppert (1, Satz III. 14.23 page 375),

$P$ must have maximal class. So either $P$ is abelian of order 4, or $P$ is non-abelian and a theorem in Gorenstein (1, Theorem 5.4.5 page 194) implies $P$ is dihedral, generalized quaternion, or semi-dihedral.

The simple groups with these Sylow 2-subgroups are all known by various deep classification theorems. Rather than refer to these, we use relatively straightforward arguments to eliminate most cases.

If $C(x_j)$ is cyclic, then $x_j$ must have order 4, since $ZP \subseteq C(x_j)$ and $x_j$ has order 2 imply $P$ is cyclic, so that $G$ has a normal 2-complement. Then $x_j$ is an element of order 4 which is self-centralizing, so Theorem (2.7) implies $G \cong L_2(7)$, $A_6 \cong L_2(9)$, or $A_7$.

We may therefore suppose that $C(x_j)$ is a Klein 4-group. Then we have an element $x \in P$ of order 2 with $C_G(x)$ a non-cyclic group of order 4. Since a generalized quaternion 2-group has only one involution, $P$ is dihedral of order at least 4 or else $P$ is semi-dihedral of order at least 16. We eliminate all of these possibilities except $P = Cx$ by various fusion arguments.

If $P$ is semi-dihedral, Proposition 1 of Alperin-Brauer-Gorenstein (1, page 10, see also exercises 6 and 7 on page 265 of Gorenstein (1)) implies $G$ has one conjugate class of involutions. Then $x$ must be in the center of some Sylow 2-group, so $|C_G x| \geq 16$, a contradiction.

If $P$ is dihedral of order at least 8, Theorem 7.7.3(i) of Gorenstein (1, page 262) implies $G$ has one conjugate class of involutions. Therefore $|Cx| \geq 8$, a contradiction.

We must therefore have $P = Cx$ is non-cyclic of order 4. Now easy fusion arguments (Theorem 7.7.1(i), page 260 of Gorentstein (1)) give that $G$ has one conjugate class of involutions and $N_G P \cong A_4$.

Now $N_G P$ satisfies the hypotheses of Theorem 9.2.1 of Gorenstein (1, page 306), so $N_G P$ is a strongly embedded subgroup of $G$. Then Theorem 9.2.2 of Gorenstein (1, page 308) with $H = M = N_G P$ and $C = P < H$ gives :

$[G:N_G P] \leq 1 + |P| = 5$, so $|G| \leq 60$, and since $G$ is assumed to be simple, $G \cong A_5$.

Therefore all of the simple groups with an $m_j = 3$ or 4 are known.

We note that Suzuki (2, and 1, Lemma 4) determines all of the 2-groups with a centralizer of order 4, and W.J. Wong (1,2) determines $G/O_{2'}(G)$ for an arbitrary group with a centralizer of order 4. Here $O_{2'}(G)$ is the unique maximal normal subgroup of $G$ of odd order.

(4.2) Conjecture. If $m_n = n-2$, for a simple group $G$ with $n$ conjugate classes, then $G \cong L_2(2^m)$ with $n = 2^m + 1 \geq 5$.

The groups $L_2(2^m)$ have $n = 2^m + 1$ conjugate classes and and $m_n = n-2$.

(4.3) Conjecture. If $m_n = n-3$ for a simple group $G$ with $n$ conjugate classes, then $G \cong L_2(q)$ with $q = 2n - 5 \geq 5$.

The groups $L_2(q)$ have $n = (q+5)/2$ and $m_n = n-3$.

Now that Lemma (4.1) gives us a bound on $m_n$, we consider the problem of bounding $m_i$ for $2 \leq i \leq n-1$. We suppose that $x$ is a lower bound for the size of a non-trivial conjugate class, so that all centralizers of non-identity elements have index greater than $x$.

