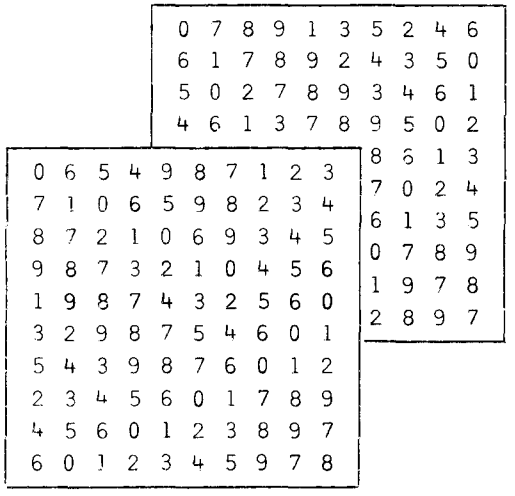

COMBINATORIAL
MATHEMATICS
YEAR

February 1969 - June 1970

A CLASS OF TRI-WEIGHT CYCLIC CODES

by

THOMAS A. DOWLING
University of North Carolina at Chapel Hill
Department of Statistics

Institute of Statistics Mimeo Series No. 600.3

JANUARY 1969

This research was partially sponsored by the Air Force Office of Scientific Research, United States Air Force, under Grant No. AF-AFOSR-68-1415; the National Science Foundation, under Grant No. GP-8624; and the National Aeronautices and Space Administration - American Society of Electrical Engineers Summer Faculty Fellowship Program.

A CLASS OF TRI-WEIGHT CYCLIC CODES

1. INTRODUCTION

Let ℓ, k be positive integers such that $\ell < k$ and $(2^\ell + 1, 2^k - 1) = 1$. Let $f_0(x)$ be a primitive polynomial of degree k over GF(2), and let $f_\ell(x)$ be the minimum polynomial of $\alpha^{2^\ell+1}$, where α is a root of $f_0(x)$. Then the cyclic code A with recursion polynomial $f_0(x)f_\ell(x)$ is a $(2^k - 1, 2k)$ code representing the direct sum of the maximal-length shift register codes with recursion polynomials $f_0(x)$, $f_\ell(x)$, respectively.

In the case k odd and $(\ell, k) = 1$, Gold [5] and Solomon [11] have shown that the code A has three non-zero weights. They give the weight distribution and an algebraic characterization of the code words of each weight. Gold [4] obtained a similar result for $k \equiv 2 \pmod 4$ and $\ell = (k + 2)/2$. We generalize these results to arbitrary k and ℓ subject to the conditions $\ell < k$, $(2^\ell + 1, 2^k - 1) = 1$. Theorem 1 below shows that A has three non-zero weights and gives the weight distribution, and Theorem 2 gives an algebraic characterization of the code words of each weight.

Remark. After completing this work, the author learned that the weight distribution (Theorem 1) had been obtained earlier by Kasami [6, 7]. Kasami's proof is purely algebraic and is based on the fact (which he proves) that A is a subcode of a second-order modified Reed-Muller code of length $2^k - 1$. Our proof involves geometric as well as algebraic methods, and is sufficiently dissimilar to Kasami's to merit its inclusion here. To the author's knowledge, Theorem 2 is new.

2. STATEMENT OF PRINCIPAL RESULTS

Throughout we shall assume k a fixed positive integer and ℓ an integer such that $1 \le \ell \le k-1$. This latter restriction is merely a convenience, since

This research was partially sponsored by the Air Force Office of Scientific Research, United States Air Force, under Grant No. AF-AFOSR-68-1415; the National Science Foundation, under Grant No. GP-8624; and the National Aeronautices and Space Administration - American Society of Electrical Engineers Summer Faculty Fellowship Program.

$2^m + 1 \equiv 2^\ell + 1 \pmod{2^k - 1}$ if $m \equiv \ell \pmod{k}$. The case $\ell = 0$ is omitted since we require $f_0(x)$ and $f_\ell(x)$ to be distinct. We begin by characterizing the set

$$L(k) = \{\ell: \ 1 \le \ell \le k-1, \ (2^\ell + 1, \ 2^k - 1) = 1\}$$

of integers ℓ for which $f_\ell(x)$ is primitive of degree k and distinct from $f_0(x)$.

For any integer t, define $m(t)$ as the exponent of two in the prime power factorization of t.

LEMMA 1: $L(k) = \{\ell: \ 1 \le \ell \le k-1, \ m(\ell) \ge m(k)\}$.

