JOURNAL OF COMBINATORIAL THEORY 6, 122–151 (1969)

New 5-Designs*

E. F. ASSMUS, JR.† AND H. F. MATTSON, JR.

Applied Research Laboratory, Sylvania Electronic Systems, Waltham, Massachusetts 02154

Communicated by A. M. Gleason

Received April 4, 1968

ABSTRACT

A t-design on a point-set S is a collection $\mathscr{D}$ of subsets of S, all of the same cardinality, with the property that every t-subset of S is contained in precisely λ elements of $\mathscr{D}$, λ a fixed integer parameter of the design. Via the theory of error-correcting codes, we construct here several new 5-designs on 24 and 48 points as well as the two classic 5-designs on 12 and 24 points associated with the Mathieu groups M_{12} and M_{24}. We are able, in many cases, to say what the automorphism groups of the new 5-designs are.

1. INTRODUCTION

Tactical configurations and Hadamard matrices, studied for many years by combinatorialists, and the newer subject called error-correcting codes, studied for less than twenty years, have some interesting interconnections. The purpose of this report is to establish a number of new results arising therefrom.

Our main result is the construction (via Theorem 4.2) of several new 5-designs on 24 and 48 points and the determination (Section 5) of their automorphism groups as $\mathrm{PSL}_2(23)$ and $\mathrm{PSL}_2(47)$, respectively. A secondary result (Section 5) is that $\mathrm{PSL}_2(l)$ is the automorphism group of certain quadratic-residue codes of length $l+1$ for all primes l having $(l-1)/2$ prime and satisfying $23 \leqslant l \leqslant 4{,}079$. (For $l = 23$ we use [15] and a new 5-design on 24 points; the other cases are an immediate consequence of the Parker and Nikolai search [22].) We have derived elsewhere [7] the consequence that for $l \equiv -1 \pmod{12}$, the Paley-Hadamard matrix of order $l+1$ has $\mathrm{PSL}_2(l)$ as automorphism group for l as above.

* The research reported in this paper was sponsored by the Air Force Cambridge Research Laboratories, Office of Aerospace Research, under contract AF19(628)-5998.

† Lehigh University and Sylvania.

The paper constructs an infinite class of designs and groups, the designs coming from the vectors of quadratic-residue codes and the groups being the automorphisms groups of these codes. The codes are indexed by the prime l; and when $(l-1)/2$ is a prime greater than 5, a result of Ito [15], moreover, implies that the group is either $\mathrm{PSL}_2(l)$ or is 5-fold transitive. The Mathieu groups M_{12} and M_{24} occur in this class; they are, of course, the only known cases with $l \geqslant 11$ in which the group is not $\mathrm{PSL}_2(l)$.

We also establish:

(1) The existence of two disjoint 5-designs of each of the types found of the smallest "club" size[1] (Section 6) and the action of $\mathrm{PSL}_2(l)$ on each of these collections.

(2) The existence of several infinite classes of 3-designs (Theorem 4.1 and Application (3) in Section 4).

(3) The optimality of "almost all" cyclic codes of a given prime length (Section 2).

(4) The non-vanishing of all subdeterminants of (z^{ij}), where z is a primitive l-th root of 1 and the non-vanishing of all coefficients of all proper divisors of $x^l - 1$ in characteristic 0 (Section 2).

We place in print the Gleason-Prange theorem, that $\mathrm{PSL}_2(l)$ acts on every quadratic-residue code (Section 3). We note here that this theorem furnishes for every prime p an explicit representation of degree $(l+1)/2$ for $\mathrm{PSL}_2(l)$ over $\mathrm{GF}(p^n)$ or $\mathrm{GF}(p^{2n})$ for any n. These derive from such a representation over a quadratic number field.

There seem to be few papers which construct designs from linear codes. Paige [21] found Steiner systems in two codes, although he did not call his linear spaces "codes." We pursued in [3] the course he had started on, finding for each Mathieu group M a code with M as automorphism group, for which the code is a representation-space of smallest possible degree; Paige did this for M_{23}. We have written other papers on two kinds of Steiner systems [4, 5, 6], all treated by the coding-theory approach presented here. Perhaps the first explicit construction of designs from codes was in Bose's paper [8] on the connections between error-correcting codes and confounding and fractional replication in the design of experiments. Surprisingly, there do not seem to be any others except a recent Codes-BIBD report [17], although numerous strong implicit connections in the literature likely exist.

In [14] Hughes considers the problem of constructing t-designs in relation to the problem of transitively extending groups. His quite different

[1] Some of these results were announced in [4].

methods yield t-designs seemingly unrelated to those here, except that the 5-design found there appears here also, since it is intimately related to the Mathieu group M_{12} (see Section 6).

ACKNOWLEDGEMENT. We are indebted to A. M. Gleason, Eugene Prange, and Richard Turyn for many interesting discussions concerning this subject. In particular, Theorem 3.1, on the automorphism groups of quadratic-residue codes, was first proved by Gleason and Prange and our proof is an adaptation of Prange's. Gleason was the first to observe the existence of gaps in the weight distribution, a fact crucial to the use of Theorem 4.2. We also thank John Thompson for pointing out to us that the Parker-Nikolai result implied that the automorphism group of the (48, 24) code in Section 4 had to be small. Finally, we gratefully acknowledge the help of Nicodemo Ciccia, who wrote the computer programs which suggested the existence of the 8; 5-12-48 design and which helped determine the orbit structure of $PSL_2(47)$ on this design.

DEFINITIONS OF CODING TERMS. There are several ways to define a code. We use the following: Let F be a field and $V = F \times \cdots \times F$ (n times) the vector space of all ordered n-tuples over F. Let A be a k-dimensional subspace of V. Then A is called an (n, k) *code* over F. Elements of A are often called *code-vectors*.

With the code A, we sometimes want to single out the coordinate function $f_0, \ldots, f_{n-1}$; $f_i(a_0, \ldots, a_{n-1}) = a_i$. When we do this, we denote the set of coordinate functions by S, viewing them in A^*, the dual of A. S is a spanning subset of A^*, and we may even speak of the code as the pair (A, S).

Sometimes we define a code a bit more abstractly by considering a finite-dimensional F-space K and a set S of F-linear functionals on K which span the dual space of K. Ordering S as $f_0, \ldots, f_{n-1}$, we define the code A as the space of all $(cf_0, cf_1, \ldots, cf_{n-1})$ for c in K.

If x is in V, the *weight* of x is defined to be the number of non-0 coordinates of x, and the *distance* between x and y in V is the weight of $x - y$. This distance function is a translation-invariant metric. The minimum distance d from one code-vector to the rest is the same for each starting point, so that the spheres of radius $(d - 1)/2$ about the code-vectors are disjoint. In the rare case that these spheres exhaust V, the code is called *perfect*.

A *cyclic* (n, k) code is one which is invariant under the permutation of coordinates sending coordinate i to $i + 1$ (modulo n). Such codes can be regarded as ideals in the ring $F[x]/(x^n - 1)$, where multiplication by (the residue class of) x is the cyclic shift. As such, they are principal ideals

generated by the divisors of $x^n - 1$ over F. Thus, if $g(x)$ divides $x^n - 1$, then all the multiples of $g(x)$ in $F[x]$ of degree less than n constitute a set of representatives of $(g(x))/(x^n - 1)$. $g(x)$ is called the *generator polynomial* of the code. The code furthermore is given *recursively* by the complementary divisor of $g(x)$, by which we mean that, if $g_1(x)\, g(x) = x^n - 1$, then the code is the set of all $(a_0, \ldots, a_{n-1})$, $a_i \in F$, such that

$$\sum_{i=0}^{k} a_{i+j} b_{k-i} = 0, \qquad j = 0, 1, \ldots, n-1,$$

where $g_1(x) = b_0 x^k + \cdots + b_k$. The reader who would like to see more discussion of these points is referred to [23, Chapter 8] or [2, Section IV2].

It is sometimes convenient to construct cyclic codes as follows. Let K be $F(z)$ where z is a primitive n-th root of 1 over the field F. Set $k = [K : F]$. Let f be any non-0 F-linear functional on K as vector space over F. Then define a set S of n coordinate functions $f_0, \ldots, f_{n-1}$ as $cf_i = (cz^i)f$, $c \in K$, $i = 0, 1, \ldots, n-1$. Then $\{(cf_0, \ldots, cf_{n-1});\ c \in K\}$ is a cyclic (n, k) code over F. This code is immediately seen to be recursive for the reverse of the minimal polynomial of z (i.e., that of z^{-1}) over F, and it is not hard to prove that the ideal generator polynomial is the complementary divisor. This construction yields only the irreducible cyclic codes, those given recursively by irreducible polynomials; but all cyclic codes are direct sums of irreducible one. An irreducible cyclic code as just defined is obviously a minimal subspace invariant under the cycling operation, since otherwise the generator polynomial would be $x^n - 1$. In the general case, the cyclic code given recursively by $g_1(x)$ dividing $x^n - 1$ contains that for each irreducible divisor of $g_1(x)$; and the sum of these irreducible codes is direct in that 0 can be represented only as $0 + \cdots + 0$. A dimension argument shows equality of the code and the direct sum.

Every F-linear functional on K has the form $T(a(\ ))$ for some a in K, where T is the trace from K to F.

The *orthogonal code* to a given code is obtained as the subspace of V orthogonal under the dot product with the code. The orthogonal of a cyclic code is cyclic.

The minimum distance of a code over F is unchanged when we extend the coefficient field F to an overfield L by the tensor product [1].

The minimum non-0 weight in an (n, k) code A is the minimum distance and is equal to $n - m + 1$, where m is the least integer such that every m-subset of S spans A^*. Here S is the set of coordinate functions of the code and A^* is the space of all linear functionals defined on the code. Since m is necessarily at least k, it follows that

$$d \leqslant n - k + 1, \tag{1}$$

where d is the minimum distance. This bound has been generalized [11, 29] to

$$n \geqslant \sum_{i=0}^{k-1} \left[\frac{d + q^i - 1}{q^i} \right] \tag{2}$$

in the case $F = GF(q)$.