(4.4) Lemma. Suppose $2 \leq i \leq n-1$, and that $m_{i+1}, \ldots, m_n$ are known. Then we have bounds on $m_i$ :

$$l_{i+1}/f_{i+1} < m_i \leq (i - 1 + 1/x)\, l_{i+1}/f_{i+1}.$$

Proof : First recall the definitions. $m_1 = |G| \geq m_2 \geq \cdots \geq m_n$ are the centralizer orders, $l_i = \mathrm{lcm}(m_i, m_{i+1}, \ldots, m_n)$ $= \mathrm{lcm}(m_i, l_{i+1})$, where $l_{n+1} = 1$, and $f_i$ is determined by the equation

$$f_i/l_i + \sum_{j=i}^{n} 1/m_j = 1.$$

Since $m_j \geq m_i$ for $1 < j \leq i$, we have $1/m_i \geq 1/m_j$ for $1 < j \leq i$. Then equation (1.1) gives:

$$1 = \sum_j 1/m_j = 1/m_1 + \sum_{j=2}^{i} 1/m_j + \sum_{j=i+1}^{n} 1/m_j$$

$$\leq 1/m_1 + (i-1)/m_i + 1 - f_{i+1}/l_{i+1} ,$$

so that

$$f_{i+1}/l_{i+1} \leq 1/m_1 + (i-1)/m_i \leq 1/xm_i + (i-1)/m_i$$

$$\leq (1 + x(i-1))/xm_i = (i-1 + 1/x) / m_i .$$

Thus the right-hand half of the inequality is proved. Now

$1/m_i < 1/m_1 + 1/m_2 + \cdots + 1/m_i = f_{i+1}/l_{i+1}$ implies

$m_i > l_{i+1}/f_{i+1}$ and we are done.

In particular, for $i = 2$ we have $1/m_1 + 1/m_2 = f_3/l_3$ and $l_3 < f_3 m_2 \leq l_3 (1 + 1/x)$, $m_1 = \text{lcm}(m_2, l_3)$.

We mention here that we use $x$ as a lower bound for the index of a centralizer, although we computed it as a lower bound for the index of a subgroup. This bound may be expected to be a poor bound, and for the known simple groups with few conjugate classes, it is so.

A table follows of simple groups with 11 or fewer conjugate classes.

| Group | n | Smallest Index of a Centralizer | Smallest Index of a Subgroup |
|---|---|---|---|
| $A_5$ | 5 | 12 | 5 |
| $L_2(7)$ | 6 | 21 | 8 |
| $A_6$ | 7 | 40 | 6 |
| $L_2(11)$ | 8 | 55 | 12 |
| $L_2(8)$ | 9 | 56 | 9 |
| $A_7$ | 9 | 70 | 7 |
| $L_2(13)$ | 9 | 84 | 14 |
| $M_{11}$ | 10 | 165 | 11 |
| $L_3(4)$ | 11 | 315 | 21 |
| $L_2(7)$ | 11 | 144 | 18 |
| Sz(8) | 11 | 455 | 65 |

Since $m_2$ is the last centralizer order chosen by the first program, we try to find more restrictive conditions for the primes dividing $m_2$. These conditions are used by the second and third programs to eliminate configurations.

We first prove a preliminary lemma:

(4.5) Lemma. Suppose $p$ is a prime dividing $m_1 = |G|$ and exactly one other $m_i$. Then a Sylow $p$-group $P$ of $G$ is elementary abelian, self-centralizing, and disjoint from its conjugates. Furthermore, $|P| = m_i$, $|N_G P| = |P|(|P| - 1)$, and $|G| = |N_G P|(r|P| + 1)$ for some integer $r \geq 0$.

Proof: Let $p \mid m_i$ for $i \neq 1$ ( p always divides $m_1$ if it divides any $m_i$), so that $p \nmid m_j$ for $j \neq 1, i$. Let P be a Sylow p-subgroup of G and let $x \in ZP$, $x \neq 1$. Then $p \mid |Cx| \neq |G|$, so $|Cx| = m_i$. If any prime $q \neq p$ divides $m_i$, there is an element $y \in Cx$ of order q, and thus $x \in C(y)$ implies $p \mid |Cy|$, which is impossible. Thus we have $m_i = |P|$ is a power of p.

Since every element of $P^{\#}$ is conjugate to every other, P must have exponent p. Therefore if $p = 2$, P must be abelian. We show that P is abelian if p is odd. Since all elements of $(ZP)^{\#}$ are conjugate in NP, $|NP/P| > 1$. In fact, NP is transitive on $(ZP)^{\#}$ since all elements of $|ZP|^{\#}$ are conjugate in G (7.1.1 page 240 Gorenstein (1)). Therefore $|ZP| - 1 \mid |NP|$, and therefore $2 \mid |NP|$. Let $y \in NP$ have order 2. Then $y \notin P$, and y induces an automorphism of P. Since $x \in P^{\#}$ implies C(x) is a p-group, $C_P(y) = 1$, so y induces a fixed-point-free automorphism of P of order 2. Then Theorem 10.1.4 of Gorenstein (1, page 336) implies P is abelian.

