# A NOTE ON THE MATHIEU GROUPS

LOWELL J. PAIGE

**1. Introduction.** The principal result of this paper is the representation of the Mathieu group $M_{23}$ as a group of $11 \times 11$ matrices over the Galois Field GF(2). This is a new representation of $M_{23}$ and in §5 an indication of how the techniques of this result might be extended to the Mathieu group $M_{11}$ is given.

The results of §3 were essentially obtained by Professor E. Spanier while investigating another problem and it was during conversations with him that the present result was observed.

**2. Steiner systems and the Mathieu groups.** A Steiner system $S(p, q, r)$, with $p \leqslant q \leqslant r$, is defined on the $r$ integers $1, 2, \ldots, r$ and consists of $\binom{r}{p}/\binom{q}{p}$ subsets $H_x$ of $q$ integers each with the property that any arbitrary set of $p$ integers is contained in one and only one of the subsets $H_x$. For example, the Steiner system $S(2, q+1, q^2+q+1)$ ($q$ a prime) can be constructed by considering the points and lines of a finite projective plane with $q+1$ points on each line.

The *group* $G$ of a Steiner system $S(p, q, r)$ consists of all those permutations of the symmetric group $\mathfrak{S}_r$ that permute the subsets $H_x$ among themselves. Witt **(1**, p. 274**)** has shown that the Steiner systems S(4, 5, 11), S(5, 6, 12), S(3, 6, 22), S(4, 7, 23) and S(5, 8, 24) are unique (i.e., for fixed $p, q, r$, there exists a permutation of $\mathfrak{S}_r$ carrying $S_1(p, q, r)$ into $S_2(p, q, r)$) and the groups associated with these Steiner systems are the Mathieu groups $M_{11}$, $M_{12}$, $M_{22}$, $M_{23}$, and $M_{24}$ respectively.

**3. Generation of** S(4, 7, 23)**.** Let $V(n)$ be the vector space consisting of all $n$-tuples $(x_1, x_2, \ldots, x_n)$, with each $x_i$ contained in the Galois Field GF(2), under the usual definitions of addition and scalar multiplication.

The distance $d(x, y)$ between two vectors $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_n)$ of $V(n)$ is defined to be the number of coordinates for which $x_i \neq y_i$ $(i = 1, 2, \ldots, n)$.

A subset $S(r, n)$ of $V(n)$ is defined to be an exact $r$-covering of $V(n)$ if and only if

(i) For every vector $x \in V(n)$, $\min_{s \in S(r,n)} \{d(x, s)\} \leqslant r$;

(ii) For $s_1, s_2 \in S(r, n)$, $d(s_1, s_2) > 2r$.

For a fixed vector $s$ of an exact $r$-covering $S(r, n)$, the number $N(r, n)$ of vectors $x \in V(n)$ and satisfying $d(x, s) \leqslant r$ is obviously

Received April 7, 1956.

$$N(r, n) = \binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{r}. \tag{3.1}$$

The number of vectors in an exact $r$-covering $S(r, n)$ is clearly $2^n/N(r, n)$ since the equation $d(x, s) \leqslant r$ can have but one solution $s$ in $S(r, n)$ for every vector $x$ of $V(n)$.

It may be possible for $S(r, n)$ to be a linear subspace of $V(n)$. Certainly a necessary condition for such a possibility is that $N(r, n)$ divide $2^n$. In the case that $n = 23$ and $r = 3$ we have $N(3, 23) = 2^{11}$ and in the following lemma an exact 3-covering of $V(23)$ is obtained that is a linear subspace.

