On Generalized Reed–Muller Codes and Their Relatives

P. DELSARTE AND J. M. GOETHALS

MBLE Research Laboratory, Brussels, Belgium

AND

F. J. MAC WILLIAMS

Bell Telephone Laboratories, Murray Hill, New Jersey, 07974

Received April 20, 1969; revised December 10, 1969

The polynomial formulation of generalized Reed–Muller codes, first introduced by Kasami, Lin, and Peterson is somewhat formalized and an extensive study is made of the interrelations between the m-variable approach of Kasami, Lin, and Peterson and the one-variable approach of Mattson and Solomon. The automorphism group is studied in great detail, both in the m-variable and in the one-variable language. The number of minimum weight vectors is obtained in the general case. Two ways of restricting generalized Reed–Muller codes to subcodes are studied: the nonprimitive and the subfield subcodes. Connections with geometric codes are pointed out and a new series of majority decodable codes is introduced.

INTRODUCTION

The definition of the binary Reed–Muller codes originally introduced by Reed [22] can be stated as follows.

Let $M$ be a $m \times (2^m - 1)$ matrix, whose columns are the binary representations of all numbers $a, 0 < a < 2^m$. (The subspace of $[GF(2)]^{2^m-1}$ generated by the rows of $M$ is the dual of the binary Hamming code; every nonzero vector of this subspace has weight $2^{m-1}$.) Add to $M$ a column of zeros and an all unity vector $J$ (of length $2^m$). Let $M'$ be the extended matrix. The 1-st order binary Reed–Muller code is the subspace of $[GF(2)]^{2^m}$ generated by the rows of $M'$. It has dimension $1 + m$, and minimum distance $2^{m-1}$.

For any two vectors $a = a_0, a_1, ..., a_r, b = b_0, b_1, ..., b_r$, define $a \cdot b = a_0 \cdot b_0 + a_1 \cdot b_1 + ... + a_r \cdot b_r$. The Hamming weight of a vector is the number of ones in it. The weight of a code is the minimum weight of all nonzero vectors in it.
pointwise product vector \( \mathbf{a} \ast \mathbf{b} = a_0b_0, a_1b_1, \ldots, a_nb_n \). The 2-nd order binary Reed–Muller code is the subspace of \([GF(2)]^{2m}\) generated by all pointwise products \( \mathbf{a} \ast \mathbf{b} \), where \( \mathbf{a}, \mathbf{b} \) are rows of \( M' \). It has dimension \( 1 + (\binom{m}{1}) + (\binom{m}{2}) \) and minimum distance \( 2^{m-2} \). The 3-rd order binary Reed–Muller code is generated by all triple products \( \mathbf{a} \ast \mathbf{b} \ast \mathbf{c} \), where \( \mathbf{a}, \mathbf{b}, \mathbf{c} \) are rows of \( M' \); it has dimension \( 1 + (\binom{m}{1}) + (\binom{m}{2}) + (\binom{m}{3}) \) and minimum distance \( 2^{m-3} \), and so on.

The generalization consists in using for the columns of \( M \), (which becomes an \( m \times (q^m - 1) \) matrix), the \( q \)-ary representations of all numbers \( a, 0 < a < q^m \). To get \( M' \) we add a column of zeros and an all unity vector \( \mathbf{J} \) as before. The 1-st order G.R.M. code is the subspace of \([GF(q)]^{q^m}\) generated by the rows of \( M' \). The pointwise product of two vectors is defined as before, but note that in the binary case \( \mathbf{a} \ast \mathbf{a} = \mathbf{a} \), which is no longer true. The \( v \)-th order G.R.M. code can be defined by exactly the same words as before, however, it would be rash to say that it is an interesting generalization of the \( v \)-th order binary Reed–Muller code.

The properties of a binary Reed–Muller code were originally obtained by Muller [21] using Boolean algebra, or, equivalently the incidence properties of sets of points in a Euclidean geometry \( EG(m, 2) \) over \( GF(2) \). The columns of \( M \) can be regarded as the (nonzero) points of \( EG(m, 2) \); if \( (x_1, x_2, \ldots, x_m) \) is the generic point, a 1 in the \( i \)-th row of \( M \) corresponds in an obvious way to the equation \( x_i = 1 \). A moment’s reflection will show that the 1-st order binary Reed–Muller code contains all the incidence vectors of points and hyperplanes of \( EG(m, 2) \); in fact every vector in the code except \( \mathbf{J} \) and \( \mathbf{0} \) is such an incidence vector, so that the code is clearly generated by this set of vectors. The 2-nd order binary Reed–Muller code contains the pointwise product of every pair of vectors of the 1-st order code. In particular it contains the incidence vectors of points and \( (m - 2) \)-dimensional spaces of \( EG(m, 2) \), and is generated by this set of vectors, and so on. Clearly all these codes are invariant under the collineation group of \( EG(m, 2) \), regarded as a permutation group on the points, which corresponds to the coordinate places of a code vector. These geometric properties were implicitly used in the majority decoding algorithm devised by Reed [22]. A first attempt to extend these properties to nonbinary codes was made by Dwork and Heller [9]. But it was the discovery by Kasami, Lin, and Peterson [13, 14] of the extended-cyclic structure of the binary Reed–Muller Codes, and their natural generalization to the nonbinary case, which gave the initial impulse in the investigation of generalized Reed–Muller (G.R.M.) codes. Quite independently, Rudolph [23] discovered a new class of codes with a majority decoding algorithm based on the properties of finite geometries. Some important questions about these
codes remained unanswered, such as the determination of their dimension and minimum distance. These questions were solved by Graham and MacWilliams [11] for the subclass of difference-set codes, discovered by Weldon [25]. By an extension of the methods of Graham and MacWilliams, Goethals and Delsarte [10] solved the problem for the whole class of projective-geometry codes, while Weldon [27], working independently, found similar results in the binary case, using methods of Kasami, Lin, and Peterson [14]. Using the same approach, Euclidean geometry codes were studied by Weldon [26]. Some additional results on these geometric codes were obtained by Chow [3, 4], Smith [24] and MacWilliams and Mann [18]. By an extension of the definition of finite geometry, Delsarte [5] introduced a new class of codes, which contains the projective and Euclidean geometry codes, and which are majority decodable, in a way quite similar to one of the methods proposed by Weldon [28]. A first attempt to unify the treatment of all these codes by a polynomial approach was made by Kasami, Lin, and Peterson [15]. The basic idea of this polynomial approach, which was implicitly contained in Lin [16], was later applied to geometric codes by Lin [17].