Now all elements of $P^{\#}$ are conjugate in G, so they are conjugate in NP, and therefore $|P| - 1 \mid |NP|$. Since every non-trivial element of NP/P acts fixed-point-freely on P, we have NP/P acting regularly on $P^{\#}$, so $|NP| = |P|(|P| - 1)$.

Finally, we note that if $P$ and $Q$ are Sylow p-subgroups of $G$ with $y \in P \cap Q$, then $y \neq 1$ implies $P, Q \leq C(y)$ since $P$ and $Q$ are abelian, and so $P = C(y) = Q$, since $C(y)$ is a p-group. Therefore $P \neq Q$ implies $P \cap Q = 1$ and so $P$ is disjoint from its conjugates. Then we have that the number of Sylow p-subgroups in $G$ is $[G : NP] \equiv 1 \pmod{|P|}$.

(4.6) Three Cases. We will describe three possible divisions of our arguments, depending on the prime powers dividing $m_1$ and $l_3$. Recall that $m_1 = \text{lcm}(m_2, l_3)$ by definition, and that this implies $\pi(m_1) = \pi(m_2) \cup \pi(l_3)$.

Case I. $m_1 = l_3$. This is equivalent to $m_2 | l_3$ since $m_1 = \text{lcm}(m_2, l_3)$.

Case II. $m_1 > l_3$, but $\pi(m_1) \subseteq \pi(l_3)$. This means that all primes dividing $m_2$ also divide $l_3$, but that one or more of the primes dividing $m_2$ has a higher power in $m_2$ than in $m_3$.

Case III. $m_1 > l_3$, and $\pi(m_1) \nsubseteq \pi(l_3)$.

We first note that exactly one of these cases holds for any given group $G$. For each of the cases, we will derive certain numerical conditions on $G$ which have the property that they may be tested without knowing $m_2$ or $m_1$. In fact, they will produce for any sequence $m_3, m_4, \ldots, m_n$, all possible values of $m_2$ and $m_1$ that give solutions to equation (1.1) corresponding to a simple group.

The program uses this division into cases as follows: when it has determined $m_n, m_{n-1}, \ldots, m_3$, it checks the numerical conditions derived from Case I. If these are satisfied, the program determines the possible values of $m_2$, and prints each solution with message indicating that it is a Case I solution. It then checks the numerical conditions derived from Case II, and prints out the possible solutions. This avoids the problem of determining whether or not it is possible for two non-isomorphic simple groups to have the same values $m_3, m_4, \ldots, m_n$, and yet have one solution be of Case I and the other of Case II.

As we shall show, Case III cannot occur for a simple group, so the program does not check the conditions for Case III.

(4.7) Lemma. If G is a finite group with n conjugate classes satisfying Case I, then there is a positive integer a such that $a + 1 = f_3$, $a \mid l_3$, and $l_3 \geq am_3$.

Proof: $l_3 = m_1$ implies $m_2 \mid l_3$, so let $l_3 = am_2$ for a positive integer a. Then $1/m_1 + 1/m_2 = f_3/l_3$ implies $1/a\,m_2 + 1/m_2 = f_3/am_2$, so $1 + a = f_3$. Since $m_2 \geq m_3$, we have $l_3 \geq am_3$.

The program tests this case by checking whether $f_3 - 1 \mid l_3$ and $l_3 \geq (f_3 - 1)\, m_3$.

(4.8) Lemma. If G is a finite group with n conjugate classes satisfying Case II, then there is a prime power $p^a > 1$ and a

positive integer $d$ such that $f_3 p^a = 1 + l_3/d$, and $p \mid d \mid l_3$.

Proof: We have $\pi(m_2) \subseteq \pi(l_3)$ and $m_1 > l_3$, so at least one prime $p$ has $(m_2)_p > (l_3)_p$. In fact, there is at most one such prime $p$, since if $q$ is any prime for which $(m_2)_q > (l_3)_q$, $x_2$ is in the center of a Sylow $q$-subgroup of $G$.