The *square-root bound* for cyclic codes is the following: Suppose $x^n - 1 = (x - 1)\, g_1(x)\, g_2(x)$ over F, where $g_1(x)$ and $g_2(x)$ both have degree $(n - 1)/2$. Suppose also that the codes A and B having $g_1(x)$ and and $g_2(x)$, respectively, as generator polynomials have the same minimum weight d (as we shall see is often the case). Furthermore, if the minimum weight vectors, as polynomials,

$$m(x) = \sum_{i}^{d} a_i x^{e_i} \qquad \text{and} \qquad \sum_{i}^{d} b_i x^{f_i} = m_1(x),$$

are not multiples of $x - 1$, it follows that $m(x)\, m_1(x)$ is a scalar multiple of $x^{n-1} + x^{n-2} + \cdots + 1$. This implies $d^2 \geqslant n$. It is sometimes possible to choose $f_i \equiv -e_i \pmod{n}$, and then we get $d(d - 1) \geqslant n - 1$.

If A and B are (n, k) and $(n, n - k)$ codes orthogonal to each other over $GF(q)$, and A_i, B_i denote the number of vectors of A, B of weight i, then MacWilliams has proved [20] that

$$\sum_{i=0}^{n-\nu} A_i \binom{n - i}{\nu} = q^{k-\nu} \sum_{i=0}^{\nu} B_i \binom{n - i}{n - \nu}, \qquad \nu = 0, 1, \ldots, n. \tag{3}$$

These MacWilliams identities are basic to our main result, Theorem 4.2.

2. Optimal Codes

Motivated by the inequality (1), we call an (n, k) code *optimal* if $d = n - k + 1$. The $(n, 1)$ code $\{(\alpha, \alpha, \ldots, \alpha);\ \alpha \in \mathrm{GF}(q)\}$ is optimal, and the main result of this section is that "almost all" cyclic codes of prime length are optimal.

Let l be prime and consider all the cyclic codes of length l over $\mathrm{GF}(l) = F$. Since $x^l - 1 = (x - 1)^l$ over F, these codes, considered as ideals in $F[x]/(x^l - 1)$, are the ideals $A_i = ((x - 1)^i)$ for $i = 0, 1, \ldots, l$. Thus they satisfy

$$(1) = A_0 \supsetneq A_1 \supsetneq \cdots \supsetneq A_l = (0).$$

The dimension of A_i is $l - i$. The minimum weight in A_i is easy to

determine directly: If $f(x)$ is a minimum-weight polynomial in A_i, $i = 1,..., l-1$, cycled so that the constant term is not 0, then the ordinary derivative $f'(x)$ is a vector in A_{i-1} with weight 1 less than that of $f(x)$. Therefore, if d_i denotes the minimum weight in A_i, we have

$$1 = d_0 < d_1 < \cdots < d_{l-1} = l,$$

since we have $d_0 = 1$ and $d_{l-1} = l$ by inspection. Therefore $d_i = i + 1$ for $i = 0, 1,..., l-1$, and $(x-1)^i$ is a minimum-weight vector. We have proved

LEMMA. *The cyclic (l, k) codes of prime length l over* GF(l) *are all optimal.*

THEOREM 2.1. *Let l be prime and let z be a primitive l-th root of* 1 *over the rational field Q. Let E be any subfield of $K = Q(z)$ and let A be a cyclic (l, k) code over E. Then the minimum weight of A is $l - k + 1$.*

PROOF: The module consisting of all code-vectors of A with coordinates in $\mathcal{O}$, the integers of E, has the same minimum weight that A has. The ideal $\mathcal{O}l$ is a power of principal prime ideal, of $\mathcal{O}$, of degree 1. If we reduce by the residue-class map of this prime ideal we obtain a cyclic (l, k) code over GF(l), which, by our lemma, has minimum weight $l - k + 1$. If d denotes the minimum weight of A, then $d \leqslant l - k + 1$, in general; and we have just proved $d \geqslant l - k + 1$, since there are minimum weight code-vectors in the module not all coordinates of which are in the principal prime ideal.

COROLLARY. *Any proper divisor of $x^l - 1$ over $Q(z)$ has all coefficients non-*0.

REMARKS. 1. Enlarging the base field E preserves the optimality in view of the result in Section 1 on tensor products.

2. This theorem furnishes a simple indirect proof of the following: Let $r = [K : E]$. Then every set of r distinct powers of z is linearly independent over E. We can even conclude from the present theorem that *every subdeterminant of the $l \times l$ determinant (z^{ij}) is non-vanishing.* We do this by first considering an arbitrary (l, k) cyclic code over K given recursively by

$$(x - z^{e_1}) \cdots (x - z^{e_k}), \qquad 0 \leqslant e_i < l,$$

the e_i's distinct modulo l. This code consists of the space $K \times \cdots \times K$ (k times) and the coordinate functions f_j defined by

$$(c_1, ..., c_k) f_j = c_1 z^{e_1 j} + \cdots + c_k z^{e_k j},$$

$c_1, \ldots, c_k \in K$, $j = 0, 1, \ldots, l-1$. That is, it is the direct sum of the codes

$$(c_i, c_i z^{e_i}, c_i z^{2e_i}, \ldots, c_i z^{(l-1)e_i}) \qquad \text{for} \quad i = 1, \ldots, k.$$

By Theorem 2.1 and the preceding remark, this code has optimal minimum weight. Therefore every set of k coordinate functions is linearly independent over K. But if for some k choices of j, say $t_1, \ldots, t_k$, the determinant $| z^{e_i t_j} |$ vanished, then it would follow that $f_{t_1}, \ldots, f_{t_k}$ were linearly dependent over K.

THEOREM 2.2. *Let l be a prime. Then for all but a finite number of primes p, each cyclic code of length l over* GF(p^i) *is optimal (for all i).*

PROOF: A cyclic (l, k) code over GF(q) is optimal if and only if every $k \times k$ determinant in (ζ^{je_i}), for $i = 1, \ldots, k$, and $j = 0, \ldots, l-1$, is non-vanishing, where the code is defined recursively by

$$(x - \zeta^{e_1}) \cdots (x - \zeta^{e_k}).$$

Such determinants are the images under residue-class maps of the non-vanishing global determinants in (z^{je_i}). These determinants are non-0 integers in K and are, therefore, divisible by only a finite number of primes. Q.E.D.

We have proved the following result for the linear case [1], and it has also been proved more generally, in [27] and implicity in [26], which note a connection with latin squares. We omit the proof here.

THEOREM 2.3. *If an (n, k) code over* GF(q) *is optimal, then*

$$q - 1 \geqslant \min\{k, n - k\}.$$

Furthermore, if $1 < k < n - 1$ (i.e., if this minimum is at least 2), then $q - 1 \geqslant \max\{k, n - k\}$.

We note that the conclusion of this theorem is not sufficient to give an optimal code. For example, one could extend the coefficient-field of any non-optimal code.

3. ON AUTOMORPHISM GROUPS OF CODES

In this section we prove a basic result due to Gleason and Prange on the automorphism group of an extended quadratic-residue code, to be defined. We will then find some corollaries on weights in codes.

An *invariance* of a code (A, S) is a linear transformation σ of A onto A such that for each f in S, $\sigma f = \alpha g$ for some scalar α (depending on f) and some g in S. That is, σ is a monomial matrix which preserves the code-space. An invariance preserves the weight of each code-vector. For example, the cyclic shift is an invariance of a cyclic code.

The *automorphism group* of the code is the group of all invariances modulo scalar multiplications. In this report we are mainly concerned with the permutation aspects of the automorphism group, so we remark that the mapping which sends each invariance to its underlying permutation is a homomorphism of the invariance group which sends the scalar multiplications to the identity permutation; therefore, we shall often speak of this or that permutation group as being "contained in" the automorphism group of the code.

We now prove that the projective unimodular group $\mathrm{PSL}_2(l)$ is "contained in" the automorphism group of the extended quadratic-residue codes, defined below.

Let l be an odd prime and let z be a primitive l-th root of unity over the field Q of rational numbers. Let $K = Q(z)$ be the cyclotomic field of all l-th roots of 1 over Q. Then K/Q is a cyclic extension of degree $l - 1$, and K contains a unique subfield L of degree 2 over Q. L is, in fact, generated by $\eta = \sum z^r$, the sum being taken over the quadratic residues r modulo l, since $\eta = T_{K/L}(z)$[2]. The irreducible polynomial for η over Q is

$$x^2 + x + (1 \pm l)/4,$$

where the sign is chosen to make $(1 \pm l)/4$ an integer. Thus $L = Q(\sqrt{\pm l})$, and the sign is that in $l \equiv \pm 1 \pmod 4$. The polynomial $x^{l-1} + \cdots + 1$, which is irreducible over Q, splits into $g_1(x)\, g_2(x)$, irreducibles of degree $(l - 1)/2$ over L. There are cyclic $(l, (l \pm 1)/2)$ codes over L denoted as follows:

A, recursive for $g_1(x)$, generated as ideal by $(x - 1)\, g_2(x)$.

A^+, recursive for $(x - 1)\, g_1(x)$, generated as ideal by $g_2(x)$.

B and B^+ are defined by interchanging $g_1(x)$ and $g_2(x)$ above. These are called *global quadratic-residue codes*, since

$$g_1(x) = \prod_{r \in R} (x - z^r), \qquad g_2(x) = \prod_{s \in R'} (x - z^s),$$

where R and R' are, respectively, the quadratic residues and non-residues modulo l.

A and B have the same weight distributions (so do A^+ and B^+), because

[2] $T_{K/L}$ denotes the trace from K to L.

the permutation of coordinates sending i to si for each $i = 0, 1, \ldots, l-1$ for any fixed quadratic non-residue s modulo l interchanges the two codes.