Proof: It is easily verified that if a, b, c are integers, and $(a, b) = 1$, then $(a, c) = 1$ if and only if $(ab, c) = (b, c)$. Setting $a = 2^\ell + 1$, $b = 2^\ell - 1$, $c = 2^k - 1$, we have $(2^\ell + 1, 2^k - 1) = 1$ if and only if $(2^{2\ell} - 1, 2^k - 1) = (2^\ell - 1, 2^k - 1)$. But $(2^r - 1, 2^s - 1) = 2^{(r,s)} - 1$. Hence $(2^\ell + 1, 2^k - 1) = 1$ if and only if $(2\ell, k) = (\ell, k)$, i.e., if and only if $m(\ell) \ge m(k)$.

COROLLARY 1: $L(k) = \emptyset$ if and only if $k = 2^m$ for some $m \ge 0$.

COROLLARY 2: If $\ell \in L(k)$, $(\ell, k) \equiv k \pmod 2$ and $k/(\ell, k) \equiv 1 \pmod 2$.

Proof: Write $k = 2^m s$, where $m = m(k)$, and $\ell = 2^m t$. Then

$$k + (\ell, k) = 2^m(s + (s, t)),$$

$$k/(\ell, k) = s/(s, t),$$

and the right-hand expressions are even and odd, respectively, since s is odd.

THEOREM 1: Suppose $k \neq 2^m$ for any $m \geq 0$, and let $\ell \in L(k)$. Then the cyclic code A with recursion polynomial $f_0(x)f_\ell(x)$ is a $(2^k - 1, 2k)$ code with three non-zero weights. The weight distribution of A is given below:

Weight	Number of Code Words
2^{k-1}	$(2^k - 1)(2^k - 2^{k-(\ell,k)} + 1)$
$2^{k-1} - 2^{(k+(\ell,k)-2)/2}$	$(2^k - 1)(2^{k-(\ell,k)-1} + 2^{(k-(\ell,k)-2)/2})$
$2^{k-1} + 2^{(k+(\ell,k)-2)/2}$	$(2^k - 1)(2^{k-(\ell,k)-1} - 2^{(k-(\ell,k)-2)/2})$

The proof of Theorem 1, and Theorem 2 below, will be given in Section 5. Before stating Theorem 2, we require some preliminary remarks on the algebraic characterization of the code words of A, following Solomon [11] and Gold [5].

Let $a = (a_0, a_1, \ldots, a_{2^k-2})$ be a code word of A. Then a is characterized by its Mattson-Solomon polynomial [8]

$$g_a(x) = \mathrm{Tr}\, cx + \mathrm{Tr}\, dx^{2^\ell+1},$$

where $c, d \in GF(2^k)$, and $\mathrm{Tr}\, x = \sum_{i=0}^{k-1} x^{2^i}$ is the trace of $GF(2^k)/GF(2)$. The polynomial $g_a(x)$ satisfies $g_a(\alpha^i) = a_i$, where α is a root of $f_0(x)$. Thus the mapping

$$\psi: \; a \to (c, d)$$

is a one-one linear mapping of the code A onto $GF(2^k) \times GF(2^k)$. We define $w(c, d)$ as the weight of the code word $a = \psi^{-1}(c, d)$.

If $a \in A$, $\psi(a) = (c, d)$, a cyclic shift T_s to the right of length s maps $a \to T_s(a)$ and $(c, d) \to (\alpha^s c, \alpha^{s(2^\ell+1)} d)$. If $c \neq 0$, $d = 0$, then clearly $a \in A_0$, so $w(c, 0) = 2^{k-1}$. Similarly, if $c = 0$, $d \neq 0$, then $a \in A_\ell$, $w(0, d) = 2^{k-1}$. If $c \neq 0$, $d \neq 0$, we can choose s above so that

$\alpha^s = d^{-\frac{1}{2^\ell+1}}$ since $2^\ell + 1$ is prime to $2^k - 1$. Since T_s is obviously weight-preserving,

$$w(c, d) = w(cd^{-\frac{1}{2^\ell+1}}, 1).$$

Thus we can restrict attention to code words a such that $\psi(a) = (c, 1)$, where $c \neq 0$.