Let $d = \gcd(l_3, m_2)$. Then $m_1 = \operatorname{lcm}(m_2, l_3) = m_2 l_3/d$, so $f_2/l_2 = 1/m_1 = f_3/l_3 - 1/m_2$ implies $d/m_2 l_3 = f_3/l_3 - 1/m_2$, so $f_3 m_2 - l_3 = d$. Now $f_3(m_2/d) - (l_3/d) = 1$, so that $\gcd(f_3 m_2/d, l_3/d) = 1$, and therefore $\pi(m_2/d) \cap \pi(l_3/d) = \emptyset$. Since $m_2$ has $\pi(m_2) \subseteq \pi(l_3)$ by hypothesis, we have : for every prime $q$ dividing $m_2/d$ (by assumption it must divide $l_3$), $d_q = (l_3)_q$, so that $(m_2)_q > (l_3)_q$. From the above paragraph, we see that $m_2/d$ must be a prime power $p^a$, and we must have $f_3 p^a = 1 + l_3/d$.

Remark. The programs test this lemma in the following form : given $f_3, l_3$, solve $f_3 p^a = 1 + l_3/d$ for some $d \mid l_3$ and prime power $p^a$.

(4.9) Lemma. If $G$ is a finite group with $n$ conjugate classes satisfying Case III, then $(1 + l_3)/f_3$ is a prime power $p^a > m_3$, and $p^a - 1 \mid f_3 - 1$. Furthermore, $G$ satisfies the conclusions of Lemma (4.5).

Proof : We have $\pi(m_2) \not\subseteq \pi(l_3)$, so that there is a prime $p \mid m_2$ with $p \nmid l_3$. But $l_3 = \operatorname{lcm}(m_3, m_4, \ldots, m_n)$, so that $p \mid m_1$ and $m_2$

only. Thus G satisfies the hypotheses of Lemma (4.5) with $i = 2$.

We have by definition $1/m_1 + 1/m_2 = f_3/\ell_3$. Then Lemma (4.5) implies $m_2 = |P| = p^a$, $m_1 = |G| = p^a(p^a - 1)(1 + rp^a) = m_2 l_3$, so that $l_3$ is $(p^a - 1)(1 + rp^a)$. Thus :

$$1/p^a(p^a - 1)(1 + rp^a) + 1/p^a = f_3/l_3$$

$1 + l_3 = f_3 p^a$, so $f_3 p^a = 1 + (p^a - 1)(rp^a + 1) = 1 + rp^{2a} - rp^a + p^a - 1$, so $f_3 = rp^a - r + 1$ and $p^a - 1 \mid f_3 - 1$. The lemma is proved.

(4.10) Theorem. Case III of (4.6) does not occur for a simple group.

Remark. If G is an arbitrary finite group satisfying Case III, then the Sylow p-group is normal. This is proved by a slight extension of the proof below. As we do not use it in this work, we do not prove it here.

Proof of (4.10) : Our proof is based on the following theorem of Zassenhaus :

Theorem (Passman (1), Theorem 20.5, page 263). If G is sharply triply transitive, then G is not simple (all such groups are known, but this fact suffices). Here a sharply triply transitive group is a triply transitive group in which the stabilizer of three points is trivial.

We have the following situation : a Sylow p-group $P$ is elementary abelian, self-centralizing, disjoint from its conjugates, and it has order $q = p^a$. If $x \in P^{\#}$, then $C(x) = P$, so if $x$ is a p-element in $G$, $|Cx| = m_2 = q$. Also, $NP/P$ is regular on $P^{\#}$, so $|NP| = q(q-1)$.

Now $|G| = q(q-1)(1 + rq)$ and $P \triangleleft G \Rightarrow r \geq 1$. We have $x \in G^{\#}$ implies $|C_G(x)| \leq |P| = q$ since $|P| = m_2$ and $m_2$ is the largest nontrivial centralizer. Since $|ZG| = 1$ is odd, a theorem of Brauer and Fowler (Gorenstein (1), Theorem 9.1.6 page 303) implies $|G| < |C_G(x)|^3$ for some $x \in G^{\#}$. Therefore $|G| < q^3$.

Thus $r = 1$ and $|G| = q(q-1)(q+1)$. This is the expected order for sharp triple transitivity, so we look for a set of $1+q$ elements.