The present paper originated from a report by Delsarte and Goethals [8] in which some results obtained by Lin [16] in the binary case were extended to the $q$-ary case (Theorem 2.6.3 of the present paper). The main objectives of our paper are to provide a somewhat formalized formulation of the polynomial approach of Kasami, Lin, and Peterson, and to collect a number of results (which appeared or will appear in other papers) which are strongly related to the polynomial formulation of G.R.M. codes. In addition to this reformulation, the main contributions are: (i) a clear distinction between the two ways of restricting G.R.M. codes to subcodes, that is, the nonprimitive and the subfield subcodes (ii) an extensive study of the interrelations between the $m$-variable approach of Kasami, Lin, and Peterson, and the 1-variable approach of Mattson and Solomon [20]; (iii) an expanded treatment of the automorphism group, both in the $m$-variable and in the 1-variable language; (iv) an enumeration of the number of minimum weight vectors of $q$-ary G.R.M. codes; and (v) introduction of a new series of majority decodable geometric codes (Section 5.3). The matter is organized in five sections. The first section introduces some material for the polynomial approach; the second contains an extensive study of the (primitive) G.R.M. codes; Sections 3 and 4 are devoted, respectively, to the nonprimitive and subfield subcodes; finally geometric codes are briefly discussed in Section 5. The proof of Theorem 2.6.3, which is rather long, is given in the appendix.
1. Definitions and Preliminaries

Let \( q = p^t \), \( p \) a prime; \( E = GF(q) \); \( E^m \) = the set of \( m \)-tuples of elements of \( E \).

Let

\[ \bar{x} = (x_1, x_2, \ldots, x_m) \]  

(1)

be a generic element of \( E^m \), and \( P(\bar{x}) \) any polynomial in the \( m \) variables \( x_1 \cdots x_m \), with coefficients in \( E \).

**Lemma 1.1.** Let \( \omega \) be any element of \( E \), \( x \) an indeterminate; then, one has, in \( E \)

\[ \prod_{\alpha \in E \atop \alpha \neq \omega} (x - \alpha) = (x - \omega)^{q-1} - 1. \]  

(2)

**Proof.** It is well-known that the \( q \) elements of \( E \) are roots of \( x^q - x \), and, over \( E \),

\[ x^q - x = (x - \omega)^q - (x - \omega). \]

Dividing both sides by \( x - \omega \), one obtains the desired result.

**Corollary 1.2.** The polynomial

\[ P_\omega(\bar{x}) = \prod_{i=1}^{m} [1 - (x_i - \omega_i)^{q-1}] \]  

(3)

has value zero at every point of \( E^m \), except at the point

\[ \bar{x} = \bar{\omega} = (\omega_1, \omega_2, \ldots, \omega_m), \]

where it assumes the value 1.

The value of a given polynomial \( P(\bar{x}) \) at any point of \( E^m \) is unchanged if \( x_i^q \) is replaced by \( x_i \), or, in other words, if \( P(\bar{x}) \) is reduced \( \text{mod}(x_i^q - x_i) \), \( i = 1, 2, \ldots, m \). Every polynomial in reduced form is uniquely expressed as a sum of terms

\[ P(\bar{x}) = \sum_{i_k} c_{x_1^{i_1}x_2^{i_2} \ldots x_m^{i_m}} \]  

(4)

where

\[ 0 \leq i_k \leq q - 1. \]
Lemma 1.3. A polynomial $P(\bar{x})$ cannot assume the value zero at every point of $E^m$, unless its reduced form is identically zero.

Proof. Consider the polynomial in $x_i$
\[
f(x_i) = P(\omega_1, \ldots, \omega_{i-1}, x_i, \omega_{i+1}, \ldots, \omega_m)
\]
obtained from the reduced form of $P(\bar{x})$ by assigning fixed values $\omega_j$ to each of the remaining variables. This polynomial has degree at most $q - 1$ and thus cannot be zero for each $x_i$ in $E$, unless it is identically zero. Since this is true whatever the $\omega_j$ and the variable $x_i$ are, the lemma is easily proved by induction. We assume that all polynomials are in reduced form, unless specifically stated otherwise.

Lemma 1.4. The reduced form $P(\bar{x})$ of a polynomial is uniquely determined by the set of $q^m$ values it assumes on each point of $E^m$. More precisely,
\[
P(\bar{x}) = \sum_{\omega \in E^m} P(\bar{\omega}) F_{\omega}(\bar{x})
\]
where the $F_{\omega}(\bar{x})$ are the $q^m$ polynomials (3), each of which is associated with a given point $\bar{\omega}$ of $E^m$.

Proof. Both sides of (5) are polynomials in reduced form, assuming the value $P(\bar{\omega})$ at every point $\bar{\omega}$ of $E^m$. Thus, according to Lemma 1.3, the difference is identically zero.

Let us denote by $P(m, q)$ the set of polynomials $P(\bar{x})$ (in reduced form), in the indeterminate $\bar{x} \in E^m$, over $E = GF(q)$.

Theorem 1.5. The set $P(m, q)$ of polynomials $P(\bar{x})$ is a $q^m$-dimensional vector space over $E$.

Proof. From Lemma 1.4, every polynomial in the set can be expressed as a linear combination of the $q^m$ polynomials $F_{\omega}(\bar{x})$, which, from Lemma 1.3, are linearly independent, and thus form a basis for $P(m, q)$.

The set of $q^m$ monomials
\[
x_1^{i_1}x_2^{i_2} \cdots x_m^{i_m}, \quad 0 \leq i_k \leq q - 1, \quad k = 1, 2, \ldots, m,
\]
is another basis for $P(m, q)$. Let us denote by $P_\nu(m, q)$ the subspace of $P(m, q)$ generated by the subset of monomials whose degrees do not exceed a given integer $\nu \leq m(q - 1)$, i.e., those monomials (6) for which
\[
\sum_{k=1}^{m} i_k \leq \nu.
\]
Of course, for \( v = m(q - 1) \), \( P_v(m, q) \) is the space \( P(m, q) \) itself. For \( v < m(q - 1) \), let us define \( \mu \) by
\[
\nu + \mu + 1 = m(q - 1) \tag{8}
\]
We prove three lemmas which will be useful later on.

**Lemma 1.6.** If \( P(\bar{x}) \) has degree \(< m(q - 1) \), then
\[
\sum_{\bar{\omega} \in E^m} P(\bar{\omega}) = 0.
\]

**Proof.**
\[
F_\omega(x) = \prod_{i=1}^{m} \left[ 1 - (x_i^{q-1} + \omega_1 x_i^{q-2} + \cdots + \omega_i^{q-1}) \right]
= (-1)^{m} (x_1 x_2 \cdots x_m)^{q-1} + \text{terms of lower degree.}
\]
\[
\sum_{\bar{\omega} \in E^m} P(\bar{\omega}) \quad \text{is the coefficient of} \quad (-1)^{m} (x_1 x_2 \cdots x_m)^{q-1}\quad \text{in} \quad P(\bar{x});\quad \text{since the degree of} \quad P(\bar{x}) < m(q - 1),\quad \text{this coefficient is zero.}
\]
Let \( j_1, j_2, \ldots, j_m \) be integers, \( 0 \leq j_k \leq q - 1, j = \sum_{k=1}^{m} j_k \leq \mu. \)

**Lemma 1.7.** For \( P(\bar{x}) \in P_v(m, q) \), \( \sum_{\omega \in E^m} \omega_1^{j_1} \cdots \omega_m^{j_m} P(\bar{\omega}) = 0. \)

**Proof.** Apply 1.6 to the polynomial \( x_1^{j_1} \cdots x_m^{j_m} P(\bar{x}) \), of degree \( \leq \mu + v < m(q - 1). \)

For any integer \( a \), and any base \( S \), define \( w_S(a) \), the \( S \)-weight of \( a \), as the ordinary integer sum of the digits of the \( S \)-ary expansion of \( a \):
\[
a = \sum_{i=0}^{\infty} a_i S^i; \quad w_S(a) = \sum_{i=0}^{\infty} a_i .
\]

Let \( \alpha_1, \alpha_2, \ldots, \alpha_m \) be elements in any extension field \( GF(q^r) \) of \( E \), \( \bar{\omega} \) any element of \( E^m \), and denote by \((\bar{\omega}, \bar{\alpha})\) the scalar product
\[
(\bar{\omega}, \bar{\alpha}) = \alpha_1 \omega_1 + \alpha_2 \omega_2 + \cdots + \alpha_m \omega_m,
\]
which is an element of \( GF(q^r) \).