As Gleason [9] and Prange [25] observed in the finite case, these codes can be embedded in spaces of $l+1$ dimensions in a nice way, which allows the projective unimodular group to act. We now carry over Prange's construction to the present global situation.

We first embed the codes. The coordinates functions for A^+ are the $f_j : L \times K \to L$ defined by

$$(c_0, c)f_i = c_0 + T_{K/L}(cz^i) \qquad c_0 \in L, \quad c \in K,$$

$i = 0, 1, \ldots, l-1$. Similarly for B, with z replaced by z^s for some fixed $s \in R'$. A is the subcode of A^+ given by restricting the f_i to $0 \times K$, i.e., by setting $c_0 = 0$. A will embed as a subcode of A^+ so we define the embedding for A^+. We will introduce a new coordinate function

$$f_\infty = \gamma \sum_{i=0}^{l-1} f_i$$

for some $\gamma \in L$ to be chosen so that the new code, called A_∞, will be orthogonal to itself or to the corresponding new code B_∞ for B^+. A_∞ and B_∞ are called *extended quadratic-residue codes*. For convenience, we denote vectors of A_∞ by $\langle c_0, c\rangle = (\ldots, (c_0, c)f_i, \ldots)$ for $c_0 \in L$ and $c \in K$.

Observe that $(c_0, c)f_\infty = \gamma l c_0$; letting f_i' and f_∞' be the coordinate functions for B_∞ with $f_\infty' = -\gamma \sum f_i'$, we obtain $(c_0, c)f_\infty' = -\gamma l c_0$.

A now also denotes the subcode of A_∞ with "infinite" coordinate equal to 0.

Orthogonality depends on the congruence of l modulo 4. The results are summarized here before embedding:

$l \equiv -1 \pmod 4$	$l \equiv +1 \pmod 4$
$A^\perp = A^+$	$A^\perp = B^+$
$B^\perp = B^+$	$B^\perp = A^+$

Thus, after embedding, we have

$$A_\infty{}^\perp = \begin{cases} A_\infty, & l \equiv -1 \pmod 4, \\ B_\infty, & l \equiv +1 \pmod 4, \end{cases}$$

provided only that $\langle 1, 0\rangle = (1, 1, \ldots, 1; l\gamma)$ is orthogonal to itself or to the corresponding vector in B_∞, which is to say

$$\begin{aligned} 1 + l\gamma^2 &= 0, \qquad l \equiv -1 \pmod 4, \\ 1 - l\gamma^2 &= 0, \qquad l \equiv +1 \pmod 4, \end{aligned} \tag{1}$$

Thus γ is determined up to sign as $1/\sqrt{\pm l}$, which is in L as it should be.

The invariance group of A_∞ obviously contains the cyclic shift τ on the "finite" f_i (τ fixes f_∞); similarly for B_∞. It also contains the Galois automorphisms ρ_r, which send f_i to f_{ri}, $i = 0,..., l-1$; $r \in R$; these also fix f_∞.

We now prove that a certain interchange of f_0 and f_∞ is an invariance σ of A_∞; also, the permutation parts of σ, τ^i, and ρ_r generate the (one-dimensional) projective unimodular group over GF(l). The same will hold for B_∞. (The projective unimodular group, $\mathrm{PSL}_2(l)$, is the group of all 2×2 matrices over GF(l) with determinant 1 modulo the center $\pm\left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right)$. Element of this group can be factored as follows:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & a/c \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} c & d \\ 0 & 1/c \end{pmatrix}$$

provided $c \neq 0$. This uses $ad - bc = 1$.)

We define σ as follows: As permutation on the coordinate functions, σ sends f_i to $f_{-1/i}$ (subscripts modulo l), interchanging f_0 and f_∞. Signs are introduced via the Legendre symbol; thus $\sigma f_i = \epsilon_i f_{-1/i}$, where $\epsilon_i = (i/l)$ $i = 1,..., l-1$. We shall choose ϵ_0 and ϵ_∞ later, as ± 1. Thus

$$(a_0 ,..., a_{l-1} ; a_\infty)\sigma = (\epsilon_0 a_\infty ,..., \epsilon_i a_{-1/i} ,..., \epsilon_\infty a_0).$$

We must prove that, with proper choice of ϵ_0 and ϵ_∞, σ maps A_∞ onto itself and also that this σ maps B_∞ onto itself.

CASE 1: $l \equiv -1 \pmod 4$. Since $A_\infty = L\langle 1, 0\rangle \oplus A$, it suffices to show $\langle 1, 0\rangle \sigma \in A_\infty$ and $A\sigma \subset A_\infty$. Thus

$$\langle 1, 0\rangle \sigma = (1, 1,..., 1; l\gamma)\sigma = (\epsilon_0 l\gamma ,..., \epsilon_i ,..., \epsilon_\infty);$$

and therefore

$$\langle 1, 0\rangle \sigma^2 = (\epsilon_0\epsilon_\infty , -1,..., -1; \epsilon_0\epsilon_\infty \gamma l)$$

since $\epsilon_i\epsilon_{-1/i} = (-1/l) = -1$. This vector obviously cannot be in A_∞ unless $\epsilon_0\epsilon_\infty = -1$. Thus we choose

$$\epsilon_\infty = -\epsilon_0 = -\epsilon. \tag{2}$$

Now $\langle 1, 0\rangle\sigma$ is in A_∞ if and only if it annihilates A_∞ under the usual dot-product. This means that we must find

$$\epsilon\gamma l + \sum_1^{l-1} \epsilon_i - \epsilon\gamma l = 0$$

as is indeed the case; and also we need $\langle 1, 0\rangle\sigma \perp \langle 0, c\rangle$ for all $c \in K$. That is, we must also have

$$(\epsilon l\gamma,..., \epsilon_i ,...; -\epsilon) \cdot (T(c),..., T(cz^i),...; 0) = 0,$$

or

$$\epsilon l\gamma T(c) + \sum_{r\in R} T(cz^r) - \sum_{s\in R'} T(cz^s) = \epsilon l\gamma T(c) + (\eta - \eta')\, T(c) = 0,$$

where $\eta = \sum z^r (r \in R)$ and $\eta' = \sum z^s (s \in R')$, and we make use of the L-linearity of T, which denotes the trace from K to L here. Thus σ maps A_∞ onto A_∞ if and only if ϵ and γ are chosen so that

$$\epsilon l\gamma + \eta - \eta' = 0. \tag{3}$$

Now from (1), $(\gamma l)^2 = -l$, so $l\gamma = \pm\sqrt{-l}$, and $\eta - \eta'$ is also either $\sqrt{-l}$ or $-\sqrt{-l}$, so ϵ must be taken as ± 1. The choice depends on the choice of notation for $g_1(x)$ and $g_2(x)$. We chose z to be a root of $g_1(x)$; thus η is the negative of the coefficient of $x^{(l-3)/2}$ in $g_1(x)$. Thus the choice of notation determines the sign of $\epsilon\gamma$, and we are free to choose $\epsilon = 1$ or $\epsilon = -1$. (For the code B, z is replaced by a root of $g_2(x)$, interchanging η and η' in (3); hence the choice $-\gamma$ for B.)

We now show that $\langle 0, c\rangle\sigma \perp A_\infty$ for all $c \in K$. Now

$$\langle 0, c\rangle\sigma = (0,..., \epsilon_i T(cz^{-1/i}),...; -\epsilon T(c)) = (a_0 , a_1 ,...; a_\infty)$$

is in A_∞ if and only if the polynomial $\sum a_i x^i$ is a multiple of $g_1(x)$, since

$$\gamma \sum_0^{l-1} a_i = \gamma(\eta' - \eta)\, T(c) = \epsilon l\gamma^2 T(c) = -\epsilon T(c),$$

from (2) and (1). Now $g_1(x)$ is irreducible and has z as a root; therefore $\langle 0, c\rangle\sigma \in A_\infty$ if and only if the quantity $D(c) = 0$ for all $c \in K$, where $D(c)$ is defined as

$$D(c) = \sum_1^{l-1} \epsilon_i T(cz^{-1/i})\, z^i.$$

If τ is any automorphism of K/Q, such that $z^\tau = z^t$, then

$$D(c)^\tau = \epsilon_t D(c^{\tau^{-1}}),$$

as one can easily verify using $T(c)^\tau = T(c^\tau)$. Since D is linear and $z, z^2,\ldots$ span K/L, it suffices to prove $D(z) = 0$. Now,

$$D(z) = \sum_{1}^{l-1} \epsilon_i T(z^{1-1/i})\, z^i$$

$$= \sum_{i=1}^{l-1} \epsilon_i \sum_{r \in R} z^{r(1-1/i)}\, z^i$$

$$= \sum_{i,r} \epsilon_i z^{r-r/i+i}.$$

This is a polynomial in z of degree at most $l - 1$ with integral coefficients. For each $k = 0, 1,\ldots, l - 1$ we find the coefficient of z^k as $\sum_{r,i} \epsilon_i$, where i rns over the solutions of $r - r/i + i \equiv k \pmod{l}$. These i are the same as those for which $i^2 + (r - k)\, i - r \equiv 0 \pmod{l}$. The polynomial $x^2 + (r - k)\, x - r$ never has double roots in GF(l) since the constant term is in R'. Thus for each value of k and r there are two distinct roots roots i and i'; one is in R, the other R'. Thus the polynomial in z is identically 0. This completes the proof that σ maps A_∞ onto itself.

PROPOSITION 3.1. *Let* $l \equiv -1 \pmod 4$. *If we embed* A *with* γ *and* B *with* $-\gamma$, *then there is a choice of* $\epsilon = \pm 1$, *given in* (3), *such that* σ *maps each of* A_∞ *and* B_∞ *onto itself.*

CAUTION. We have defined σ monomially on L^{l+1}. $L \times K$ is embedded in L^{l+1} in distinct ways as A_∞ and B_∞. The linear transformations of $L \times K$ induced by σ are distinct.