We consider the action of $G$ on the Sylow p- subgroups of $G$. This action is certainly transitive, and the stabilizer of a point $P$ is $NP$. Now Proposition 17.2 of Passman (1, page 181) implies $NP$ is a Frobenius group with complement $R$(say) of order $q-1$.

We claim $NP$ is transitive on the $q$ Sylow p-subgroups of $G$ different from $P$. In fact, $P$ is transitive on the Sylow p- subgroups different from $P$, since $x \in P$ fixes a Sylow p-subgroup $Q$ of $G$ implies $x \in NQ$, but $x$ is a p-element of $NQ$ implies $x \in Q$ implies $x \in P \cap Q = 1$. Therefore the stabilizer in $P$ of a Sylow p-group $Q \neq P$ has order 1, so the orbit containing $Q$ has

size $q$ and must therefore contain all of the other Sylow p-groups.

Now let $S$ be a two-point stabilizer and suppose one of the points is $P$. Then $S \leq NP$ and $|S| = q-1$, so $|S| = |R|$ implies $S$ is conjugate to $R$ in $NP$ by the Schur-Zassenhaus theorem. Therefore $R$ is also a two point stabilizer, say of $P$ and $Q \neq P$.

A three point stabilizer, with one of the points equal to $P$, is the intersection of two distinct conjugates of $R$. Say $R$ fixes $P$ and $Q_1$ and $S$ fixes $P$ and $Q_2$. Then $R, S \leq NP$, so $R$ is conjugate to $S$ in $NP$, so $R \cap S = 1$, since $R$ is the Frobenius complement in the Frobenius group $NP$. Since $|R| = q-1$, this implies $R$ is transitive on the $q-1$ Sylow p-groups it does not fix, so we are done.

Remark. Cases I and II of (4.6) do occur in simple groups :

Case I

| Group | Order = $l_3$ | $m_2$ | $f_3$ | a |
|---|---|---|---|---|
| $A_7$ | 2520 | 36 | 71 | 70 |
| $A_9$ | 20160 | 108 | 113 | 112 |

Case II

| Group | Order | $m_2$ | $f_3$ | $l_3$ | $p^a$ | d |
|---|---|---|---|---|---|---|
| $L_3(3)$ | 5616 | 54 | 35 | 1872 | 3 | 36 |
| $U_3(3)$ | 6048 | 108 | 19 | 2016 | 3 | 54 |

Remark. One might prove (4.10) using Theorem 9.1.7 page 304 of Gorentstein (1). Using the notation there, we have $b \leq q$, $c \leq q$, $|G| = q(q-1)(1+rq) \leq b(b-1)(c+1)$, which implies $b = c = q$. Since $b$ and $c$ are orders of centralizers, respectively, of an involution and of an element of odd order, we get an immediate contradiction unless $r = 0$, whence (as advertised) $P \lhd G$.

(4.11) Lemma. If $G$ is simple and if a prime $p$ divides $m_3$ and does not divide $l_4$, then either $m_2$ and $m_3$ are powers of $p$, or else the conclusions of Lemma (4.5) hold for $p$ and $m_3$.

Proof: If $x_3$ is not a p-element, then $q \mid |x_3|$ for some prime $q \neq p$. Then there are classes of elements of orders $pq$, $p$, and $q$, with $pq$ dividing their centralizers. Since this is impossible by hypothesis, we have $x_3$ is a p-element. The same argument shows we cannot have a prime $q \neq p$ dividing $m_3$. Therefore, $m_3$ is a power of $p$.

If $p \mid m_2$, then the above argument shows that $m_2$ is also a power of $p$. If $p \nmid m_2$, then $p$ divides $m_1 = |G|$ and $m_3$ and no other $m_i$, so Lemma (4.5) can be applied.

(4.12) Conjecture. The only simple groups $G$ satisfying the hypotheses of Lemma (4.11) have $m_2 = m_3$ and $G \cong L_2(q)$, where $q \equiv 1 \pmod 4$.

The groups $L_2(q)$ with $q \equiv 1 (\mathrm{mod}\ 4)$ satisfy the hypotheses of Lemma (4.11) and have $m_2 = m_3 = q$.

We now prove some related results that do not affect the performance of the program.