**Lemma 1.8.** For any polynomial \( P(\bar{x}) \) in \( P_v(m, q) \) and any integer \( u \) whose \( q \)-weight is less than or equal to \( \mu \), the sum
\[
\sum_{\omega \in E^m} (\omega, \bar{\alpha})^u P(\bar{\omega})
\]
is identically zero in \( GF(q^r) \).
Proof. Let \( u = u_0 + u_1 q + u_2 q^2 + \cdots + u_S q^S \), be the \( q \)-ary expansion of \( u \). Then, in any extension field \( GF(q^r) \) of \( E = GF(q) \),

\[
\sum_{\omega \in E^m} (\bar{\omega}, \bar{x})^u P(\bar{\omega}) = \sum_{\omega \in E^m} \left[ \prod_{i=0}^S (\bar{\omega}, \bar{x}^i) u_i \right] P(\bar{\omega}). \tag{9}
\]

Now, the expression under brackets in the right-hand side can be expanded as a sum of the form

\[
\sum C(\bar{x}) \omega_1^{j_1} \omega_2^{j_2} \cdots \omega_m^{j_m},
\]

where each term has degree less than or equal to

\[
\sum_{i=0}^S u_i = \omega_q(u) \leq \mu,
\]

and thus, from Lemma 1.7, the sum (9) is separately zero for each such term, hence proving the result.

2. PRIMITIVE G.R.M. CODES

2.1. Definition of G.R.M. Codes

Let \( V_k \) be any \( k \)-dimensional subspace in a given \( n \)-dimensional vector space \( V_n \) over \( E \), and let \( v_1, v_2, \ldots, v_n \) be any given basis of \( V_n \).

A \((n, k)\) linear code over \( E \) can be defined as the image of \( V_k \), with respect to the given basis \( v_1, v_2, \ldots, v_n \) of \( V_n \), in \( E^n \); that is the \( n \)-tuple

\[
(a_1, a_2, \ldots, a_n)
\]

of elements of \( E \) is a code-vector if the vector

\[
v = a_1 v_1 + a_2 v_2 + \cdots + a_n v_n
\]

belongs to \( V_k \). The length of the code is \( n \), and \( k \) its dimension.

The \( v \)-th order G.R.M. code \( C_v(m, q) \) of length \( q^m \) over \( E \) will be defined as the image of \( P_v(m, q) \) with respect to the basis \( \{F_v(\bar{x})\} \) of \( P(m, q) \). According to Lemma 1.4, the \( q^m \) coordinates of a given code vector are the values \( P(\bar{\omega}) \) assumed by a given polynomial \( P(\bar{x}) \) in \( P_v(m, q) \) on each of the \( q^m \) points of \( E^m \). If \( 0, \bar{\omega}_1, \bar{\omega}_2, \ldots, \bar{\omega}_v, v = q^m - 1 \), is some ordering of the points of \( E^m \), a typical code vector is

\[
P(\bar{0}), P(\bar{\omega}_1), P(\bar{\omega}_2), \ldots, P(\bar{\omega}_v).
\]
2.2. Dual Codes

Two vectors \( a, b \) are said to be orthogonal (properly quasiothogonal, but we shall never define any other sort) if the scalar product \( \langle a, b \rangle \) is zero in \( E \).

The dual code of a linear code \( C_k \) of dimension \( k \) of \( E^n \) is the set of vectors of \( E^n \) which are orthogonal to every vector of \( C_k \). This is clearly a linear code of dimension \( n - k \). We recall that \( \mu \) is defined by \( \nu + \mu + 1 = m(q - 1) \).

**Theorem 2.2.1.** \( C_s(m, q) \) and \( C_\mu(m, q) \) are dual codes.

The proof of this theorem, which can easily be derived from Kasami, Lin, and Peterson [14], already appeared in Lin [16].

2.3. Automorphism group

The automorphism group of a linear \((n, k)\) code is the largest group, all of whose elements, acting as permutations of the \( n \) coordinate places, transform code vectors into code vectors.

Let \( g_2 \) be any \( m \times m \) nonsingular matrix over \( E \), and \( \omega_0 \) any given point of \( E^m \). Then, the substitution

\[
\bar{x} \rightarrow \bar{y} = \bar{x} \Omega + \omega_0
\]  

acts as a permutation on the \( q^m \) points of \( E^m \).

It is well-known that the set of substitutions (10) forms a group, namely the general linear nonhomogeneous group \( \text{GLNH}(m, q) \) which, for the sake of simplicity, will be denoted by \( G(m, q) \). Its order is

\[
| G(m, q) | = q^m(q^m - 1)(q^m - q) \cdots (q^m - q^{m-1}).
\]

Since, obviously, any substitution (10) cannot transform a polynomial in \( P_s(m, q) \) into a polynomial of higher degree, the following theorem, quoted by Lin [16], is easily derived.

**Theorem 2.3.1.** The group \( G(m, q) \) acting as a permutation group on the \( v + 1 \) \((=q^m)\) coordinate places, is contained in the automorphism group of any G.R.M. code \( C_s(m, q) \).

Let \( \alpha \) be a primitive root in \( GF(q^m) \). Then \( \alpha \) satisfies an irreducible equation of degree \( m \) over \( E \). In fact, this equation is \( \epsilon(x) = 0 \), with

\[
\epsilon(x) = \prod_{j=0}^{m-1} (x - \alpha^j) = \sum_{t=0}^{m} \epsilon_t \alpha^t, \quad \epsilon_t \in E, \quad \epsilon_m = 1.
\]
Let $S$ be any $m \times m$ matrix over $E$, whose minimal polynomial is $e(x)$. $S$ may, for instance, be the companion matrix of $e(x)$

$$S = \begin{pmatrix}
0 & 1 & 0 & 0 & \cdots & 0 \\
0 & 0 & 1 & 0 & \cdots & 0 \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & 0 & \cdots & 1 \\
\end{pmatrix}. \tag{12}$$

Then, $S$ generates a cyclic subgroup of order $q^m - 1$ in $G(m, q)$, namely the group of substitutions of the form

$$\bar{x} \rightarrow \bar{x}S^i, \quad 0 \leq i \leq q^m - 2,$$

which leaves the point $\bar{0} = (0, 0, \ldots, 0)$ of $E^m$ unchanged. The whole subgroup of $G(m, q)$, all of whose substitutions leave the point $\bar{0}$ of $E^m$ unchanged, clearly is the general linear homogeneous group, $GLH(m, q)$, of substitutions of the form

$$\bar{x} \rightarrow \bar{x}\Omega.$$

For the sake of simplicity, this group will be denoted by $H(m, q)$. Its order is known to be

$$|H(m, q)| = \frac{1}{q^m} |G(m, q)|.$$

Let us define the punctured G.R.M. code $HC_v(m, q)$ to be the code of length $q^m - 1$ over $E$, obtained by systematically deleting the coordinate $P(\bar{0})$ from any vector in $C_v(m, q)$. By Lemma 1.6 this does not change the dimension of the code. From the preceding remarks, one easily deduces

**Theorem 2.3.2.** The group $H(m, q)$, acting as a permutation group of degree $q^m - 1$, is contained in the automorphism group of any punctured G.R.M. code $HC_v(m, q)$ of length $q^m - 1$.