Let $Tr_{k/(\ell,k)} x = \sum_{i=0}^{t-1} x^{2^{i(\ell,k)}}$ denote the trace of $GF(2^k)/GF(2^{(\ell,k)})$, where $t = k/(\ell, k)$. We then have

THEOREM 2: Let $c \in GF(2^k)$, $c \neq 0$. Then

(i) if $Tr_{k/(\ell,k)} c \neq 1$,

$$w(c, 1) = 2^{k-1}$$

(ii) if $Tr_{k/(\ell,k)} c = 1$,

$$w(c, 1) = \begin{cases} w(1, 1) & \text{if } Tr(\beta + \beta^{2^{\ell+1}}) = 0, \\ 2^k - w(1, 1) & \text{if } Tr(\beta + \beta^{2^{\ell+1}}) = 1, \end{cases}$$

where β is any solution of

$$x^{2^{2\ell}} + x = (c + 1)^{2^\ell}. \tag{1}$$

Remarks: Note that since $t = k/(\ell, k)$ is odd by Corollary 2, $Tr_{k/(\ell,k)} 1 = 1$. Hence $w(c, 1) = 2^{k-1} \pm 2^{(k+(\ell,k)-2)/2}$ if $Tr_{k/(\ell,k)} c = 1$. The proof that $w(c, 1) = w(1, 1)$ or $2^k - w(1, 1)$ in this case according as $T_r(\beta + \beta^{2^{\ell+1}}) = 0$ or 1 will not be given below, as it is entirely analogous to the proof given by Solomon [11] and Gold [5] for the case $(\ell, k) = 1$. If $Tr_{k/(\ell,k)} c = 1$, a

theorem of McEliece [9] shows that the Eq. (1) has $2^{(\ell,k)}$ solutions in $GF(2^k)$, the solutions forming a coset of $GF(2^k)$ with respect to $GF(2^{(\ell,k)})$. Hence, if β is any solution of (1), $\beta + y$ is a solution for any $y \in GF(2^{(\ell,k)})$. But

$$Tr[(\beta + y) + (\beta + y)^{2^\ell+1}] = Tr(\beta + \beta^{2^\ell+1}) + Tr(y + y^{2^\ell+1}) + Tr(\beta^{2^\ell} y + \beta y^{2^\ell}) .$$

Since $y \in GF(2^{(\ell,k)})$, $y^{2^\ell} = y$, so $Tr(y + y^{2^\ell+1}) = 0$, and

$$\begin{aligned} Tr(\beta^{2^\ell} y + \beta y^{2^\ell}) &= Tr(\beta^{2^\ell} + \beta)y . \\ &= Tr_{(\ell,k)/1} [Tr_{k/(\ell,k)} (\beta^{2^\ell} + \beta)y] \\ &= Tr_{(\ell,k)/1} [y\, Tr_{k/(\ell,k)} (\beta^{2^\ell} + \beta)] \\ &= 0 \qquad \text{(Ref. 1, pp. 118-119).} \end{aligned}$$

since $Tr_{k/(\ell,k)} (\beta^{2^\ell} + \beta) = (Tr_{k/(\ell,k)} \beta)^{2^\ell} + (Tr_{k/(\ell,k)} \beta) = 0$. Hence, any two solutions to (1) have the same value of $Tr(x + x^{2^\ell+1})$, so the weight is well-defined in (ii).

3. TRANSLATION OF THE PROBLEM

The remainder of this report will be devoted to the proofs of Theorem 1 and part (i) of Theorem 2. By our earlier remarks, it is sufficient to consider code words $a \in A$ such that $\psi(a) = (c, 1)$, where $c \neq 0$. Then $w(c, 1)$ is the number of $x \in GF(2^k) - \{0\}$ such that $g_a(x) = 1$, where

$$g_a(x) = Tr\, cx + Tr\, x^{2^\ell+1} .$$

Define $\rho(c)$ as the number of $x \in GF(2^k) - \{0\}$ such that

$$\begin{aligned} \mathrm{Tr}\ cx &= 0 \\ \mathrm{Tr}\ x^{2^\ell+1} &= 0 \end{aligned}$$

hold simultaneously. Then, since each equation is satisfied separately by $2^{k-1} - 1$ elements of $GF(2^k) - \{0\}$, we have

$$w(c, 1) = 2[2^{k-1} - 1 - \rho(c)] . \tag{2}$$

Hence we can consider the function $\rho(c)$ in order to determine $w(c, 1)$.