LEMMA 3.2. *Let $R$ be the subspace of $V(23)$ generated by the rows of the following rectangular array with elements in* GF(2):

(3.3)

1 0 0 0 0 0 0 0 0 0 0 1 1 1 1 0 0 1 1 0 1 0 0
0 1 0 0 0 0 0 0 0 0 0 1 1 1 0 1 0 1 0 1 0 1 0
0 0 1 0 0 0 0 0 0 0 0 1 1 1 0 0 1 0 1 1 0 0 1
0 0 0 1 0 0 0 0 0 0 0 1 1 0 1 1 0 0 0 1 1 0 1
0 0 0 0 1 0 0 0 0 0 0 1 1 0 1 0 1 1 0 0 0 1 1
0 0 0 0 0 1 0 0 0 0 0 1 1 0 0 1 1 0 1 0 1 1 0
0 0 0 0 0 0 1 0 0 0 0 1 0 1 1 1 0 0 1 0 0 1 1
0 0 0 0 0 0 0 1 0 0 0 1 0 1 1 0 1 0 0 1 1 1 0
0 0 0 0 0 0 0 0 1 0 0 1 0 1 0 1 1 1 0 0 1 0 1
0 0 0 0 0 0 0 0 0 1 0 1 0 0 1 1 1 1 1 1 0 0 0
0 0 0 0 0 0 0 0 0 0 1 1 0 0 0 0 0 1 1 1 1 1 1

*The linear subspace $T$ orthogonal to $R$ is an exact* 3*-covering of* $V(23)$.

*Proof.* The crucial part of the proof is the verification that no six columns of (3.3) are linearly dependent. The usual statement at this point regarding straightforward computations would be inappropriate. However, the verification was accomplished on the high speed computer SWAC, and the computations, of necessity, will be omitted.

Assuming the result of the previous paragraph, the proof proceeds by noting that, for any two vectors $t_1$ and $t_2$ of $T$, $d(t_1, t_2) > 6$, since otherwise there would exist a subset of six columns of (3.3) that would be linearly dependent. Now a simple numerical calculation (i.e. $2^{11} \cdot 2^{12} = 2^{23}$) shows that $T$ is an exact 3-covering of $V(23)$.

We now proceed to generate S(4, 7, 23). Let $H_t$ be the set of all integers $j$ such that $t_j \neq 0$ for the vector $t \equiv (t_1, t_2, \ldots, t_n)$ of the linear subspace $T$ of Lemma 3.2.

THEOREM 3.4. *The set of all sets $H_t$ containing seven integers forms a Steiner system* S(4, 7, 23).

*Proof.* $T$ is an exact 3-covering of $V(23)$ and since no six columns of (3.3) are linearly dependent it is clear that every vector of $V(23)$ with 4 non-zero

coordinates must be at distance 3 from those vectors of $T$ with 7 non-zero coordinates. Each vector of $T$ with 7 non-zero coordinates is at distance 3 from $\binom{7}{4}$ vectors with 4 non-zero coordinates and hence there are $\binom{23}{4}/\binom{7}{4} = 253$ vectors in $T$ with 7 non-zero coordinates.

An arbitrary set of 4 integers cannot be contained in $H_{t_1}$ and $H_{t_2}$ (containing 7 integers) if $t_1 \neq t_2$ because this would imply that there would be 6 linearly dependent columns of (3.3). This completes the proof of Theorem 3.4 and establishes the existence of a Steiner system S(4, 7, 23).

**4. A matrix representation of $M_{23}$.** In this section an $11 \times 11$ matrix representation over GF(2) will be obtained for the Mathieu group $M_{23}$.

Let $T$ be the exact 3-covering of $V(23)$ obtained in Lemma 3.2, and let S(4, 7, 23) be the Steiner system consisting of the sets $H_t$ constructed in Theorem 3.4. The following vectors of $T$ are linearly independent and generate $T$:

$$
\begin{aligned}
t_1 &= (0\,0\,0\,0\,0\,0\,1\,1\,1\,1\,1\,1\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0)\\
t_2 &= (1\,1\,1\,1\,1\,1\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0)\\
t_3 &= (1\,1\,1\,0\,0\,0\,1\,1\,1\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0)\\
t_4 &= (1\,0\,0\,1\,1\,0\,1\,1\,0\,1\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0)\\
t_5 &= (0\,1\,0\,1\,0\,1\,1\,0\,1\,1\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0)\\
t_6 &= (0\,0\,1\,0\,1\,1\,0\,1\,1\,1\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0)\\
t_7 &= (1\,1\,0\,0\,1\,0\,0\,0\,1\,1\,1\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0)\\
t_8 &= (1\,0\,1\,0\,0\,1\,1\,0\,0\,1\,1\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0)\\
t_9 &= (0\,1\,1\,1\,0\,0\,0\,1\,0\,1\,1\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0)\\
t_{10} &= (1\,0\,0\,1\,0\,1\,0\,1\,1\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0)\\
t_{11} &= (0\,1\,0\,0\,1\,1\,1\,1\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1)\\
t_{12} &= (0\,0\,1\,1\,1\,0\,1\,0\,1\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1)
\end{aligned}
$$