CASE 2. $l \equiv +1 \pmod 4$. We must use γ to embed A and $-\gamma$ to embed B in order to make $A_\infty{}^\perp = B_\infty$ in this case, where $l\gamma^2 = 1$. We define σ as before and find $\langle 1, 0\rangle\, \sigma^2 \in A_\infty$ if and only if $\epsilon_0 \epsilon_\infty = 1$. We take

$$\epsilon = \epsilon_0 = \epsilon_\infty = \pm 1. \tag{4}$$

Now $\langle 1, 0\rangle \sigma$ is in A_∞ if $\langle 1, 0\rangle \sigma$ annihilates B and the vector $\langle 1, 0\rangle$; the former happens if and only if, as before,

$$\epsilon\gamma l - (\eta - \eta') = 0. \tag{5}$$

Proceeding as in Case 1 we can verify that γ and ϵ are related by (5).

If we ask whether this same σ maps B_∞ onto itself, then the part relating to $\langle 1, 0\rangle$ goes through, since in (5) we replace γ by $-\gamma$ and interchange

η and η'. The rest goes through too; the part involving $D(c)$ is formally the same. We have proved

PROPOSITION 3.2. *If $l \equiv +1 \pmod 4$ and we use γ to embed A, $-\gamma$ to embed B, then A_∞ and B_∞ are orthogonal to each other and σ maps each onto itself. ϵ and γ are chosen by* (4) *and* (5).

We are equally interested in the finite codes obtained from A_∞ and B_∞ by mapping the integral submodules of these via the residue-class maps of primes in L lying over the rational prime p. These codes we denote by A_p (or B_p); they are *finite, extended quadratic-residue codes* of type $(l + 1, (l + 1)/2)$ over GF(q), where $q = p$ or p^2 depending on whether p is or is not a quadratic-residue modulo l.

Note that, when $(p/l) = -1$, the codes A_p and B_p over GF(p^2) are conjugates of each other in that $(a_0, \ldots, a_{l-1}; a_\infty) \in A_p$ implies

$$(a_0^p, \ldots, a_{l-1}^p ; a_\infty^p) \in B_p .$$

This follows from the relations between the generator polynomials $g_1(x)$ and $g_2(x)$ and the embedding chosen. In this case one can, by allowing semilinear transformations, cause $\mathrm{PGL}_2(l)$ to act on the codes A_p and B_p.

In the sequel we often refer for short to "the" $[l + 1, (l + 1)/2]$ code over GF(p) (or p^2), by which we mean the code A_p or B_p just defined; because of their equivalence under a monomial transformation, it usually does not matter which one we consider.

With Propositions 3.1 and 3.2 we have essentially proved

THEOREM 3.1. *The automorphism groups of the two extended quadratic-residue codes A_∞ and B_∞ each contain a subgroup of which the permutation part is precisely* $\mathrm{PSL}_2(l)$. *The same statement holds for the finite codes A_p and B_p.*

PROOF: We have proved this in the global case. Formally the same proof works in the finite case; or one can project the group generated by the invariances ρ_τ, τ, and σ defined globally above (the permutations of which generate $\mathrm{PSL}_2(l)$ by the residue-class map, noting that all scalars involved in the definitions of these invariances are ± 1.

COROLLARY. *The minimum distance in A^+ is* 1 *less than in A; the same for the corresponding finite codes over any* GF(q) *for which $(q/l) = +1$. In particular, the square-root bound holds for these codes.*

Gleason has also proved Theorem 3.1 by means of induced representations, and M. Hall, Jr., has proved essentially this result, but stated for Paley-Hadamard matrices [12, Theorem 2.1] for the case $l \equiv -1 \pmod 4$.

When $l \equiv -1 \pmod 4$ we can use the self-orthogonality of A_∞ and B_∞ to get some results on the weight distributions of these codes over GF(2) and GF(3).

THEOREM 3.2. *Let* $l \equiv -1 \pmod 4$. *If* $(2/l) = +1$, *then* A_2 *and* B_2 *have all weights divisible by* 4. *If* $(3/l) = +1$, *then* A_3 *and* B_3 *have all weights divisble by* 3.

PROOF: $p = 2$. Since 2 is in R, the set of quadratic-residues modulo l, l must be $8N - 1$. Then the weight-$4N$ vector $a = (a_i)$ with $a_i = 1$ for $i \in R$ and $i = \infty$, and with $a_i = 0$ otherwise, is in A_2; and, moreover, the cyclic shifts of a span A_2 (facts established by simple polynomial arguments). Since A_2 is self-orthogonal, any two code-vectors must have an even number of places with 1's in common; this implies that any sum of shifts of a has weight divisible by 4. (A. M. Gleason was the first to observe this.)

In the GF(3) cases the matter is very simple. Each vector $(a_0, \ldots, a_{l-1}; a_\infty)$ is in particular orthogonal to itself, so

$$a_\infty^2 + \sum_0^{l-1} a_i^2 = 0.$$

But the non-0 a's are ± 1, so their number must be a multiple of 3.

COROLLARY. *The extended* (24, 12) *quadratic-residue code over* GF(3) *has minimum weight* 9.

PROOF: It is greater than 6 by the square-root bound and it is less than 12 by (2) of Section 1.

It is also true that the extended quadratic-residue codes over GF(4) for $l = 8N + 5$ have all weights even. Moreover, 2, 3, and 4 are the only values of q for which extended quadratic-residue codes can have "regular" gaps in their weight distributions [30]; for $q = 2$ one might have all weights even or multiples of 4, for $q = 3$ all weights may be multiples of 3, and for $q = 4$ all weight may be even; but no larger divisors are possible.

The special cases of the above for $l = 23$, $q = 2$ and $l = 11$, $q = 3$ are closely related to the Mathieu groups. For proofs that in the first case the automorphism group is M_{24}, and in the second case, M_{12}, the reader should consult [3].

4. Combinatorial Designs Associated with Certain Cyclic Codes

A *tactical configuration* of type λ; *t-d-n*, or *t-design*, is a collection $\mathscr{D}$ of d-subsets[3] of a given n-set S such that every t-subset of S is contained in precisely λ members of $\mathscr{D}$. Here λ is a positive integer; and $0 \leqslant t \leqslant d \leqslant n$, where if any equality obtains we call the design trivial. Balanced incomplete block designs are 2-designs with restrictions on d and n; where $\lambda = 1$ the t-design is called a *Steiner system*; Steiner triple systems are 1; 2-3-n tactical configurations; the lines of any projective space define a Steiner system on the points with $t = 2$, for example. Also, (v, k, λ) configurations are special cases of λ; 2-k-v designs.

The *automorphism group* of a t-design is the group of all permutations of S which map each member of $\mathscr{D}$ onto a member of $\mathscr{D}$.

For convenience we often call the members of $\mathscr{D}$ *clubs* or *d-clubs*. A t-design is automatically a t'-design for $t' < t$. Also, the clubs of a given λ; *t-d-n* design containing a fixed point P of S form a $(t - 1)$-design on $S - P$ when P is removed from these clubs. The new parameters are $\lambda; (t - 1) - (d - 1) - (n - 1)$.

The collection of *all* d-subsets of a given set is a t-design for any $t \leqslant d$, and no one has discovered any others for t larger than 5. Two essentially unique 5-designs, the Steiner systems associated with the Mathieu group M_{12} and M_{24}, have been known for many years, however; and recently [3, 14], two disjoint Steiner systems of these types were constructed, meaning that 2; 5-6-12 and 2; 5-8-24 designs exist (see also Section 6). Aside from these and such designs obtainable as certain orbits of M_{12} and M_{24} (see below), which have been at least implicitly known for a long time, no other non-trivial 5-designs were known until recently. The main purpose of this section is to derive all of the above designs, except perhaps for some of the "orbit-designs" just mentioned, and several new 5-designs which are not "orbit-designs," by means of coding theory. Another purpose is to exhibit two infinite classes of 3-designs (Theorem 4.1 and Application (3)).

Such designs can arise from codes as follows. From a given code consider the set of all vectors of a certain weight w. For each such vector consider the set D of all coordinate places at which the vector is not 0. D is thus said to *hold* a code-vector of weight w. For certain codes and certain values of w, the collection of all such sets D forms a t-design for t as high as 5. For example, we showed this for $t = 5$ for the minimum-weight vectors of the finite extended quadratic-residue codes of type (24, 12) over GF(2) and (12, 6) over GF(3) by direct special methods in [3]. In different terms this was also done for the (23, 12) and (11, 6) codes for

[3] An x-set is a set of cardinality x.

$t = 4$ by Paige [21].[4] We shall derive these and all the other cases as applications of Theorem 4.2 below.

We begin with the following simple remark.

PROPOSITION. *A code is optimal if and only if the minimal-weight vectors yield a trivial design.*

PROOF: Suppose it is an (n, k) code of minimum weight d, such that every d-subset of coordinate places holds a code-vector. We wish to prove that $d = n - k + 1$. Consider the subcode C spanned by the minimum-weight vectors: the orthogonal code to C has every subset of d coordinate-functions linearly dependent, but no subset of size $d - 1$ with this property; it therefore has dimension $d - 1$, so that C has dimension $n - (d - 1) \leqslant k$. The reverse inequality holds in general, by (1) of Section 2.

Conversely, if $d = n - k + 1$, then every k coordinate functions are linearly independent. Given a d-subset of coordinate functions, we consider the $n - d = k - 1$ functions of the complementary subset. The intersection of the kernels of these is non-0; a non-0 vector in it must have weight at most d and hence d. Q.E.D.