Regard $GF(2^k)$ as a vector space over $GF(2)$, and let $\{w_0, w_1, \ldots, w_{k-1}\}$ be a basis. Then any element $x \in GF(2^k)$ has a unique representation in the form $\Sigma\, x_i\, w_i$, where $x_i \in GF(2)$, $i = 0, 1, \ldots, k-1$. We associate the vector $\underline{x}' = (x_0, x_1, \ldots, x_{k-1})$ with x. Then if $y = \Sigma\, y_i\, w_i$, we have

$$\mathrm{Tr}\ xy = \sum_{i=0}^{k-1} \sum_{j=0}^{k-1} x_i\, y_j\, \mathrm{Tr}(w_i w_j)$$

or

$$\mathrm{Tr}\ xy = \underline{x}'\, T\, \underline{y} ,$$

where $T = (t_{ij})$ is the $k \times k$ matrix over $GF(2)$ with $t_{ij} = \mathrm{Tr}\ w_i w_j$. T is non-singular, for otherwise there exists a non-null vector $\underline{c}'$ such that $\underline{c}'\, T = \underline{0}'$, the null vector. Then $\mathrm{Tr}\ cx = 0$ for all $x \in GF(2^k)$, which implies $c = 0$, a contradiction.

The mapping $\sigma\colon\ x \to x^{2^\ell}$ is an automorphism of $GF(2^k)$; hence there exists a non-singular $k \times k$ matrix S over $GF(2)$ such that $\underline{\sigma(x)} = S\underline{x}$. (Take $S = (s_{ij})$, where $s_{ij} = s'_{ji}$ and $w_i^{2^\ell} = \sum_j s'_{ij}\, w_j$.) Thus we can write,

(3) $$\mathrm{Tr}\ xy^{2^\ell} = \underline{x}'\ TS\underline{y}$$

for any $x,y \in GF(2^k)$. In particular, if $y = x^{2^\ell}$,

$$\mathrm{Tr}\ x^{2^\ell+1} = \underline{x}'\ TS\ \underline{x}$$

is a quadratic form in $x_0, x_1, \ldots, x_{k-1}$. Hence we see that $\rho(c)$ is the number of non-null binary k-vectors $\underline{x}$ such that the equations

(4) $$\underline{c}'\ T\ \underline{x} = 0$$

(5) $$\underline{x}'\ TS\ \underline{x} = 0$$

hold simultaneously.

We now associate the elements $x \in GF(2^k) - \{0\}$ with the points X of the finite projective geometry $PG(k-1, 2)$ by the correspondence $x \sim X$ if the coordinate vector of X is $\underline{x}' = (x_0, x_1, \ldots, x_{k-1})$, where $x = \Sigma\ x_i\ w_i$. Eq. (4) then represents a hyperplane Σ_{k-2} and Eq. (5) a quadric Q_{k-1} in $PG(k-1, 2)$. Hence the points X whose coordinate vectors satisfy (4) and (5) are the points of a quadric $Q_{k-2} = Q_{k-1} \cap \Sigma_{k-2}$ in Σ_{k-2}. Since T is non-singular, Eq. (4) establishes a one-one correspondence between the elements $c \in GF(2^k) - \{0\}$ and the hyperplanes of $PG(k-1, 2)$. We can thus determine the number of c such that $\rho(c) = \rho$ by determining the number of hyperplanes Σ_{k-2} in $PG(k-1, 2)$ such that $|Q_{k-2}| = \rho$, where $Q_{k-2} = Q_{k-1} \cap \Sigma_{k-2}$ and $|Q_{k-2}|$ is the number of points of Q_{k-2}. For this, we shall require some results on quadrics in $PG(n, 2)$. Proofs not given below may be found in Bose [3] or Ray-Chaudhuri [10].

4. RESULTS ON QUADRICS IN PG(n, 2)

A quadric Q_n in $PG(n, 2)$ consists of all points X whose coordinate vectors $\underline{x}' = (x_0, x_1, \ldots, x_n)$ satisfy an equation

$$\underline{x}' A \underline{x} = 0 ,$$

where $A = (a_{ij})$ is an $(n + 1) \times (n + 1)$ matrix over $GF(2)$. The rank of Q_n is defined to be the minimum number $n + 1 - r$ of linear forms

$$U_i = b_{io}x_o + b_{i1}x_1 + \ldots + b_{in}x_n , \quad i = 0, 1, \ldots, n+1-r$$

such that $\underline{x}' A \underline{x}$ is expressible as a quadratic form in $U_0, U_1, \ldots, U_{n+1-r}$. The rank of Q_n is related to the rank of the symmetric matrix $A + A'$ by

$$\text{rank } (A + A') = 2[\tfrac{1}{2} \text{ rank } Q_n] ,$$

where $[x]$ is the greatest integer not exceeding x.

If $r = 0$, i.e., if rank $Q_n = n + 1$, Q_n is a non-degenerate quadric. If $r > 0$, Q_n is degenerate of order r. In this case, Q_n is called a cone of order r. We shall find it convenient to regard a non-degenerate quadric as a cone of order zero.