**Corollary 2.3.3.** The punctured G.R.M. codes $HC_v(m, q)$ of length $q^m - 1$ are equivalent to cyclic codes. In fact, $HC_v(m, q)$ is a cyclic code if the coordinates are permuted so as to appear in the order

$$P(\bar{e}), P(\bar{e}S), P(\bar{e}S^2), \ldots, P(\bar{e}S^{q^m-2}),$$

where $\bar{e}$ is any nonzero element of $E^m$, for instance $\bar{e} = (1, 0, 0, \ldots, 0)$, as in the rest of this paper.
2.4. 1-variable Approach [Mattson and Solomon [20]]

Since $HC_v(m, q)$ is a cyclic code it is possible to define it in another way. We do this in a form which will make it clear how the $m$-variable and the 1-variable approach are connected.

As before set $v = q^m - 1$, and let $\alpha$ be a primitive element of $K = GF(q^m)$—in fact the same $\alpha$ as in (11). Let $z$ be a generic power of $\alpha$. If $Q(z)$ is a polynomial in $z$ with coefficients in $K$ we may reduce it mod $z^v - 1$ ($z$ is not allowed to be 0); its reduced form is given by

$$Q(z) = \sum_{i=0}^{v-1} Q(\alpha^i) G_i(z),$$

(13)

where

$$G_i(z) = \frac{1}{v} \alpha^i \frac{z^v - 1}{z - \alpha^i}$$

(14)

is zero for every value of $z$ except $\alpha^i$, and there one. The set of polynomials $G_i(z)$ clearly forms a basis for the algebra $K[z]/z^v - 1$. The set of monomials $1, z, z^2, ..., z^{v-1}$ forms another basis. If

$$Q(z) = \sum_{j=0}^{v-1} c_j z^j, \quad c_j \in K,$$

(15)

one easily deduces from (13) that

$$c_j = \frac{1}{v} \sum_{i=0}^{v-1} Q(\alpha^i) \alpha^{(v-j)i}.$$  

(16)

Let $K_v[z]$ denote the subset of polynomials $Q(z)$ which have the property that

$$Q(\alpha^i) \in E = GF(q) \quad \text{all } i.$$  

(17)

From (16) we have then

$$c_j^q = \frac{1}{v} \sum_{i=0}^{v-1} Q(\alpha^i) \alpha^{-ji} = c_{qj},$$

$qj$ taken mod $q^m - 1$, and from (15) $c_j^q = c_{qj}$ implies

$$Q(z) = Q(z^q) = Q(z)^q,$$

so that $Q(z) \in E$ for all values of $z$ in $K$. Thus (17) holds if and only if

$$c_j^q = c_{qj}, \quad \text{subscripts mod } q^m - 1.$$  

(18)
For $Q[z] \in K_v[z]$, set

$$a(x) = \sum_{i=0}^{v-1} Q(x^i) x^i.$$  \hfill (19)

**Lemma 2.4.1.** The set of polynomials defined by (19) is exactly the polynomial ring $E[x]/x^v - 1$.

**Proof.** Clearly $a(x) \in E[x]/x^v - 1$. Suppose

$$b(x) = \sum_{i=0}^{v-1} b_i x^i \in E[x]/x^v - 1.$$  
Set

$$Q(z) = \frac{1}{v} \sum_{i=0}^{v-1} b(x^{-i}) z^i$$

that is

$$Q(z) = \sum_{j=0}^{v-1} c_j z^j,$$

where

$$c_j = \frac{1}{v} b(a^{-j}).$$  \hfill (20)

Then

$$Q(x^s) = \frac{1}{v} \sum_{i=0}^{v-1} b(\alpha^{-i}) \alpha^{is}$$

$$= \frac{1}{v} \sum_{j=0}^{v-1} b_j \sum_{i=0}^{v-1} \alpha^{i(s-j)}.$$  
Now

$$\sum_{i=0}^{v-1} \alpha^{i(s-j)} = \begin{cases} 0 & s \neq j \\ v & s = j. \end{cases}$$

Thus

$$Q(x^s) = b_s.$$  

Let $g(x)$ be a divisor of $x^v - 1$. A polynomial $b(x)$ of $E[x]/x^v - 1$ belongs to the ideal (cyclic code) generated by $g(x)$ if and only if $b(\alpha^{v-j}) = 0$ for all zeros $\alpha^{v-j}$ of $g(x)$. The corresponding $Q(x) = \sum_{j=0}^{v-1} c_j z^j$ of $K_v[z]$ has, by (20), the property that $c_j = 0$ if $\alpha^{-j}$ is a zero of $g(x)$. By extension we call such $\alpha^{-j}$ the "zeros of the code."
If \( g(x) \) has degree \( v = k \) the ideal it generates has dimension \( k \), and the image of this ideal in \( K_v[z] \) is generated by the \( k \) basis monomials \( z^i \), \( g(z^i) \neq 0 \). Reciprocally, any cyclic \((v, k)\) code over \( E \) can be defined as the image with respect to basis \((14)\) of a \( k \)-dimensional subspace of \( K_v[z] \) defined by the property that \( c_j = 0 \) whenever \( \alpha^{-j} \) is a zero of the code.

We may extend any cyclic code by adjoining to a vector \((a_0, a_1, \ldots, a_{v-1})\) an extra coordinate \( a_\infty \) defined by

\[
a_\infty = \frac{1}{v} \sum_{i=0}^{v-1} a_i = \frac{1}{v} \sum_{i=0}^{v-1} Q(\alpha^i),
\]

which, from \((13)\) and \((14)\), is seen to be

\[
a_\infty = Q(0) = c_0.
\]

In our case \( v = q^m - 1 \), so that \( Q(0) = -\sum_{i=0}^{q^m-1} Q(\alpha^i) \). Such a code will be called an extended cyclic code (see Berlekamp [1]). Of course the extra coordinate is always zero if \( 1 = \alpha^0 \) is a zero of the code.

We return now to the G.R.M. codes.