(4.13) Lemma. Let $G$ be a finite non-abelian simple group in which $y \in G$ and $s$ an integer implies $y^s = 1$ or $C(y^s) = C(y)$. Then $G \cong L_2(2^m)$ for some $m \geq 2$.

Proof: We will show that if $x \in G^{\#}$, $C(x)$ is nilpotent. Then a classification theorem finishes it.

Let $x \in G^{\#}$ and consider the cyclic subgroups of $G$ containing $x$. Then any such subgroup $M$ is in $Cx$ so $x \in M = \langle y \rangle$ implies $x = y^s \neq 1$, so $Cx = Cz = CM$.

If $M$ and $N$ are two cyclic subgroups containing $x$, then $CM = Cx = CN$, so that $M$ and $N$ centralize each other. Therefore, if $y$ and $z$ in $Cx$ have order relatively prime to the order of $x$, they commute, since $zx$ and $yx$ generate cyclic subgroups of $G$ containing $x$.

Thus if $x$ has prime order $p$, the set of elements of order prime to $p$ forms an abelian normal $p$-complement $Dx$ of $Cx$.

We claim that if $x \neq 1$, $Cx$ is nilpotent, and if $|Cx|$ has more than one prime divisor, $Cx$ is abelian. If we prove these claims for elements $x$ of prime order, we will be done, since every centralizer is the centralizer of an element of prime order.

So let $x$ have prime order $p$. If $Cx$ is a $p$-group, we are done, so we assume $q \mid |Cx|$ where $q$ is a prime different from $p$. Let $y \in Cx$ have order $q$. Then since $x$ and $y$ are both powers of $yx$, $Cx = Cyx = Cy$.

The Sylow $p$-subgroup $S_p$ of $Cx$ is contained in $Dy$, so it must be abelian. Since $Dy$ is abelian, we have $S_p$ char $Dy$ char $Cx$ implies $S_p$ is characteristic in $Cx$. Since the Sylow $q$- subgroup $S_q$ of $Cx$ is in $Dx$, we have that $S_q$ is a characteristic abelian subgroup of $Cx$. Since all of the Sylow subgroups of $Cx$ are normal, $Cx$ is nilpotent. Since each Sylow subgroup is abelian, $Cx$ is abelian.

Now we have the centralizer of every non-identity element is nilpotent. Therefore (see Gorenstein (1), page 416), a theorem of Suzuki implies that $G$ is isomorphic to one of the following groups: $L_2(2^m)$, $Sz(2^m)$, $L_2(p)$ with $p$ a Fermat or Mersenne prime, $L_2(9)$, or $L_3(4)$.

If a Sylow 2-subgroup $P$ of $G$ has exponent 2, it is abelian and $G$ must be $L_2(2^m)$. We may therefore assume that $P$ has exponent 4 or more, so that $P^2 = \langle y^2 \mid y \in P \rangle \neq 1$. Then since $P^2$ is obviously characteristic in $P$, $P^2 \cap ZP \neq 1$, so if $x \in P^2 \cap ZP$ with $x \neq 1$, we have $x = y^2$ for some $y \in P$. But $x \in ZP$ implies $P \subseteq Cx = Cy2 = Cy$ implies $y \in ZP$. Thus $ZP \cap P^2 = (ZP)^2$.

Now the groups $Sz(2^m)$, $L_3(4)$, $L_2(p)$, and $L_2(9)$ all have non-abelian special Sylow 2-groups, so that $ZP = P^2 \neq 1$ and $(ZP)^2 = 1$. The lemma is complete.

We now use the lemma to prove a fact, which says roughly, if all the centralizers are small, we know the group .

(4.14) Theorem. Let $G$ be a finite simple group with $n$ conjugate classes and with $|Cx| \leq n$ for all $x \in G^{\#}$. Then $n = 2^m + 1 \geq 5$ and $G \cong L_2(2^m)$.

Proof : We will show that a group $G$ satisfying the hypotheses of this theorem also satisfies the hypotheses of Lemma (4.13).

We know $n \geq 5$ for a simple group, and we have $m_2 \leq n$ by hypothesis. We show first that $m_2 = n$. So suppose $m_2 \leq n-1$. Then $m_i \leq n-1$ for $i \geq 2$ and we get :

$$1/m_i \geq 1/n-1$$

$$1 = \sum_{i=1}^{n} 1/m_i = 1/m_1 + \sum_{i=2}^{n} 1/m_i \geq 1/m_1 + (n-1)/(n-1) > 1,$$

a contradiction, so $m_2 = n$.