These vectors yield subsets $H_{t_i}$ $(i = 1, 2, \ldots, 12)$ of S(4, 7, 23) and since $M_{23}$ consists of those permutations of the symmetric group $\mathfrak{S}_{23}$ that transpose the subsets $H_x$ of S(4, 7, 23) among themselves, it is possible to consider $M_{23}$ as the group of all $23 \times 23$ permutation matrices $Q$ which leave $T$ invariant. Thus a representation of $M_{23}$ is induced on the space $T$ and, since each $Q$ is orthogonal, on the space $R$ orthogonal to $T$.

THEOREM 4.1. *The representation $\rho$ of $M_{23}$ induced on $R$ is an isomorphism.*

*Proof.* The kernel of $\rho$ consists of those permutations $Q$ that leave the array (3.3) invariant. Since no two columns of (3.3) are the same, the kernel of $\rho$ is the identity.

We thus obtain an $11 \times 11$ matrix representation over GF(2) for $M_{23}$, and it is of interest to note that this representation is irreducible. The referee has suggested the following simple proof: If $\rho$ were not irreducible, there would exist an invariant subspace $S$ of $R$ of dimension $k$ with $0 < k < 11$. Then $\rho(M_{23})$ would be a subgroup of the group of all non-singular transformations

of $R$ leaving $S$ invariant. However, the order of $\rho(M_{23})$ is divisible by 23 and the order of the group of all non-singular transformations leaving $S$ invariant,

$$2^{k(11-k)} \prod_{i=1}^{k} (2^k - 2^{i-1}) \prod_{j=1}^{11-k} (2^{11-k} - 2^{j-1}),$$

is not. This argument also proves that $M_{23}$ does not have a faithful representation by $k \times k$ matrices over GF(2) for any $k < 11$.

**5. Comments and generalizations.** If the field of coefficients in §3 of $V(n)$ is allowed to be the Galois field GF($p^k$), the same definitions of distance and exact $r$-covering $S(r, n)$ yield the fact that there are

$$N(r, n, p^k) = \binom{n}{0} + (p^k - 1) \cdot \binom{n}{1} + \ldots + (p^k - 1)^r \cdot \binom{n}{r}$$

vectors of $V(n)$ that satisfy $d(x, s) \leqslant r$ for $s \in S(r, n)$.

In the case that $p = 3, k = 1, r = 2$ we find that $N(2, 11, 3) = 3^5$; as in §3, it is possible to construct a $5 \times 11$ rectangular array over GF(3) such that no 4 columns are linearly dependent. The subsequent analysis of the orthogonal space in $V(11)$ over GF(3) leads to a Steiner system S(4, 5, 11).

It had been hoped that the matrix representations of the Mathieu group obtained in this paper might lend itself to the determination of a simple set of generators of $M_{23}$; unfortunately, this aim has not been realized.

It should also be pointed out that the divisibility of $(p^k)^n$ by $N(r, n, p^k)$, although necessary, is not sufficient to ensure the existence of an exact $r$-covering of $V(n)$. For example, $N(2, 90, 2) = 2^{12}$, yet a simple analysis of vectors having three non-zero coordinates shows that no exact 2-covering can exist. Here again the techniques of the present note become hopelessly involved in combinatorial analysis if one attempts to find new Steiner systems or simple groups.

## Reference

1. E. Witt, *Ueber Steinersche Systeme*, Abhand. Math. Sem. Univ. Hamburg, *12* (1938), 265–275.

*University of California at Los Angeles*