It is well known that \((1, \alpha, \alpha^2, \ldots, \alpha^{m-1})\) is a basis for \( GF(q^m) \) as a vector space over \( E \). Let

\[
\bar{\alpha} = (1, \alpha, \alpha^2, \ldots, \alpha^{m-1}).
\]

Suppose the nonzero \( \bar{\omega}_i \) of \( E^m \) arranged as in 2.3.3. The mapping

\[
\bar{0} \to 0, \quad \bar{\omega}_i \to \alpha^i = (\bar{\alpha}^i, \bar{\alpha})
\]

is an isomorphism between the vector space structures of \( E^m \) and \( GF(q^m) \). From the fact that \( \alpha^i = (\bar{\alpha}^i, \bar{\alpha}) \) and from Lemma 1.8, we get immediately the following theorem, which is equivalent to Theorem 1 of Kasami, Lin, and Peterson [14].

**Theorem 2.4.2.** The elements \( \alpha^u, u \neq 0 \), are zeros of the codes \( HC_\epsilon(m, q) \) and \( C_\epsilon(m, q) \) if and only if \( \omega_\epsilon(u) \leq \mu = m(q - 1) - v - 1 \).

We wish to extend \((22)\) to obtain a mapping between polynomials \( P(\bar{x}) \) in \( x_1, \ldots, x_m \) and polynomials \( Q(z) \) in \( z \). Now \( \bar{x} \) represents a generic vector of \( E^m \), including zero, and \( z \) a generic power of \( \alpha \) which cannot be zero; clearly zero will be a special case. For \( \bar{x} \neq \bar{0} \), the correspondence

\[
\bar{x} = (x_1, x_2, \ldots, x_m) \leftrightarrow (\bar{x}, \bar{\alpha}) = x_1 + x_2\alpha + \cdots + x_m\alpha^{m-1} = z
\]

does not enable us to turn polynomials into polynomials in either direction. For this we need a subsidiary lemma.
For \( \lambda \in GF(q^m) \) define the \( E \)-trace of \( \lambda \)

\[
T_E(\lambda) = \lambda + \lambda^q + \lambda^{q^2} + \cdots + \lambda^{q^{m-1}}.
\]

**Lemma 2.4.3.** For any basis \( \alpha_1, \alpha_2, \ldots, \alpha_m \) of \( GF(q^m) \) over \( E \), there exists a complementary basis \( \lambda_1, \lambda_2, \ldots, \lambda_m \) such that

\[
T_E(\lambda_i, \alpha_j) = \begin{cases} 0 & i \neq j \\ 1 & i = j. \end{cases}
\]

**Proof.** Let \( A \) be the matrix

\[
A = \begin{pmatrix}
\alpha_1 & \alpha_1^q & \cdots & \alpha_1^{q^{m-1}} \\
\alpha_2 & \alpha_2^q & \cdots & \alpha_2^{q^{m-1}} \\
\cdots & \cdots & \cdots & \cdots \\
\alpha_m & \alpha_m^q & \cdots & \alpha_m^{q^{m-1}}
\end{pmatrix}
\]

which is known to be invertible since \( \alpha_1 \cdots \alpha_m \) are linearly independent over \( E \). Let \([A]\) be the determinant of \( A \). Since \([A]^q = [A] \), \([A] \in E \). Let \( A^{-1} = (\mu_{ij})/[A] \). By elementary algebra

\[
\mu_{11} = \det \begin{pmatrix}
\alpha_2^q & \cdots & \alpha_2^{q^{m-1}} \\
\cdots & \cdots & \cdots \\
\alpha_m^q & \cdots & \alpha_m^{q^{m-1}}
\end{pmatrix}, \quad \mu_{21} = \det \begin{pmatrix}
\alpha_2^{q^2} & \cdots & \alpha_2^{q^{m-1}} & \alpha_2 \\
\cdots & \cdots & \cdots & \cdots \\
\alpha_m^{q^2} & \cdots & \alpha_m^{q^{m-1}} & \alpha_m
\end{pmatrix}.
\]

Thus \( \mu_{21} = \mu_{11}^q \), similarly \( \mu_{31} = \mu_{11}^{q^2} \) and so on.

We have seen that

\[
A^{-1} = \begin{pmatrix}
\lambda_1 & \lambda_2 & \cdots & \lambda_m \\
\lambda_1^q & \lambda_2^q & \cdots & \lambda_m^q \\
\cdots & \cdots & \cdots & \cdots \\
\lambda_1^{q^{m-1}} & \lambda_2^{q^{m-1}} & \cdots & \lambda_m^{q^{m-1}}
\end{pmatrix}.
\]

Clearly \( \lambda_1, \lambda_2, \ldots, \lambda_m \) are linearly independent over \( E \). From the equation \( AA^{-1} = I \) we obtain the desired result. For future use we note that the equation \( A^{-1}A = I \) gives

\[
\sum_{i=1}^m \lambda_i^q \alpha_i^q = 1, \quad \sum_{i=1}^m \lambda_i^q \alpha_i^k = 0 \quad j \neq k.
\]
Now take \( \lambda_1, \lambda_2, \ldots, \lambda_m \) to be the complementary basis of \( 1, \alpha, \alpha^2, \ldots, \alpha^{m-1} \).
Then
\[
z = x_1 + x_2 \alpha + \cdots + x_m \alpha^{m-1} \iff x_i = T_E(\lambda_i z).
\]
(24)
To express \( P(\bar{x}) \) as a polynomial in \( z \), set
\[
x_i = T_E(\lambda_i z).
\]
(25)
The coefficients of \( P(\bar{x}) \) (in \( E \)) are unchanged.

**Lemma 2.4.4.** If \( P(\bar{x}) \in P_r(m, q) \) and \( Q(z) = \sum_{j=0}^{v-1} c_j z^j \) is obtained from \( P(\bar{x}) \) by (25), then \( c_j = 0 \) whenever \( w_q(j) > v \).

**Proof.**
\[
P(\bar{x}) = \sum_{i_1, i_2, \ldots, i_m} c_{i_1 i_2 \cdots i_m} x_1^{i_1} x_2^{i_2} \cdots x_m^{i_m},
\]
with
\[
0 \leq i_k \leq q - 1; \quad \sum_{k=1}^{m} i_k \leq v.
\]
Its image \( Q(z) \) appears as a sum of terms of the form
\[
T_{E}^{i_1}(\lambda_1 z) T_{E}^{i_2}(\lambda_2 z) \cdots T_{E}^{i_m}(\lambda_m z).
\]
(26)
Expanding a typical term of (26), one obtains
\[
T_{E}^{i_k}(\lambda_k z) = (\lambda_k z + (\lambda_k z)^q + \cdots + (\lambda_k z)^{q^{m-1}})^{j_k}
\]
\[
= \sum_{j_k} c_{j_k} (\lambda_k z)^{y_k}
\]
with
\[
j_k = j_{k,0} + j_{k,1}q + j_{k,2}q^2 + \cdots + j_{k,m-1}q^{m-1},
\]
and
\[
c_{j_k} = \frac{i_k!}{(j_{k,0})! \cdots (j_{k,m-1})!},
\]
\[
i_k = \sum_{i=0}^{m-1} j_{k,i} = w_q(j_k).
\]
Thus \( Q(z) \) contains only terms of the form
\[
\prod_{k=1}^{m} (\lambda_k z)^{y_k} \text{ of degree } \sum_{k=1}^{m} j_k \mod q^m - 1.
\]
Now
\[ w_q \left( \sum_{k} j_k \mod q^m - 1 \right) \leq w_q \left( \sum_{k} j_k \right) \leq \sum_{k} w_q(j_k) = \sum_{k} i_k \leq v. \]
Thus \( z^j \) occurs with nonzero coefficient in \( Q(z) \) only if \( w_q(j) \leq v \).