The following result is an immediate consequence of Theorem 3.1 and the fact that the action of $\mathrm{PSL}_2(l)$ on the projective line is 2-fold transitive, in general, and 3-set transitive when $l = 4N - 1$. Also, $\mathrm{PGL}_2(l)$ is 3-fold transitive and acts on $A_\infty \cup B_\infty$; in the case $(p/l) = -1$, since for a given weight the design from A_p is the same as that for B_p, this implies that $\mathrm{PGL}_2(l)$ acts on these designs.

THEOREM 4.1. *The finite extended quadratic-residue codes of length $l + 1$ yield 2-designs for all l and 3-designs when $l \equiv -1 \pmod 4$, from every weight class of code-vectors. Also, in all cases the union of A_p and B_p yields 3-designs from each weight class; when $(p/l) = -1$, each code yields the same 3-design.*

REMARK. In view of the proposition above and Theorem 2.3, we see that the minimum weight vectors in A_p always yield a non-trivial design (on which $\mathrm{PSL}_2(l)$ acts) whenever $q - 1 < (l + 1)/2$. (Recall that $q = p$ or p^2 depending on whether p is a quadratic residue modulo l or not.) In particular then, A_2 yields a non-trivial design whenever $l > 5$ and, of course, $d \leqslant (l + 1)/2$, $d(d - 1) \geqslant l - 1$. The determination of d seems to be, in general, a difficult problem.

[4] These are the designs having Mathieu groups as automorphism groups (see Witt [31]).

Let A and B be linear orthogonal (n, k) and $(n, n-k)$ codes over GF(q) with minimum weights d and e. Let t be an integer less than d. Let v_0 be the largest integer satisfying

$$v_0 - \left[\frac{v_0 + (q-2)}{q-1}\right] < d,$$

and w_0 the largest integer satisfying

$$w_0 - \left[\frac{w_0 + (q-2)}{q-1}\right] < e,$$

where, if $q = 2$, we take $v_0 = w_0 = n$. Then two vectors of A with weight at most v_0 having their non-0 coordinates in the same places must be scalar multiples of each other, and the same for B. This property is essential to our method of proof of our main result,

THEOREM 4.2. *Suppose that the number of non-0 weights of B which are less than or equal to $n - t$ is itself less than or equal to $d - t$. Then, for each weight v with $d \leqslant v \leqslant v_0$, the vectors of weight v in A yield a t-design, and for each weight w with $e \leqslant w \leqslant \min\{n - t, w_0\}$, the vectors of weight w in B yield a t-design.*

Before proving the above result we remark that for B we will in fact show that for each weight w, with $e \leqslant w \leqslant \min\{n - t, w_0\}$, the vectors of weight w yield blocks the complements of which form a t-design. We will need the following combinatorial

LEMMA. *Suppose $(S, \mathscr{D})$ is a t-design. Then, if T and T' are two t-subsets of S, and k an integer satisfying $0 \leqslant k \leqslant t$, we see that*

$$|\{D \in \mathscr{D};\ |\ D \cap T\ | = k\}| = |\{D \in \mathscr{D};\ |\ D \cap T'\ | = k\}|.$$

That is, the number of subsets in $\mathscr{D}$ intersecting a given t-subset in precisely k points is independent of the chosen t-subset.

PROOF: For $k = t$ the assertion is simply the condition that $(S, \mathscr{D})$ is a t-design. Now we use induction downward observing that for $K \subseteq T$, $|\ K\ | = k$, we see that

$$|\{D \in \mathscr{D};\ K \subseteq D\}| = \frac{\lambda \binom{n-k}{t-k}}{\binom{d-k}{t-k}} = \lambda_k,$$

where $(S, \mathscr{D})$ has parameters λ; $t - d - n$, and hence that

$$|\{K, D); K \subseteq D, K \subseteq T, |K| = k\}| = \binom{t}{k} \lambda_k .$$

Then an inclusion-exclusion argument yields the result.

COROLLARY. *The complement of a t-design is a t-design.*

(Here, if $(S, \mathscr{D})$ is a t-design, then its complement is $(S, \{S - D; D \in \mathscr{D}\})$. Of course, if $n - d < t$ it is trivially so.) Complementary t-designs have parameters λ; $t - d - n$ and λ'; $t - (n - d) - n$, where

$$\lambda' = \lambda \binom{n-d}{t} \div \binom{d}{t}.$$

PROOF OF THE THEOREM: If T is a coordinate set with $|T| = t$ we denote by A^T the code of length $n - t$ obtained by neglecting the coordinates in T. We denote by $B^{0@T}$ the code of length $n - t$ obtained from the vectors in B which have 0's at the coordinates in T by neglecting those coordinates. Clearly, $A^T \perp B^{0@T}$. Since every $n - d + 1$ coordinate functionals of A span and $t < d$, A^T is an $(n - t, k)$ code. Since the vectors of A are the relations on the functionals of B and $t < d$, the functionals corresponding to the coordinates in T are linearly independent and $B^{0@T}$ is an $(n - t, n - k - t)$ code. Thus, A^T and $B^{0@T}$ are orthogonal. Let $0 < v_1 < v_2 < \cdots < v_{d-t} \leqslant n - t$ be the possible non-0 weights less than or equal to $n - t$ appearing in B. Then the only non-0 weights appearing in $B^{0@T}$ are among $v_1, \ldots, v_{d-t}$. The minimum weight in A^T is at least $d - t$.

The MacWilliams relations for A^T and $B^{0@T}$ determine the number of vectors of each of these weights uniquely in terms of n, t, q, and k via $d - t$ equations

$$\sum_{j=v_1,\ldots,v_{d-t}} \binom{n-t-j}{\mu} x_j = q^{n-t-k-\mu} \binom{n-t}{\mu} - \binom{n-t}{\mu},$$

$\mu = 0, 1, \ldots, d - t - 1$, since the determinant of the coefficients is essentially Vandermonde. Since the weight distribution alone of a code determines that of the orthogonal code, again from MacWilliams [20], the weight distributions of A^T and $B^{0@T}$ are independent of the particular t-subset, T, chosen.

We now turn to the assertion concerning the t-designs which B yields. Suppose v is a weight in B satisfying $v \leqslant w_0$, $v \leqslant n - t$. If b and b' are two vectors of B of weight v with their non-0 coordinates at the same

coordinate set, then, since $v \leqslant w_0$, b' is a scalar multiple of b. Consider the collection $\mathscr{E}_v$ of coordinate v-subsets holding vectors of weight v in B. Let $\mathscr{E}'_v$ be the set of complements. By the corollary to the lemma, to show that $\mathscr{E}_v$ is a t-design, it is enough to show that $\mathscr{E}'_v$ is. But, for a given t-set T, the number of subsets in $\mathscr{E}'_v$ containing T is $1/(q-1)$ times the number of vectors in $B^{0(2)T}$ of weight v, and this number, by the above, is independent of which t-subset, T, is chosen.

The similar assertion for A is a bit more complicated to prove and we must apply the full lemma. We start with $w = d$, which certainly satisfies $w \leqslant v_0$. As before, any two vectors of A of weight w held by the same coordinate set are scalar multiples of one another. Let $\mathscr{D}_w$ be the collection of coordinate w-subsets holding vectors of weight w in A. The number of subsets in $\mathscr{D}_w$ containing a given t-subset T is $1/(q-1)$ times the number of vector of weight $d-t$ in A^T and this, again, is independent of which t-subset, T, is chosen. We proceed by induction. So suppose we know the assertion of the theorem for $w' < w$ where $w \leqslant v_0$. With $\mathscr{D}_w$ as before, we know that the number of subsets in $\mathscr{D}_w$ containing a given t-subset, T, is $1/(q-1)$ times the number of vectors in A^T of weight $w-t$ which come from vectors of weight w in A. Now, the total number of weight $w-t$ in A^T is independent of T and it follows immediately from the lemma and the induction assumption that the number of vectors of weight $w-t$ in A^T coming from vectors of weight less than w in A is independent of T. Thus, $\mathscr{D}_w$ yields a t-design. This concludes the proof of the Theorem.

APPLICATIONS OF THE THEOREM. (1) Suppose A is a perfect code over GF(q) with minimum weight d. Then d is necessarily odd and the number of non-0 weights in its orthogonal complement is at most $(d-1)/2$ [10, 18]. Thus, we can take $t = (d+1)/2$ and the theorem yields t-designs (cf. [6, Theorem 1]).

MacWilliams [19] has shown that a necessary and sufficient condition for A to be perfect is that its orthogonal complement have precisely $(d-1)/2$ non-0 weights. Our methods yield part of this result for GF(2), namely, that a perfect linear code over GF(2) has at least $(d-1)/2$ distinct non-0 weights in its orthogonal code: Let $d = 2e+1$. If there were fewer than e weights, the theorem would yield an $(e+2)$-design from the minimum-weight vectors of the perfect code. In general there are

$$(q-1)^{e-1}\binom{n}{e+1}\Big/\binom{d}{e+1}$$

such vectors in the code, because the parameters of the $(e+1)$ design are known (see [6]); this means that for the $(e+2)$ design λ would be

$(q-1)^e e/(n-e-1)$. When $q=2$, this cannot be an integer unless $n=d$, implying that the code is $\{(0\cdots 0),(11\cdots 1)\}$, which does have exactly e distinct non-0 weights in its orthogonal code and which yields a trivial 1; t-n-n design for all t. This proof cannot work in general, however, because the perfect (11, 6) code over GF(3) (see Section 4) having $d=5$ yields a 3-design by the theorem, but also yields in fact a 4-design, a 1; 4-5-11 Steiner system.

(2) We now derive well-known 5-designs and several new 5-designs by applying Theorem 4.2 to certain extended quadratic-residue codes.