If n is even, non-degenerate quadrics are of one type. These contain $2^n - 1$ points and flat spaces of dimension $(n-2)/2$. If n is odd, there are two types of non-degenerate quadrics: hyperbolic (ruled) quadrics contain $2^n + 2^{(n-1)/2} - 1$ points and flat spaces of dimension $(n-1)/2$; elliptic (unruled) quadrics contain $2^n - 2^{(n-1)/2} - 1$ points and flat spaces of dimension $(n-3)/2$. (By convention, a flat space of dimension -1 is empty.)

If Q_n is a cone of order r, there exists a unique $(r-1)$-flat Σ_{r-1}, called the vertex of Q_n, such that the points of Q_n are those of the lines joining points of Σ_{r-1} to points of Q_{n-r}, where Q_{n-r} is a non-degenerate quadric in $n - r$ dimensions obtained by intersecting Q_n with any $(n-r)$-flat Σ_{n-r} which is skew to Σ_{r-1}. If $n - r$ is odd, Q_n is an

elliptic or hyperbolic cone according as Q_{n-r} is an elliptic or hyperbolic quadric. The number $|Q_n|$ of points on Q_n is given by

$$|Q_n| = 2^r - 1 + 2^r|Q_{n-r}| .$$

We therefore have

$$(6) \qquad |Q_n| = \begin{cases} 2^n - 1 & \text{if } n - r \text{ even,} \\ 2^n + 2^{(n-r-1)/2} - 1 & \text{if } n - r \text{ odd, } Q_{n-r} \text{ hyperbolic,} \\ 2^n - 2^{(n-r-1)/2} - 1 & \text{if } n - r \text{ odd, } Q_{n-r} \text{ elliptic.} \end{cases}$$

A point B of $PG(n, 2)$ with coordinate vector $\underline{b}$ is said to be irregular (regular) with respect to Q_n if $\underline{b}'(A + A')$ is null (non-null). The set of irregular points clearly form a flat space, called the nucleus of polarity of Q_n. If Q_n is non-degenerate, every point is regular if n is odd. If n is even, the nucleus of polarity consists of a single point $B \notin Q_n$. More generally, if Q_n is a cone of order r, the nucleus of polarity is the vertex Σ_{r-1} if $n - r$ is odd. If $n - r$ is even, the nucleus of polarity is the r-flat Σ_r containing Σ_{r-1} and B, where B is the nucleus of polarity of the non-degenerate quadric Q_{n-r}. In this case, $\Sigma_r \cap Q_n = \Sigma_{r-1}$.

If Q_n is non-degenerate, n is even, and Σ_{n-1} is any hyperplane of $PG(n, 2)$, then the quadric $Q_{n-1} = Q_n \cap \Sigma_{n-1}$ is non-degenerate if and only if $B \notin \Sigma_{n-1}$, where B is the nucleus of polarity of Q_n. If $B \in \Sigma_{n-1}$, Q_{n-1} is a cone of order one. We use these results to prove

LEMMA 2: Let Q_n be a non-degenerate quadric in $PG(n, 2)$, n even, and let B be the nucleus of polarity of Q_n. Let Σ_{n-1} be a hyperplane, and define $Q_{n-1} = Q_n \cap \Sigma_{n-1}$. Then if $B \in \Sigma_{n-1}$,

1. Q_{n-1} is a cone of order one;

if $B \not\in \Sigma_{n-1}$, then either

2. Q_{n-1} is a non-degenerate hyperbolic quadric,

or

3. Q_{n-1} is a non-degenerate elliptic quadric.

The numbers N_t, $t = 1, 2, 3,$ of hyperplanes Σ_{n-1} for which Q_{n-1} is of type t are

$$N_1 = 2^n - 1,$$

$$N_2 = 2^{n-1} + 2^{(n-2)/2},$$

$$N_3 = 2^{n-1} - 2^{(n-2)/2}.$$

Proof: The first part is simply a restatement of the above results. To determine the N_t, we count the number of pairs (P, Σ_{n-1}) where P is a point of Q_n and Σ_{n-1} is a hyperplane containing P. Since each point of $PG(n-1, 2)$ is contained in $2^n - 1$ hyperplanes and there are $2^n - 1$ points on Q_n by (6), the number of such pairs is $(2^n-1)^2$. Counting these pairs in a second way, using (6), we obtain

$$(2^n-1)^2 = N_1(2^{n-1}-1) + N_2(2^{n-1}+2^{(n-2)/2}-1) + N_3(2^{n-1}-2^{(n-2)/2}-1)$$