**Lemma 2.4.5.** With the same hypotheses as 2.4.4

\[ Q(\alpha^v) = P(\omega); \text{ thus } Q(\alpha^q) \in E. \]

**Proof.**

\[ Q(z) = P(T_E(\lambda_1 z), T_E(\lambda_2 z), \ldots, T_E(\lambda_m z)). \]

Set \( z = \alpha^v = \omega_{x_1} + \omega_{x_2} + \cdots + \omega_{x_m} \alpha^{m-1} \), where \( (\omega_{x_1}, \ldots, \omega_{x_m}) = \bar{E} \).
Then \( T_E(\lambda_1 \alpha^v) = \omega_{x_1} \), so \( Q(\alpha^v) = P(\omega). \)

Let \( Q_n[z] \) be the subset of polynomials of \( \bar{K}_n[z] \) with the property that \( w_q(j) \geq v \). We have shown that (25) maps \( P_\nu(m, q) \) into the set \( Q_n[z] \). We now show that the mapping is onto as follows: Let

\[ F_j(z) = (c_{j_1} z^{j_1} + c_{j_2} z^{j_2} + \cdots + c_{j_m} z^{j_m}) \]

where \( d \) is the least positive integer such that

\[ jq^d \equiv j \mod v. \]

From (18) \( K_n[z] \) is generated over \( E \) by the distinct polynomials \( F_j(z) \) and we may write

\[ F_j(z) = c_{j_1} z^{j_1} + c_{j_2} z^{j_2} + \cdots + c_{j_m} z^{j_m}. \]

Let \( j = i_1 + i_2 q + \cdots + i_m q^{m-1} \). Then

\[ q j \mod q^m - 1 = i_m + i_1 q + \cdots + i_{m-1} q^{m-1}, \quad (27) \]

so that \( w_q(j) = w_q(qj) = w_q(q^2 j) = \cdots \). We set \( w_q(F_j(z)) = w_q(j) \). By 2.4.4 \( Q_n[z] \) is generated over \( E \) by the polynomials \( F_j(z) \) for which \( w_q(F_j(z)) \leq v \). \( Q_n[z] \) is a linear space over \( E \).

Let \( U_\nu \) be the set of integers \( j, 0 \leq j \leq q^m - 1 \) such that \( w_q(j) \leq v \), and let \( |U_\nu| \) be the cardinality of \( U_\nu \).

**Lemma 2.4.6.** The dimension of \( Q_n[z] \) over \( E \) is \( |U_\nu| \).
**Proof.** Let $j$ be an integer such that it is the least integer in the set $jq^k \mod q^m - 1$, $K = 0, 1, m = 1$ and let $d_j$ be the number of distinct integers in this set. Note that this definition implies that $d_j$ divides $m$. Then

$$|U_v| = \sum_{w_q(j) \leq v} d_j.$$

Now $c_j^q = c_{jq}$ implies $c_j^{d_j} = c_j$, so that $c_j \in GF(q^{d_j})$ [which is a subfield of $GF(q^m)$]. The number of choices for $c_j$ in a polynomial of $Q_v[z]$ is $q^{d_j}$. Thus the number of distinct polynomials in $Q_v[z]$ is

$$\prod_{w_q(j) \leq v} q^{d_j} = q^{|U_v|}.$$

**Lemma 2.4.7.** The dimension of $P_v(m, q)$ is also $|U_v|$.

**Proof.** The dimension of $P_v(m, q)$ is the number of distinct sets of integers

$$i_1 i_2 \ldots i_m, \quad 0 \leq i_k \leq q - 1, \quad \Sigma i_k \leq v.$$

Set $j = i_1 + i_2 q + \cdots + i_m q^{m-1}$; then $0 \leq j \leq q^m - 1$, $w_q(j) \leq v$. The number of distinct integers in the set $jq^k \mod q^m - 1$ is, by (27), the number of distinct cyclic permutations of $i_1, i_2, \ldots, i_m$. Thus the dimension of $P_v(m, q) = |U_v|$.

We now have

**Theorem 2.4.8.** The code HC_v(m, q) is the image of the set $Q_v[z]$ with respect to basis (14).

**Proof.** The mapping (25) sets up a (one-to-one) correspondence between $P_v(m, q)$ and $Q_v[z]$, which by 2.4.5 maps the vector $P(\bar{e}), P(\bar{e}S), \ldots, P(\bar{e}S^{v-1})$ of $HC_v(m, q)$ onto $Q(1), Q(\alpha), \ldots, Q(\alpha^{v-1})$.

Since from Lemma 1.6

$$P(\bar{e}) = -\sum_{i=0}^{v-1} P(\bar{e}S^i),$$

and from (21)

$$Q(0) = \frac{1}{v} \sum_{i=0}^{v-1} Q(\alpha^i) = -\sum_{i=0}^{v-1} Q(\alpha^i),$$

$P(\bar{e}) = Q(0)$ and we may define $C_v(m, q)$ as the set of vectors $Q(0), Q(1), Q(\alpha), \ldots, Q(\alpha^{v-1})$ for $Q(z) \in Q_v[z]$. We obtain immediately a second proof of 2.4.2
Since \( c_j = 0 \) whenever \( \alpha^{v-j} \) is a zero of the code, the zeros of \( HC_q(m, q) \) are \( \alpha^{v-a} \), where \( w_q(a) > v \). Now
\[
w_q(q^m - 1 - a) = m(q - 1) - w_q(a) < m(q - 1) - v = \mu + 1.
\]
Thus \( \alpha^u, u \neq 0 \), is a zero of \( HC_q(m, q) \) if and only if \( w_q(u) \leq \mu \).
For future use we investigate a little more carefully the relation between \( P_q(m, q) \) and \( Q_u[z] \).

**Lemma 2.4.9.** The inverse mapping from \( z \) to \( \bar{z} \) is given by
\[
Q(z) \rightarrow Q((\bar{x}, \bar{\alpha})) = P(\bar{x});
\]
it maps \( Q_u[z] \) onto \( P_q(m, q) \). This simply results from (24), Lemmas 2.4.6 and 2.4.7.

**Lemma 2.4.10.** Suppose \( Q_u(z) = \sum_k c^k_u z^u \). Set \( \bar{x} = (\alpha_1, ..., \alpha_m) \) (for ease of notation). Equation (24) transforms \( Q_u(z) \) into
\[
F_u(\bar{x}) = \sum_k c^k_u (x_1^{\alpha_1} + \cdots + x_m^{\alpha_m})^u.
\]
Then one has, after reduction mod \( (x_i^q - x_i) \)
\[
F_u(\bar{x}) = \sum_{l_1, \ldots, l_m} d(l_1, \ldots, l_m) x_1^{l_1} \cdots x_m^{l_m} (0 \leq l_i \leq q - 1)
\]
where \( d(l_1, \ldots, l_m) \in E \), and
\[
\sum_{i=1}^m l_i \text{ (mod } q - 1),
\]
for all sets \( \{l_i\} \).