We also know $m_n \leq n-2$ by Theorem (2.2). We find a lower bound for $m_n$.

$1/m_i \geq 1/n$ for $i \geq 2$ gives :

$$1 = \sum_{i=1}^{n} 1/m_i = 1/m_1 + \sum_{i=2}^{n-1} 1/m_i + 1/m_n \geq 1/m_1 + (n-2)/n + 1/m_n,$$

so $2/n \geq 1/m_1 + 1/m_n > 1/m_n$, so $m_n > n/2$.

Now we have $n \geq m_2 \geq m_i \geq m_n > n/2$, for all $i > 1$, so if $y \in G$, and $y^s \neq 1$, $C(y^s) \supseteq C(y)$ and $[C(y^s) : C(y)] < 2$, so $C(y^s) = C(y)$. The hypotheses for the previous lemma are satisfied and we are done.

The groups $L_2(2^m)$ have the property of the theorem.

(4.16) Conjecture. Let $G$ be a finite simple group with $n$ conjugate classes and with $|Cx| \leq 2n$ for all $x \in G^{\#}$. Then if $\exists x \in G^{\#}$ for which $|Cx| > n$, $G \cong L_2(q)$ with $q = 2n - 5$.

The groups $L_2(q)$ have $n = (q + 5)/2$ and all of the centralizers of order less than $2n$.

Table I: The conjugate simple groups with $n \leq 11$ conjugate classes.

| n | $\|G\|$ | G |
|---|---|---|
| 5 | 60 | $A_5 \approx PSL(2,4) \approx PSL(2,5)$ |
| 6 | 168 | $PSL(2,7) \approx PSL(3,2)$ |
| 7 | 360 | $A_6 \approx PSL(2,9)$ |
| 8 | 660 | $PSL(2,11)$ |
| 9 | 504 | $PSL(2,8)$ |
| | 1092 | $PSL(2,13)$ |
| | 2520 | $A_7$ |
| 10 | 7920 | $M_{11}$ (Mathieu Group) |
| | 20160 | $PSL(3,4)$ |
| 11 | 2448 | $PSL(2,7)$ |
| | 29120 | $Sz(8)$ (Suzuki Group) |

6379

306

1 2 3 4 5 6 7 8 9 10 11
0 0 0 0 1 1 1 1 3 2 2

12 13 14 15 16 17 18 19 20 21
3 0 4 3 1 2 2 0 1 2

Table II : The known simple groups with n conjugate classes, $12 \leq n \leq 21$.

| n | $\|G\|$ | G |
|---|---|---|
| 12 | 3420 | PSL (2, 19) |
| | 5616 | PSL (3, 3) |
| | 443, 520 | $M_{22}$ (Mathieu Group) |
| 13 | | |
| 14 | 6048 | PSU (3, 3) |
| | 6072 | PSL(2, 23) |
| | 20100 | $A_8 \approx$ PSL (4, 2) |
| | 126000 | PSU (3, 5) |
| 15 | 7800 | PSL (2, 25) |
| | 95040 | $M_{12}$ (Mathieu Group) |
| | 175, 560 | $J_1$ (Janko Group) |
| 16 | 9828 | PSL (2, 27) |
| 17 | 4080 | PSL (2, 16) |
| | 12180 | PSL (2, 29) |
| 18 | 14880 | PSL (2, 31) |
| | 181440 | $A_9$ |
| 19 | | |
| 20 | 25920 | PSU (4, 2) $\approx Sp_4(3)$ |
| 21 | 25308 | PSL (2, 37) |
| | 604800 | HJ(Hall-Janko Group) |

Note on Table II : There are no known simple groups with 13 or 19 conjugate classes. I suspect that the table is actually complete up to n = 14 or 15, and that therefore there are no simple groups with n = 13.

# REFERENCES

The references are arranged alphabetically by author and then numbered consecutively for each author.

Alperin, Brauer, Gorenstein

(1) Finite Groups with quasi-dihedral and wreathed Sylow 2-groups, Trans. Am. Math. Soc. vol. 151 pp. 1-261 (1971).

Annaveddar, Edwin K.