or

$$(2^n-1)^2 = (N_1 + N_2 + N_3)(2^{n-1}-1) + 2^{(n-2)/2}(N_2 - N_3) .$$

Since $N_1 + N_2 + N_3 = 2^{n+1} - 1$, the total number of hyperplanes, and $N_1 = 2^n - 1$, the number of hyperplanes containing B, we have

$$N_2 + N_3 = 2^n ,$$

and

$$N_2 - N_3 = 2^{n/2}.$$

Solving these equations for N_2, N_3, we have

LEMMA 3: Let Q_n be a cone of order r in PG(n, 2), where $n-r$ is even. Let Σ_r be the nucleus of polarity of Q_n and $\Sigma_{r-1} = \Sigma_r \cap Q_n$ the vertex. Let Σ_{n-1} be a hyperplane and define $Q_{n-1} = Q_n \cap \Sigma_{n-1}$. Then if $\Sigma_{r-1} \not\subset \Sigma_{n-1}$,

0. Q_{n-1} is a cone of order $r - 1$;

if $\Sigma_r \subset \Sigma_{n-1}$,

1. Q_{n-1} is a cone of order $r + 1$;

if $\Sigma_{r-1} \subset \Sigma_{n-1}$ but $\Sigma_r \not\subset \Sigma_{n-1}$; then either

2. Q_{n-1} is a hyperbolic cone of order r,

or

3. Q_{n-1} is an elliptic cone of order r.

The number N_t, $t = 0, 1, 2, 3$, of hyperplanes Σ_{n-1} for which Q_{n-1} is of type t is

$$N_0 = 2^{n+1} - 2^{n-r+1},$$
$$N_1 = 2^{n-r} - 1,$$
$$N_2 = 2^{n-r-1} + 2^{(n-r-2)/2},$$
$$N_3 = 2^{n-r-1} - 2^{(n-r-2)/2}.$$

Proof: If $\Sigma_{r-1} \not\subset \Sigma_{n-1}$, then Σ_{n-1} contains an $(n-r)$-flat Σ_{n-r} skew to Σ_{r-1}. The quadric $Q_{n-r} = Q_n \cap \Sigma_{n-r}$ is non-degenerate in Σ_{n-r}, and Q_{n-1} clearly consists of all points on the lines joining points of Q_{n-r} to points of $\Sigma_{r-2} = \Sigma_{r-1} \cap \Sigma_{n-1}$. Hence, Q_{n-1} is a cone of order $r - 1$ with vertex Σ_{r-2}.

Suppose now $\Sigma_{r-1} \subset \Sigma_{n-1}$. Let Σ_{n-r} be a fixed $(n-r)$-flat skew to Σ_{r-1}, and let $Q_{n-r} = Q_n \cap \Sigma_{n-r}$. There is a one-one correspondence between

hyperplanes Σ_{n-1} containing Σ_{r-1} and $(n-r-1)$-flats Σ_{n-r-1} of Σ_{n-r}, such that $\Sigma_{n-r-1} \sim \Sigma_{n-1}$ if and only if $\Sigma_{n-r-1} = \Sigma_{n-1} \cap \Sigma_{n-r}$. Since Q_{n-r} is non-degenerate, we can apply Lemma 2 to obtain the numbers N_1, N_2, N_3 of $(n-r-1)$-flats Σ_{n-r-1} in Σ_{n-r} for which $Q_{n-r-1} = Q_{n-r} \cap \Sigma_{n-r-1}$ is a cone of order one, a non-degenerate hyperbolic quadric, and a non-degenerate elliptic quadric, respectively. But if $\Sigma_{n-1} \sim \Sigma_{n-r-1}$, and Q_{n-r-1} is a cone of order s in Σ_{n-r}, then Q_{n-1} is a cone of order $r + s$ in Σ_{n-1}. The vertex Σ_{r+s-1} of Q_{n-1} is the join of Σ_r and Σ_s, where Σ_s is the vertex of Q_{n-r-1}. The proof is completed by noting that if B is the nucleus of polarity of Q_{n-r-1}, then $B = \Sigma_r \cap \Sigma_{n-r}$, and hence $B \in \Sigma_{n-r-1}$ if and only if $\Sigma_r \subset \Sigma_{n-1}$.

COROLLARY 3: Let $M(\rho)$ be the number of hyperplanes Σ_{n-1} which intersect Q_n in exactly ρ points. Then we have

ρ	$M(\rho)$
$2^{n-1} - 1$	$2^{n+1} - 2^{n-r} - 1$
$2^{n-1} + 2^{(n+r-2)/2} - 1$	$2^{n-r-1} + 2^{(n-r-2)/2}$
$2^{n-1} - 2^{(n+r-2)/2} - 1$	$2^{n-r-1} - 2^{(n-r-2)/2}$

Proof: Apply (6) with $n - 1$ replacing n and note that the quadrics of types 0 and 1 have the same number of points.