**Proof.** Expanding \( F_u(\bar{x}) \), one has before reduction mod \( x_i^q - x_i \)
\[
F_u(\bar{x}) = \sum_h \Sigma b(h) x_1^{h_1} \cdots x_m^{h_m},
\]
with \( \Sigma h_i = w_q(u) \). Reduction mod \( x_i^q - x_i \) transforms \( x_i^{h_i} \) into \( x_i^{l_i} \), with \( l_i \leq h_i \) and \( l_i = h_i \) (mod \( q - 1 \)), hence proving the lemma.

2.5. **Description of the group \( G(m, q) \) in the 1-variable approach**

Let
\[
\bar{x} \rightarrow \bar{y} = \bar{x} \Omega + \bar{\alpha}_0 , \quad (\Omega, \bar{\alpha}_0) \in G(m, q).
\]
Then \( z = (\vec{x}, \vec{\alpha}) \) goes into \( \zeta = x' \Omega \vec{\alpha}' + \vec{\omega}_0 \vec{\alpha}' \) where \( \vec{\alpha}' \) denotes the transpose of \( \vec{\alpha} \). Let \( \lambda = (\lambda_1, \lambda_2, ..., \lambda_m), \lambda_\nu = (\lambda_1^\nu, \lambda_2^\nu, ..., \lambda_m^\nu), \) etc. By (25) we replace \( \vec{x} \) by \( \lambda \vec{x} + \lambda_2 \vec{\omega}^\nu + \cdots + \lambda_m^{m-1} \vec{\omega}^{m-1} \), thus

\[
z \to \zeta = z(\lambda \Omega \vec{\alpha}') + z'(\lambda \nu \Omega \vec{a}') + \cdots + z'^{m-1}(\lambda^{m-1} \Omega \vec{a}') + \vec{\omega}_0 \vec{a}'. \tag{28}\]

Now \( \Omega \vec{a}' = \vec{\beta}' \), where \( \vec{\beta} = (\beta_1, \beta_2, ..., \beta_m) \) is a basis of \( GF(q^m) \) over \( GF(q) \). Thus

\[
\zeta = \beta_1 T_E(\lambda_1 z) + \beta_2 T_E(\lambda_2 z) + \cdots + \beta_m T_E(\lambda_m z) + \vec{\omega}_0 \vec{a}',
\]

\[
T_E(\lambda_i z) \in \mathbb{E} \quad \text{for any choice of } z \in K. \tag{29}\]

\( \sum_{i=1}^m \beta_i T_E(\lambda_i z) \) is not zero if \( z \neq 0 \) since the \( \beta_i \) are linearly independent over \( \mathbb{E} \), and \( T(\lambda_i z) \) are not all zero for \( z \in K - \{0\} \). Hence \( \zeta = 0 \) has at most one solution in \( K \). It clearly has one, namely that given by \( \vec{x} = -\vec{\omega}_0 \Omega^{-1} \), that is \( z = -\vec{\omega}_0 \Omega^{-1} \vec{a}' \).

Polynomials of the form

\[
f(z) = \gamma_0 + \gamma_1 z + \gamma_2 z^2 + \cdots + \gamma_m z^{m-1}, \quad \gamma_i \in \mathbb{K} \tag{30}\]

are called affine polynomials (Berlekamp [1]) as their roots form an affine space over \( \mathbb{E} \). One easily verifies that for any \( a \in \mathbb{E} \)

\[
f(z_1 + a(z_2 - z_1)) = f(z_1) + a[f(z_1) - f(z_2)].
\]

The set of substitutions (28) is thus a set of affine polynomials over \( K \) having exactly one root in \( K \). In fact if \( f(z) \) in (30) is an affine polynomial with exactly one zero in \( K \), then \( z \to \zeta = f(z) \) is a transformation of the form (28) for some \( (\Omega, \vec{\omega}_0) \) in \( G(m, q) \). We prove this as follows.

**Theorem 2.5.1.** Let \( \zeta = \gamma_1 z + \gamma_2 z^2 + \cdots + \gamma_m z^{m-1} \) be an affine polynomial which has only one zero \( (z = 0) \) in \( GF(q^m) \). Then \( z \to \zeta \) is a transformation of the form (28) with \( \vec{\omega}_0 = 0 \).

**Proof.** From (28) and (29) it suffices to show that there is a basis \( \vec{\beta} = \beta_1, \beta_2, ..., \beta_m \) of \( GF(q^m) \) over \( \mathbb{E} \) such that

\[
\lambda \vec{\beta}' = \gamma_1, \lambda^\nu \vec{\beta}' = \gamma_2, ..., \lambda^{m-1} \vec{\beta}' = \gamma_m.
\]
From Lemma 2.4.3 this set of equations is equivalent to $A^{-1}\beta' = \gamma'$ or $\beta' = A\gamma'$, where now

$$A = \begin{pmatrix}
1 & 1 & \cdots & 1 \\
\alpha & \alpha^q & \cdots & \alpha^{q^{m-1}} \\
\alpha^2 & \alpha^{2q} & \cdots & \alpha^{2q^{m-1}} \\
\vdots & \vdots & \ddots & \vdots \\
\alpha^{m-1} & (\alpha^{m-1})^q & \cdots & (\alpha^{m-1})^{q^{m-1}}
\end{pmatrix}.$$  

It remains to show that the $\beta_1, \ldots, \beta_m$ so defined form a basis.

$$\beta_1 = \gamma_1 + \gamma_2 + \cdots + \gamma_m$$
$$\beta_2 = \gamma_1\alpha + \gamma_2\alpha^q + \cdots + \gamma_m\alpha^{q^{m-1}},$$
$$\vdots$$
$$\vdots$$
$$\vdots$$
$$\beta_m = \gamma_1\alpha^{m-1} + \gamma_2\alpha^{(m-1)q} + \cdots + \gamma_m(\alpha^{m-1})^{q^{m-1}}.$$  

If $a_1\beta_1 + a_2\beta_2 + \cdots + a_m\beta_m = 0$, $a_i \in E$, set

$$a = a_1 + a_2\alpha + \cdots + a_m\alpha^{m-1}.$$  

Then, by adding Eqs. (31),

$$\gamma_1a + \gamma_2a^q + \cdots + \gamma_m a^{q^{m-1}} = 0.$$  

From the definition of $\gamma'$ this implies $a = 0$, i.e., $a_i = 0$ for all $i$. Thus $\beta_1, \beta_2, \ldots, \beta_m$ are linearly independent over $GF(q)$.

**Corollary 2.5.2.** The number of affine polynomials of the form (30) with exactly one zero in $GF(q^m)$ is $|G(m, q)|$.

**Corollary 2.5.3.** If $f(z)$ is an affine polynomial with exactly one zero in $GF(q^m)$, then the transformation $z \rightarrow f(z)$ preserves the code $C_2(m, q)$.