(a) 5-*designs on* 12 *points*. Consider the (12, 6) code over GF(3). This code is self-orthogonal and has vectors of weights 0, 6, 9, and 12 only. Thus for $t=5$ there is only one non-0 weight less than $7=12-5$, and $d-t=6-5=1$. Therefore, the theorem yields a λ; 5-6-12 design as the 6-subsets of coordinate places holding code-vectors. The weight distribution shows now that $\lambda=1$, because there are 4.66 weight-6 vectors and, for a λ; t-d-n design obtained in this way, we have

$$\lambda\binom{n}{t}=\frac{N}{q-1}\binom{d}{t},$$

where N is the number of code-vectors of weight d.

For this code the weight-9 vectors also yield a design, but it is the trivial design since all 9-subsets arise in this way. This follows simply from the way $\mathrm{PSL}_2(11)$ acts.

The 1; 5-6-12 design is the well-known Steiner system having the Mathieu group M_{12} as automorphism group; M_{12} is also the automorphism group of the code [3, Section 4].

(b) 5-*designs on* 24 *points*. Consider first the (24, 12) code over GF(2). This again is self-orthogonal, with non-0 weighs 8, 12, 16, and 24. With $t=5$ we find three weights less than or equal to $24-5=19$ and $d-t=3$. Therefore, since $q=2$ we have 5-designs of 8-, 12-, and 16-subsets as follows:

$$\begin{aligned} 1;&\quad 5-8-24,\\ 48;&\quad 5-12-24,\\ 78;&\quad 5-16-24. \end{aligned}$$

These λ's are calculated from the weight distribution, which appears in [23, p. 70]. Note that the first and third of these are complementary designs and the second of these is self-complementary, because of the presence of the all-1 vector in the code. Again, the 1; 5-8-24 design is the well-known Steiner system having the Mathieu group M_{24} as auto-

morphism group, and the code also has M_{24} as automorphism group [3, Section 5].

Second, consider the (24, 12) code over GF(3). It is self-orthogonal with non-0 weights 9, 12, 15, 18, 21, and 24. For $t = 5$ there are four weights below 19 and $d - t = 4$. Thus we get some new 5-designs from the 9-, 12-, and 15-subsets holding code-vectors, namely:

$$\begin{aligned} 6; &\quad 5 - 9 - 24, \\ 2^6 \cdot 3^2; &\quad 5 - 12 - 24, \\ 2^2 \cdot 3 \cdot 5 \cdot 11 \cdot 13; &\quad 5 - 15 - 24. \end{aligned}$$

The first and third of these are not complementary, but we do not know whether the second design is self-complementary. The automorphism group of the 6; 5-9-24 design is not M_{24} but $PSL_2(23)$—hence the same for the code—a fact which will be proved later,

(*c*) *5-designs on* 48 *points*. The (48, 24) code over GF(2) has 8 non-0 weights: 12, 16, 20, 24, 28, 32, 36, and 48. It is self-orthogonal and $d = 12$. Thus again $d - 5$ is the number of weights less than or equal to $48 - 5$, so the theorem applies. From the weight distribution we find the following parameters for the resulting designs:

$$\begin{aligned} 2^3; &\quad 5 - 12 - 48, \\ 3 \cdot 5 \cdot 7 \cdot 13; &\quad 5 - 16 - 48, \\ 2^4 \cdot 7 \cdot 17 \cdot 19; &\quad 5 - 20 - 48, \\ 2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 227; &\quad 5 - 24 - 48. \end{aligned}$$

The code-vectors of weights 28, 32, and 36 form the 5-designs complementary to the first three of these. The last is self-complementary. We shall prove later that the automorphism group of each of these designs and of the (48, 24) code is $PSL_2(47)$.

The (48, 24) code over GF(3) has only 12 non-0 weights, namely, 15, 18, 21, 24,..., 48. Again Theorem 4.2 implies that the subsets of coordinate places holding vectors of weight 15, 18, 21, 24, and 27 each form 5-designs. Although we have used the equations (3) to calculate that there are no weight-12 vectors in the code having already shown [2, III.2] the absence of weight-9's, we have not calculated the weight distribution of this code. Therefore, we say only that there exist λ_i ; 5-3i-48 designs for $i = 5,..., 9$.

Note added in proof: $\lambda_5 = 4 \cdot 7 \cdot 13$, $\lambda_6 = 8 \cdot 7 \cdot 17 \cdot 53$, $\lambda_7 = 2{,}957{,}388$, $\lambda_8 = 71{,}307{,}600$, and $\lambda_9 = 749{,}999{,}640$. (We have also found 5-designs on 30 points from the (30,15) code over GF(4). The club sizes are 12, 14, and 16.) Though the code

has automorphism group $PSL_2(47)$, the designs may have a larger group.

There are more 5-designs obtainable as the orbits of subsets of sets on which 5-fold transitive groups act; but, as we have said, some of the above 5-designs are not obtainable in this way. As an example of such a 5-design, consider a 12-subset U of the 24 points on which M_{24} acts such that the stability subgroup in M_{24} of U is M_{12} (see [31, Satz 9]). Then the orbit of U under M_{24} is a 5-design on 24 points consisting of $|M_{24}| \div |M_{12}|$ 12-subsets; it is a 48; 5-12-24 design with M_{24} as automorphism group. It is not clear whether this is the same design as that under (b).

(3) Finally, we apply the theorem to the construction of 3-designs.

(a) *3-designs on 14 points.* Consider the (14, 7) quadratic-residue code over GF(4). The non-0 weights that appear are 6, 8, 12, 14. Both Theorems 4.1 and 4.2 produce 3-designs. The parameters are

$$5; \quad 3 - 6 - 14,$$
$$2 \cdot 3^2 \cdot 7; \quad 3 - 8 - 14.$$

(b) *3-designs on 2^k points, k odd.* Finding designs and their parameters via Theorem 4.2 depends on knowing the weight distributions of the code and its orthogonal. Pless and Prange [24] have computed these distributions for all the cyclic codes of length 31. For example, several (31, 21) cyclic codes over GF(2) yield the following designs and their complements (obtained by introducing a new coordinate equal the sum of all the others):

λ;	$3 - d - 32$
4;	6
119;	8
1,464;	10
10,120;	12
32,760;	14
68,187;	16

(plus the complements of these)

The orthogonal code yields these designs:

$$2 \cdot 4; \quad 3 - 12 - 32,$$
$$2 \cdot 136; \quad 3 - 16 - 32,$$
$$2 \cdot 76; \quad 3 - 20 - 32.$$

The designs of 16-clubs in both collections are self-complementary, and the designs of 12-clubs and 20-clubs from the orthogonal code are complements of each other. Also, the last three designs are each the union of two disjoint 2-designs.

These designs on 32 points are the first of an infinite class of 3-designs arising from a class of cyclic codes recently investigated by Solomon [28] and Kasami [16]. For each odd k, there are several $(2^k - 1, 2k)$ cyclic codes with the following (non-0) weight distribution:

weight w	N_w = number of code-vectors
2^{k-1}	$(2^k - 1)(2^{k-1} + 1)$
$2^{k-1} + 2^{(k-1)/2}$	$(2^k - 1)(2^{k-2} - 2^{(k-3)/2})$
$2^{k-1} - 2^{(k-1)/2}$	$(2^k - 1)(2^{k-2} + 2^{(k-3)/2})$

One can show that the orthogonal code to any of these codes has minimum distance 5 (for it must be odd and at least 5; if 7 the code would be perfect! The sphere-count condition for perfection, namely,

$$\sum_{0}^{3} \binom{n}{i} = 2^{2k},$$

where $n = 2^k - 1$, fails grossly for $k > 3$.) Using the MacWilliams relations, one could calculate the weight distribution of the orthogonal and find the λ's for the 3-designs obtained by introducing, as above, the new coordinate. For the $(2^k, 2k + 1)$ codes, the designs are of type $2N_w$; $3 - w - 2^k$, with w and N_w as above.

Kasami [16, Theorem 15] has also found, for odd $k \geqslant 5$, that a class of codes of type $(2^k, 3k)$ has only 5 non-0 weights less than 2^k. The orthogonal code has, in each of these cases, the same weight distribution as the extension of the intersection of three Hamming codes generated by the minimal polynomial of α, α^3, α^5, where α is a primitive element of GF(2^k); the well-known Bose-Chaudhuri and sphere-packing bounds then give minimum distance 8. Thus there is another infinite class of 3-designs, for which the parameters can be derived immediately from the weight distribution of the codes in [16].

(4) *Examples for small n.* Some 2- and 3-designs obtained from extended quadratic-residue codes are presented in Table I, along with the weight distributions of the codes. N_w stands for the number of code-vectors of weight w in the indicated $(n, n/2)$ code over GF(q); the entry λ; t in column w means that the code-vectors of weight w for that code yield a λ: t-w-n design.

TABLE I

	$w =$ 6	7	8	9	10	11	12	13	14		
N_w	330	396	495	1320	990	396	168			n	q
$\lambda; t$	10; 3	21; 3	42; 3							12	4
N_w	440	528	2640	2640	5544	2640	1192			12	5
$\lambda; t$	10; 3	21; 3									
N_w	182	156	364	364	546	364	182	0	28	14	3
$\lambda; t$	15; 2	18; 2	56; 2	72; 2	135; 2	110; 2	trivial				
N_w	102		153		153		102				
$\lambda; t$	10; 2		28; 2							18	2
$\lambda; t$*	5; 3		21; 3								

* These 3-designs are obtained from the union of the two disjoint quadratic-residue codes, on which the 3-set transitive $PGL_2(17)$ acts.

Another code which might repay investigation is the (60, 30) over GF(3). In order for Theorem 4.2 to produce a 5-design, the minimum distance would have to be 18. The (72, 36) code over GF(3) has a vector of weight 18, so the theorem gives no information on that case; similarly, computations by Prange rule out the $(l + 1, (l + 1)/2)$ codes over GF(2) for $47 < l < 200$. For a 5-design over GF(2), d must be greater than $l/6$, an unlikely result for large l.