5. PROOF OF THEOREMS 1 AND 2

We now consider the quadric Q_{k-1} in $PG(k-1, 2)$ with equation

$$\underline{x}' \, TS \, \underline{x} = 0.$$

The points of Q_{k-1}, we recall, correspond to the elements $x \in GF(2^k) - \{0\}$ for which $\mathrm{Tr}\, x^{2^{\ell}+1} = 0$. Then it is clear that Q_{k-1} has $2^{k-1} - 1$ points, and by comparison with Eq. (6), we see that Q_{k-1} is a cone of order $r \geq 0$, where $k - 1 - r$ is even. The previous corollary then shows that the function $\rho(c)$ is three-valued. In order to specify the values and the number of c's mapped into each value, we must determine the order r of Q_{k-1}.

Since $k - 1 - r$ is even, the nucleus of polarity of Q_{k-1} is an r-flat Σ_r intersecting Q_{k-1} in the vertex Σ_{r-1}. We have

LEMMA 4: The order of Q_{k-1} is $r = (\ell, k) - 1$. The points of the nucleus of polarity $\Sigma_{(\ell,k)-1}$ correspond to the elements of $GF(2^{(\ell,k)}) - \{0\}$. The points of the vertex $\Sigma_{(\ell,k)-2}$ correspond to the elements b of $GF(2^{(\ell,k)}) - \{0\}$ for which $\mathrm{Tr}\, b = 0$.

Proof: The points B of Σ_r are those whose coordinate vectors $\underline{b}$ satisfy

$$\underline{b}'(TS + (TS)') = \underline{0}',$$

where $\underline{0}'$ denotes the null vector. Equivalently, $B \in \Sigma_r$ if and only if

$$\underline{b}'\, TS\, \underline{x} = \underline{x}'\, TS\, \underline{b} \tag{7}$$

for all binary k-vectors $\underline{x}$. Using Eq. (2), (7) holds if and only if, for all $x \in GF(2^k)$,

$$\mathrm{Tr}\, bx^{2^{\ell}} = \mathrm{Tr}\, b^{2^{\ell}} x$$

or

$$\mathrm{Tr}\, b^{2^{-\ell}} x = \mathrm{Tr}\, b^{2^{\ell}} x.$$

Thus $b^{2^{-\ell}} = b^{2^{\ell}}$, or $b^{2^{2\ell}} = b$. Hence, if e is the order of b, then $e \mid 2^{2\ell} - 1$. Since $e \mid 2^k - 1$, e divides $(2^{2\ell}-1, 2^k-1) = 2^{(2\ell,k)} - 1 = 2^{(\ell,k)} - 1$ for $\ell \in L(k)$. Thus $b \in GF(2^{(\ell,k)})$. Conversely, if $b \in GF(2^{(\ell,k)})$, $b^{2^{2\ell}} = b$. Hence Σ_r contains $2^{(\ell,k)} - 1$ points, and therefore $r = (\ell, k) - 1$.

The points of the vertex $\Sigma_{(\ell,k)-2}$ thus correspond to the elements b of $GF(2^{(\ell,k)}) - \{0\}$ such that $\mathrm{Tr}\, b^{2^{\ell}+1} = 0$. But

$$2^{\ell} + 1 = \left(\frac{2^{\ell}-1}{2^{(\ell,k)}-1}\right)(2^{(\ell,k)}-1) + 2 ,$$

so that $b^{2^{\ell}+1} = b^2$, and $\mathrm{Tr}\, b^{2^{\ell}+1} = \mathrm{Tr}\, b^2 = \mathrm{Tr}\, b$. Thus $B \in \Sigma_{(\ell,k)-2}$ if and only if $b \in GF(2^{(\ell,k)}) - \{0\}$ and $\mathrm{Tr}\, b = 0$.