(1) Determination of the finite groups having eight conjugate classes, Thesis, Arizona State Univ., (1971).

Brauer, R.

(1) On groups whose order contains a prime number to the first power I, Am. J. Math. vol. 64, pp. 401-420 (1942).

(2) On simple groups of order $5 \cdot 3^a \cdot 2^b$, Bull. Am. Math. Soc. vol. 74, pp. 900-903 (1968).

Brauer and Leonard

(1) On finite groups with an abelian Sylow p-group, Can. J. Math. vol. 14, pp. 436 - 450 (1962).

Brauer and Reynolds

(1) On a problem of E. Artin, Ann. Math. vol. 86, pp. 713-720 (1958).

Burnside, W.

(1) Theory of groups of finite order, Dover, NY, 1955 (Same as 2nd. ed., Cambridge, 1911).

Feit and Thompson

(1) Finite groups which contain a self-centralizing subgroup of order 3, Nagoya Math. J. vol. 21. pp.185-197(1962).

Fong, P.

(1) Some Sylow 2-groups of order 32 and a characterization of $U_3(3)$, J. Alg. vol. 6 pp. 65-76 (1967).

(2) Sylow 2-groups of small order (to appear).

Gorenstein, D.

(1) Finite Groups, Harper and Row, NY, 1968.

Hall, M. Jr.

(1) On the number of Sylow subgroups in a finite groups, J. Alg. vol. 7, pp. 363-371 (1967).

(2) A search for simple groups of order less than one million, pp. 137-168 in Leech (1).

(3) Construction of finite simple groups, Proc. Symp. Appl. Math. AMS no. 23, pp. 109-134 (1970).

(4) Simple groups of order less than one million, J. Alg. vol. 20 pp. 98-102(1972).

Higman, G.

(1) Odd characterizations of simple groups, Lecture notes, U. Michigan, Summer 1968.

Huppert, B.

(1) Endliche Gruppen: I, Springer, Berlin, 1967.

Landau, E.

(1) Über die Klassenzahl der binaren quadratischen Formen von negativer Diskriminanten, Math. Ann. vol. 56 pp. 671-676 (1903).

Leech, J. (ed.)

(1) Computational Problems in Abstract Algebra, Pergamon Press, NY, 1970.

Miller, G.A.

(1) Groups involving only a small number of sets of conjugate operators, Arch. Math. und Phys. vol. 17, pp. 199-204 (1910).

(2) Groups involving only a small number of sets of conjugate operators, Proc. Nat. Acad. Sci, USA vol. 30 pp. 359-362 (1944).

Passman, D.S.

(1) Permutation Groups, Benjamin, NY, 1968.

Poland reference at end.

Sims, C.C.

(1) Computational methods in the study of permutation groups, pp. 169-184 in Leech (1).

Suzuki, M.

(1) A characterization of the simple group LF(2, p) , J. Fac. Sci, Univ. Tokyo (Sect. I) vol. 6, pp. 259-293 (1951).

(2) On finite groups containing an element of order 4 which commutes only with its powers, Ill. J. Math. vol. 3, pp. 255-271 (1959).

(3) Applications of group characters, Proc. Symp. Pure Math. AMS no. 6, pp. 101-105 (1962).

Thompson, J.G.

(1) Nonsolvable groups all of whose local subgroups are solvable, Sec. 1-6 : Bull. Am. Math. Soc. vol. 74, pp. 383 -437 (1968), Sec. 7-9: Pac. J. Math. vol. 33, pp. 451-537 (1970), Sec. 10-12: Pac. J. Math. vol. 39, pp. 483 - 534 (1971), balance to appear.

Wales, D. B.

(1) Classification of Simple Groups of Order $p \cdot 3^a \cdot 2^b$, p a Prime, Proc. Symp. Pure Math. AMS no. 21, pp. 161-163 (1971).

Wong, W.J.

(1) On finite groups whose 2-Sylow subgroups have cyclic subgroups of index 2, J. Aust. Math. Soc. vol. 4, pp. 90-112 (1964).

(2) Finite groups with a self-centralizing subgroup of order 4, J. Aust. Math. Soc. vol. 7, pp. 570-576 (1967).

Poland, John

(1) Groups with 6 and 7 conjugate classes. Can. J. Math. v. 20 pp. 456-464 (1968).