5. Automorphism Groups of Quadratic-Residue Codes and 5-Designs

Let l be an odd prime, p a prime distinct from l, and A and B the two finite

$$\left(l + 1, \frac{l+1}{2}\right)$$

extended quadratic-residue codes over GF(q) defined in Section 3, where $q = p$ or p^2 depending on whether or not p is a quadratic residue modulo l. Let G be the automorphism group of A. We know that $PSL_2(l)$ is "contained in" G and that equality does not always obtain. This section will establish equality in certain cases.

We know, in general, that $PGL_2(l)$ is not "contained in" G, since any element of $PGL_2(l)$ not in $PSL_2(l)$ will interchange A and B.

Let G_∞ be the stability group of ∞, i.e., $G_\infty = \{\sigma \in G; \sigma(\infty) = \infty\}$. G_∞ is a transitive permutation group on l letters; it contains the per-

mutations of the form $x \to ax + b$ where $a \in \mathrm{GF}(l)^\times$ is a quadratic residue and b is an arbitrary element of $\mathrm{GF}(l)$. Call the group of all such permutations H. Then $G = \mathrm{PSL}_2(l)$ if and only if $G_\infty = H$. Moreover, the intersection of G_∞ with the full $ax + b$ group is always H since $G \cap \mathrm{PGL}_2(l) = \mathrm{PSL}_2(l)$.

Now, by a theorem of Galois, a transitive group on l letters is solvable if and only if the only element fixing two letters is the identity. It follows that a transitive solvable group on l letters has order less than or equal to $l(l-1)$. Since

$$|H| = l\left(\frac{l-1}{2}\right)$$

divides the order of G_∞, if G_∞ is solvable either $G_\infty = H$ or $|G_\infty| = l(l-1)$ and H is normal in G_∞. But the normalizer of H in the symmetric group on l letters is the group of all σ: $x \to ax + b$ where $a \in \mathrm{GF}(l)^\times$ and $b \in \mathrm{GF}(l)$, as one sees easily by examining $\pi^{-1}Z\pi$, where π is in the normalizer and $\pi(0) = 0, \pi(1) = 1$, and Z in H sends x to $x + 1$, and thus in the second case G_∞ is the full $ax + b$ group, a case that cannot occur. We now have

THEOREM 5.1. *If G properly "contains" $\mathrm{PSL}_2(l)$ then G_∞ is a non-solvable transitive permutation group on l letters. Moreover, if $(l-1)/2 \geqslant 7$ and is prime, then G properly "contains" $\mathrm{PSL}_2(l)$ if and only if G is 5-fold transitive.*

PROOF. The first assertion follows from the above discussion. As for the second, the 5-fold transitivity of G immediately implies $G \supset \mathrm{PSL}_2(l)$; and the reverse implication is an immediate consequence of the non-solvability of G_∞ and a deep result of Ito [15, p. 151].

Parker and Nikolai have demonstrated the non-existence of non-solvable transitive permutation groups on l letters for l a prime such that $l \neq 11, 23$, $l \leqslant 4{,}079$, and $(l-1)/2$ prime. Therefore, we have

COROLLARY 1. *For each Parker-Nikolai value of l, the codes A and B (for each p) have $\mathrm{PSL}_2(l)$ as automorphism group. In particular, the 5-designs on 48 points have $\mathrm{PSL}_2(47)$ as automorphism group.*

We remark that we first discovered that the group for $l = 47$ is not 5-fold transitive by calculating and examining some of the weight-12 code-vectors.

COROLLARY 2. *The (24, 12) codes A and B over GF(3) and the 5-design arising from the minimal weight vectors have $\mathrm{PSL}_2(23)$ as automorphism group.*

PROOF: If the group were larger than $PSL_2(23)$, it would have to be the Mathieu group M_{24}, since that is the only non-trivial 5-fold transitive group on 24 letters [13, p. 80]. M_{24} is the automorphism group of the 1; 5-8-24 design, and, if it also acted on the 6; 5-9-24 design associated with the minimum-weight vectors of the present code, then the subgroup M_0 of M_{24} fixing each of 5 given points would have to permute the 6 9-subsets of the new design containing those 5 points. M_0 has order 48 and it has two orbits on the remaining 19 points: one of length 3 and one of length 16. If we set down an incidence matrix of 6 rows and 24 columns for the 6 9-subsets mentioned above, then M_0, acting on the columns, permutes the rows of the matrix. Ignoring the first 5 columns with all 1's, we find that each of the 3 columns in one orbit therefore has the same number, say x, of 1's; similarly, each of the 16 other columns has y 1's. Therefore $3x + 16y = 24$; but this is not solvable in integers since $x \leqslant 6$. Therefore M_{24} cannot act on the 6; 5-9-24 design, and the group of the latter is $PSL_2(23)$. (We are indebted to A. M. Gleason for suggesting the above argument.)

(One can see that M_0 acts as claimed directly from the description of M_{24} in [31]; or, taking M_{24} as the automormphism group of the 5-8-24 Steiner system, assuming only the 5-fold transitivity and the order of M_{24} one can prove that only the identity of M_{24} can fix each of 7 points not contained in an 8-set of the 1; 5-8-24 design. From this the action of M_0 follows directly.)

These two corollaries allow us to prove [7] that $PSL_2(l)$ is the automorphism group of the Paley-Hadamard matrix of order $l + 1$ when $(l - 1)/2$ is prime, $l \equiv -1 \pmod{12}$, and $23 \leqslant l \leqslant 4{,}079$. The reason for the condition $l = 12N - 1$ is that, since $(3/l) = +1$, we can regard the row-space of the matrix over GF(3) as an extended quadratic-residue code.

One should remark that the 6; 5-9-24 design coming from the (24, 12) extended quadratic-residue code over GF(3) is suggestive of the design arising from a perfect code; a code is perfect if and only if the minimal-weight vectors yield a $(q - 1)^e; (e + 1) - d - n$ design (proved in [6]), where $d = 2e + 1$; here we have $\lambda = 6$ instead of 16, but otherwise the parameters are the same.

6. DISJOINT 5-DESIGNS

Each of the foregoing 5-designs arises from a finite extended quadratic residue code. Since such codes occur in pairs, there are two 5-designs of each type; we ask whether they are disjoint. The answer is obviously yes for the designs arising from codes over GF(2), because the codes are

disjoint except for the all-1 vector. The codes over GF(3) are disjoint but the problem is that there are now two possible non-0 coefficients instead of only one; this means that a given set of coordinate places might hold a vector from each code. We shall show, however, that this is not the case for the minimum-weight vectors of the codes in question (Hughes was the first to observe the existence of 5-design on 12 letters which was a union of two disjoint copies of the classical Steiner system of type 5-6-12 [14].)

PROPOSITION. *Let* l *and* $(l-1)/2$ *be primes, and let the minimum distance* d *in the finite extended quadratic-residue code of length* $l+1$ *be less than* $(l-1)/2$. *Then the stability subgroup* H *in* $\mathrm{PSL}_2(l)$ *of a* d*-club has order* h *dividing* d *and* $l+1$; *the orbits of* H *on the* d*-club are all of length* h.

PROOF: In $\mathrm{PSL}_2(l)$ the subgroup fixing 1 point has order $l(l-1)/2$. That fixing 2 points has order $(l-1)/2$. Since the latter is prime and any element in the stability subgroup is the product of cycles of lengths at most d, such an element cannot fix any points unless it is trivial. Therefore, H has only the trivial stability subgroup on any point of the d-club.

We shall apply this proposition to some of the codes yielding 5-designs, retaining the notations H and h.

(1) *The* (24, 12) *code over* GF(3). Here d is known to be 9. The number of 9-clubs in the 6; 5-9-24 design is $N = 8 \cdot 11 \cdot 23$ and $|\mathrm{PSL}_2(23)| = 3N$. Therefore H is non-trivial. Now it follows that $h = 3$, since $3 = gcd(9, 24)$. Therefore $\mathrm{PSL}_2(23)$ is transitive on the 9-clubs of each of the two 5-designs, which means that the 5-designs are disjoint or equal. That the 5-designs are disjoint follows from the fact that we can produce two 9-clubs, one from each design, meeting in 7 points, which is impossible for two 9-clubs from the same design (because it would imply the existence of a non-0 code vector of weight at most 7). The two 9-clubs arise from the code-polynomials $(x-1)g(x)$ and its reverse, $(x-1)\,g^*(x)$, where $g(x)\,g^*(x) = x^{22} + \cdots + 1$ over GF(3). Here

$$g(x) = x^{11} - x^8 - x^6 + x^4 + x^3 - x^2 - x - 1.$$

(2) *The* (12, 6) *code over* GF(3). This case does not quite fit the Proposition because $d = 6$ is larger than $(l-1)/2 = 5$. However, we shall determine h. The 1; 5-6-12 design has $N = 11 \cdot 12$ 6-clubs and

$$|\mathrm{PSL}_2(11)| = 5 \cdot 11 \cdot 12.$$

First of all, $|H| \geqslant 5$, and 11 does not divide $|H|$ because every element has order at most 6. Let us take H to be the stability group of the 6-club

$\{1, 3, 4, 5, 9, \infty\}$ which arises from the obvious code-vector having 1 at each of these coordinate places, which are the quadratic-residues and ∞. The Galois group, sending i to $3^n i$, mod 11, fixes this 6-club, and therefore 5 divides $|H|$. Now if 2 divided $|H|$, Sylow theory would guarantee at least 6 subgroups of order 5 (since conjugation of (1 3 9 5 4) by $(a\,b)(c\,d)(e\,f)$ would move the fixed point ∞; there cannot be an element of order 2 which fixes any of the 6 points), hence at least 24 elements of order 5. Similarly there would be at least 5 elements of order 2, hence $|H| \geqslant 30$. Analogously, if 3 divided $|H|$ we would find $|H| > 30$. The only divisors of $|\mathrm{PSL}_2(11)| = 5 \cdot 11 \cdot 12$ which are possible under the circumstances would be 60 and 30. 60 is impossible because the Sylow 2-subgroup would have to be the Klein 4-group, since no elements of order 4 could exist in H. But no two distinct elements of the form $(a\,b)(c\,d)(e\,f)$ in $\sum_6$ have another such as their product. Therefore, H would have to be 30, but we have already seen that such a group would have no room for elements of order 3. Therefore $|H| = 5$ and $\mathrm{PSL}_2(11)$ is transitive on the 6-clubs of the 1; 5-6-12 design. Proposition 3.1 tells us now that the two designs of this type are disjoint or equal. To prove disjointness we examine the generator polynomials $g(x)$ and the reverse $g^*(x)$, of degree 5. The weights of these are at most 6, and if 6 then the infinite coordinate would have to be 0 (by Theorem 3.3), contradicting that $x - 1$ does not divide either. Therefore each has weight 5 and gives a non-0 coordinate at ∞. These are then two different 6-clubs meeting in 5 places, hence not members of the same 1; 5-6-12 design (cf. [14, p. 774]).