On substituting the values $n = k - 1$ and $r = (\ell, k) - 1$ into the expressions for ρ and $M(\rho)$ of the corollary, and using Eq. (2), we obtain the weight distribution of the words $a \in A$ for which $\psi(a) = (c, 1)$, $c \neq 0$:

	Weight	No. of Code Words
1.	2^{k-1}	$2^k - 2^{k-(\ell,k)} - 1$
2.	$2^{k-1} - 2^{(k+(\ell,k)-2)/2}$	$2^{k-(\ell,k)-1} + 2^{(k-(\ell,k)-2)/2}$
3.	$2^{k-1} + 2^{(k+(\ell,k)-2)/2}$	$2^{k-(\ell,k)-1} - 2^{(k-(\ell,k)-2)/2}$

We obtain the weight distribution of Theorem 1 by multiplying the numbers in the right-hand column by $2^k - 1$ to include all cyclic shifts of the type $(c, 1)$ words, and adding $2(2^k-1)$ to the number so obtained for the weight

2^{k-1} words to include the words of type (c, 0) and (0, d). This completes the proof of Theorem 1.

Returning now to the words of type (c, 1), where $c \neq 0$, we note that the words of weight $2^{k-1} \pm 2^{(k+(\ell,k)-2)/2}$ are those for which Q_{k-2} is of type 2 or 3 in Lemma 3, where $Q_{k-2} = Q_{k-1} \cap \Sigma_{k-2}$ and Σ_{k-2} is the hyperplane with equation $\underline{c}' T \underline{x} = 0$. But Q_{k-2} is of type 2 or 3 if and only if $\Sigma_{k-2} \cap \Sigma_{(\ell,k)-1} = \Sigma_{(\ell,k)-2}$. Thus $w(c, 1) \neq 2^{k-1}$ if and only if, for all $x \in GF(2^{(\ell,k)})$,

$$\text{Tr } cx = \begin{cases} 0 & \text{Tr } x = 0, \\ 1 & \text{Tr } x = 1, \end{cases}$$

i.e., if and only if $\text{Tr}(c + 1)x = 0$ for all $x \in GF(2^{(\ell,k)})$.

But

$$\begin{aligned} \text{Tr}(c+1)x &= \text{Tr}_{(\ell,k)/1}[\text{Tr}_{k/(\ell,k)}\ (c+1)x] \\ &= \text{Tr}_{(\ell,k)/1}[x\ \text{Tr}_{k/(\ell,k)}\ (c+1)] \end{aligned}$$

for $x \in GF(2^{(\ell,k)})$, [1, pp.118-119]. Hence $\text{Tr}(c+1)x = 0$ for all $x \in GF(2^{(\ell,k)})$ if and only if $\text{Tr}_{k/(\ell,k)}(c+1) = 0$. Since $k/(\ell, k)$ is odd by Corollary 2, $\text{Tr}_{k/(\ell,k)}1 = 1$. Hence $w(c, 1) \neq 2^{k-1}$ if and only if $\text{Tr}_{k/(\ell,k)}c = 1$. This completes the proof of part (i) of Theorem 2.

REFERENCES

1. Albert, A.A., Fundamental Concepts of Higher Algebra, The University of Chicago Press (Chicago), 1956.

2. Berlekamp, E., Algebraic Coding Theory, McGraw-Hill (New York), 1968.

3. Bose, R.C., Combinatorial Problems of Experimental Design, Vol. I., John Wiley & Sons (New York), 1969.

4. Gold, R. "Optimal Binary Sequences for Spread-Spectrum Multiplexing", IEEE Transactions on Information Theory, IT-13 (1967), 619-621.

5. Gold, R., "Maximal Recursive Sequences with 3-Valued Recursive Cross-Correlation Functions", IEEE Transactions on Information Theory, IT-14 (1968), 154-156.

6. Kasami, T., "Weight Distribution Formula for Some Classes of Cyclic Codes", Report of Coordinated Science Laboratory, University of Illinois, 1966.

7. Kasami, T., "Weight Distribution of Bose-Chaudhuri-Hocquenghem Codes", Chapter 20 in Combinatorial Mathematics and Its Applications: Proceedings of the Conference held at the University of North Carolina at Chapel Hill, April 10-14, 1967, (R.C. Bose, T.A. Dowling, eds.) University of North Carolina Press.

8. Mattson, H.F. and Solomon, G., "A New Treatment of Bose-Chandhuri Codes", J. Soc. Ind. Appl. Math., 9 (1961), 654-669.

9. McEliece, R., "Efficient Solution of Equations for Decoding", Jet Propulsion Laboratory Space Programs Summary 37-40, Vol. IV, 216-218.

10. Ray-Chaudhuri, D.K., "Some Results on Quadrics in Finite Projective Geometry Based on Galois Fields", Can. J. Math. 14 (1962), 129-138.

11. Solomon, G., "Tri-Weight Cyclic Codes," Jet Propulsion Laboratory Space Programs Summary 37-41, Vol. IV, 266-268.