Thus we have shown that each of the 5-designs of Section 4 for the minimum-weight vectors exist in disjoint pairs. This means in particular that the union of the two designs is a 5-design with λ doubled.[5]

A related question is that of the action $\mathrm{PSL}_2(l)$ on the d-clubs, where d is the minimum weight in the code. We have already shown that $\mathrm{PSL}_2(l)$ is transitive on the d-clubs for $l = 11$ and $l = 23$ over GF(3). The question naturally arises for the other two codes producing 5-designs.

Consider the (24, 12) code over GF(2). Here $d = 8$ and the number of minimum-weight vectors is $759 = 3 \cdot 11 \cdot 23 = N$. The order of $\mathrm{PSL}_2(23)$ is $8N$. From the proposition we know that H is non-trivial and has order dividing 8. But $|H| \geqslant 8$ by an orbit count. Therefore $|H| = 8$ and $\mathrm{PSL}_2(23)$ is transitive on the 8-clubs of the two 1; 5-8-24 Steiner systems.

The (48, 24) code over GF(2) is harder to analyze. All we can tell from what we have so far is that the order h of the stability subgroup of a 12-club satisfies $h \geqslant 3$ and $h \mid 12$. There are $N = 16 \cdot 23 \cdot 47$ 12-clubs and

[5] We announced this result for two 5-designs, those associated with the Mathieu groups M_{12} and M_{24}, in [4].

$|\mathrm{PSL}_2(47)| = 3N$. The Lehigh and Sylvania computers have found for us various elements of stability subgroups in $\mathrm{PSL}_2(47)$ of certain weight-12 vectors in our code. It is simple to verify these facts by hand checks. The situation is best described as follows: $\mathrm{PSL}_2(47)$ has three orbits on the weight-12 vectors of the code; one orbit (σ) consists of $\frac{1}{2}N$ vectors, the other two (σ_1 and σ_2) of $\frac{1}{4}N$ vectors each. The stability subgroup H of one of the vectors in σ has the property that it is isomorphic to $\sum_3$, the symmetric group on 3 letters, its normalizer G in $\mathrm{PSL}_2(47)$ is isomorphic to $\sum_3 \times Z_2$; and the eight orbits a, b, c, d, e, f, g, h, of H on the underlying 48 points, when paired as ab, df, ch, eg, are the coordinate places holding weight-12 vectors from the code; ab and df are "in" σ and ch is in σ_1, eg in σ_2. Although each of these three orbits of $\mathrm{PSL}_2(47)$ is a 3-design (since the group is 3-set transitive), and the union of the three is a 5-design (application 2c of Section 6), no one of these orbits, and hence no union of two, is even a 4-design, a fact established by the Sylvania computer. (G pairs the eight orbits as follows: ad, bf, ch, eg.) In terms of the natural action of $\mathrm{PSL}_2(47)$ on the projective line,

$$a = \{0, 1, 3, 16, 33, 40\}, \qquad b = \{\infty, 2, 13, 34, 41, 43\},$$
$$c = \{4, 5, 6, 18, 23, 26\}, \qquad d = \{7, 12, 15, 17, 29, 30\},$$
$$e = \{8, 27, 32, 37, 42, 45\}, \qquad f = \{9, 24, 31, 36, 38, 44\},$$
$$g = \{10, 11, 14, 22, 39, 46\}, \qquad h = \{19, 20, 21, 25, 28, 35\};$$

H is generated by $\left(\begin{smallmatrix} 6 & -6 \\ 14 & -6 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 2 & 15 \\ -16 & -2 \end{smallmatrix}\right)$ and G by H together with $\left(\begin{smallmatrix} 14 & 17 \\ 5 & -14 \end{smallmatrix}\right)$.

References

1. E. F. Assmus, Jr., and H. F. Mattson, Jr., Cyclic Codes, *Summary Scientific Report* #4, Air Force Cambridge Research Laboratories, AFCRL-65-332, April 28, 1965.
2. E. F. Assmus, Jr., and H. F. Mattson, Jr., Cyclic Codes, *Final Report*, Air Force Cambridge Research Laboratories, AFCRL-66-348, April 28, 1966.
3. E. F. Assmus, Jr., and H. F. Mattson, Jr., Perfect Codes and the Mathieu Groups, *Arch. Math.* **17** (1966), 121–135.
4. E. F. Assmus, Jr., and H. F. Mattson, Jr., Disjoint Steiner Systems Associated with the Mathieu Groups, *Bull. Amer. Math. Soc.* **72** (1966), 843–845.
5. E. F. Assmus, Jr., and H. F. Mattson, Jr., On the Number of Inequivalent Steiner Triple Systems, *J. Combinatorial Theory* **1** (1966), 301–305.
6. E. F. Assmus, Jr., and H. F. Mattson, Jr., On Tactical Configurations and Error-Correcting Codes, *J. Combinatorial Theory* **2** (1967), 243–257.
7. E. F. Assmus, Jr., and H. F. Mattson, Jr., On the Automorphism Groups of Paley-Hadamard Matrices, *Proceedings of the Conference on Combinatorial Mathematics and Its Applications*, University of North Carolina, April 1967. Univ. of North Carolina Press, Chapel Hill, 1968.

8. R. C. Bose, On Some Connections between the Design of Experiments and Information Theory, *Bull. Intern. Statist. Inst.* vol. 38, pp. 257–271; 1961.
9. A. M. Gleason, private communications (many of these are recorded in [1] and [2]).
10. M. J. E. Golay, Binary Coding, *IRE Trans. Information Theory* **IT-4** (1954), 23–28.
11. J. H. Griesmer, A Bound for Error-Correcting Codes, *IBM J. Res. Develop.* **4** (1960), 532–542; *MR* **23B** (1962), #B3081.
12. M. Hall, Jr., Note on the Mathieu Group M_{12}, *Arch. Math.* **13** (1962), 334–340.
13. M. Hall, Jr., *The Theory of Groups*, Macmillan, New York, 1959.
14. D. R. Hughes, t-Designs and Groups, *Amer. J. Math.* **87** (1965), 761–778.
15. N. Ito, Transitive Permutation Groups of Degree $p = 2q + 1$, p and q Being Prime Numbers, III, *Trans. Amer. Math. Soc.* **116** (1965), 151–166.
16. T. Kasami, Weight-Distribution of Bose-Chaudhuri-Hocquenghem Codes, *Proceedings of Conference on Combinatorial Mathematics and Its Applications*, University of North Carolina, April 1967, Univ. of North Carolina Press, Chapel Hill, 1968.
17. T. Kasami and S. Lin, Some Codes Which Are Invariant under a Doubly-Transitive Permutation Group and Their Connection with Balanced Incomplete Block Designs, AFCRL-66-142, *Scientific Report No.* 6, January 28, 1966, AF19(628)-4379.
18. S. P. Lloyd, Binary Block Coding, *Bell System Tech. J.* **36** (1957), 517–535; *MR* **19** (1958), 465.
19. F. J. MacWilliams, Ph.D. dissertation, Harvard University, 1961, unpublished.
20. F. J. MacWilliams, A Theorem on the Distribution of Weights in a Systematic Code, *Bell System Tech. J.* **42** (1963), 79–94; *MR* **26** (1963), #7462.
21. L. J. Paige, A Note on the Mathieu Groups, *Canad. J. Math.* **9** (1956), 15–18.
22. E. T. Parker and P. J. Nikolai, A Search for Analogues of the Mathieu Groups, *Math. Tables Aids Comput.* **12** (1958), 38–43; *MR* **21** (1960), #450.
23. W. W. Peterson, *Error-Correcting Codes*, M.I.T. Press, Cambridge, Mass., 1961.
24. V. Pless and E. Prange, Weight Distributions of All Cyclic Codes in a Vector Space of Dimension 31 over GF(2), AFCRL memo, September 1962.
25. E. A. Prange, Codes Equivalent under the Projective Group (III), AFCRL unpublished memorandum, July 10, 1962.
26. R. Silverman, A Metrization for Power-Sets with Applications to Combinatorial Analysis, *Canad. J. Math.* **12** (1960), 158–176; *MR* **25** (1963), #4019.
27. R. C. Singleton, Maximum Distance q-nary Codes, *IEEE Trans. Information Theory* **IT-10** (1964), 116–118.
28. G. Solomon, Tri-weight Cyclic Codes, Jet Propulsion Lab., SPS 37-41.
29. G. Solomon and J. J. Stiffler, Algebraically Punctured Cyclic Codes, *Information and Control* **8** (1965), 170–179; *MR* **30** (1965), #5847.
30. R. J. Turyn, A Theorem of Gleason and Pierce, Sylvania memo, December 1966.
31. E. Witt, Die 5-fach transitiven Gruppen von Mathieu, *Abh. Math. Sem. Hansischen Univ.* **12** (1938), 256–264.