### 2.6. Geometric Properties

It is well-known that: (i)—$E^m$ has the structure of an $m$-dimensional affine space or Euclidean Geometry $EG(m, q)$, (ii)—the set of points of $E^m$, satisfying $r$ linearly independent linear equations

$$\sum_{j=1}^{m} a_{ij}x_j = \omega_i, \quad i = 1, 2, \ldots, r,$$
over $E$, forms an $(m - r)$-dimensional affine subspace of $E^m$, or an $EG(m - r, q)$ contained in $EG(m, q)$.

Let us consider the polynomial

$$P(x) = \prod_{i=1}^{r} [1 - (x_i - \omega_i)^{q-1}], \quad (32)$$

of degree $r(q - 1)$, in $P(m, q)$, whose value is zero in $E^m$, unless

$$x_i = \omega_i, \quad i = 1, 2, \ldots, r, \quad (33)$$

where its value is one. Thus, the coordinate of $P(x)$, with respect to the basis polynomial $F_{\omega}(x)$ (3), is one or zero, according as the point $\omega$ of $E^m$ belongs or not to the $EG(m - r, q)$ defined by (33). These $q^m$ coordinates of $P(x)$ will be said to form the incidence vector of $EG(m - r, q)$. The following theorem, which already appeared in Kasami, Lin, and Peterson [15], is then easily derived.

**Theorem 2.6.1.** The code $C_v(m, q)$ contains the incidence vector of any $EG(m - r, q)$ if $v \geq r(q - 1)$.

Let $v = r(q - 1) + s$, $0 \leq s < q - 1$. Let

$$u_v = (q - s) q^{m-r-1} - 1. \quad (32)$$

**Theorem 2.6.2.** The code $HC_v(m, q)$ has minimum weight $u_v$, and $C_v(m, q)$ has minimum weight $u_v + 1$.

**Proof.** Kasami, Lin, and Peterson [14], Theorem 5.

Consider the polynomial

$$P(x) = \omega_0 \prod_{i=1}^{r} [1 - (x_i - \omega_i)^{q-1}] \prod_{j=1}^{s} (x_{r+1} - \omega_j) \quad (34)$$

of degree $r(q - 1) + s = v$, where $\omega_j$, in the last $s$ factors, are distinct elements of $E$ and the $\omega_i$ are arbitrary elements of $E$, with $\omega_0 \neq 0$. One easily sees that $P(x)$ is zero in $E^m$, unless

$$x_i = \omega_i, \quad i = 1, 2, \ldots, r, \quad (35)$$

$$x_{r+1} \neq \omega_j, \quad j = 1, 2, \ldots, s. \quad (36)$$

Since there are exactly $(q - s) q^{m-r-1}$ points in $E^m$ satisfying (35) and (36), the corresponding vector of $C_v(m, q)$ will have this weight. Let now the $\omega_i$,
in (35), be zero, and the \( \omega_j' \), in (36), be distinct from zero. Then, obviously, the point \( 0 = (0, 0, \ldots, 0) \) of \( E^m \) satisfies (35) and (36), and the corresponding code-vector of \( HC_v(m, q) \) will have weight \( u_v \).

Consider the \( q^{m-r-1} \) points of \( E^m \), satisfying (35) and the additional equation \( x_{r+1} = \omega_k^{e} \), where \( \omega_k^{e} \) is any element of \( E \), not among the \( \omega_j' \) in (36). These points belong to an \( EG(m-r-1, q) \); furthermore, \( P(\bar{x}) \), (34), assumes the constant value

\[
\epsilon_k = \omega_0 \prod_{j=1}^{s} (\omega_k^{e} - \omega_j'),
\]

(37)
on all these points. The same is true for any of the \( (q-s) \omega_k^{e} \) in \( E \), not among the \( \omega_j' \). The code-vector, defined by (34), is thus the sum (or union) of the incidence vectors of \( (q-s) EG(m-r-1, q) \), each of which is multiplied by a constant factor \( \epsilon_k \) (37). We emphasize that these \( (q-s) EG(m-r-1, q) \) are contained in a given \( EG(m-r, q) \), defined by (35), and are, of course, disjoint, or "parallel."

**Theorem 2.6.3.** All minimum weight code-vectors of \( C_v(m, q) \) can be obtained from the vectors corresponding to (34) by the substitutions (10) of the group \( G(m, q) \). In other words, the associated polynomials are equivalent to polynomials of the form (34) where any \((r+1)\) linearly independent linear forms are substituted for the \( x_i \).

The proof of this result is tedious and is deferred until the appendix. A consequence is that the number of minimum weight vectors in \( C_v(m, q) \), \( v = r(q-1) + s \), is given by

\[
(q - 1) \frac{q^r(q^m-1)(q^{m-1}-1) \cdots (q^{r+1}-1)}{(q^m-r-1)(q^{m-r-1}-1) \cdots (q-1)} N_s,
\]

with

\[
N_0 = 1 \quad \text{if} \quad s = 0,
\]

\[
N_s = \binom{q}{s} \frac{q^{m-r}-1}{q-1}, \quad 0 < s < q - 1,
\]

where:

(i) the first factor, other than \( (q-1) \), is the number of \( EG(m-r, q) \) contained in \( EG(m, q) \)

(ii) \( N_s \) is the number of sets of \( (q-s) \) "parallel" \( EG(m-r-1, q) \) contained in a given \( EG(m-r, q) \).

This result was already obtained in the binary case \( (q = 2) \) by Kasami, Lin, and Peterson [14].
3. NONPRIMITIVE G.R.M. CODES

3.1. 1-variable Approach

Let

\[ ab = q^m - 1 \]

be a nontrivial factorization of \( q^m - 1 \). Recall that \( HC_v(m, q) \) is defined as the set of vectors

\[ Q(1), Q(\alpha), ..., Q(\alpha^{v-1}), \quad Q(x) \in Q_v[x] \subseteq \overline{K}_v[x]. \]

Let \( Q_v[x] \) be the subset of polynomials of \( Q_v[x] \) with the property that

\[ Q(\alpha^i) = Q(\alpha^{i+a}) \quad \text{for all } i. \]

From (16), one has

\[
\begin{align*}
\epsilon_s &= \frac{1}{v} \sum_{i=0}^{v-1} Q(\alpha^i) \alpha^{-si} = \frac{1}{v} \sum_{i=0}^{v-1} Q(\alpha^{i+a}) \alpha^{-si} \\
&= \frac{1}{v} \sum_{j=0}^{v-1} Q(\alpha^j) \alpha^{-s(j-a)} = \alpha^{sa} \epsilon_s,
\end{align*}
\]

or \( \epsilon_s = 0 \) unless \( \alpha^{sa} = 1 \), i.e., \( s \equiv 0(b) \). If this holds, then

\[
Q(x) = \sum_{i=0}^{v-1} c_{bi} \alpha^{bi},
\]

and \( Q(\alpha^i) = Q(\alpha^{i+a}) \). Thus \( Q_v[x] \) is the subset of \( Q_v[x] \) with the property that \( \epsilon_s = 0 \) unless

\[ s \equiv 0(b). \]

Let

\[ U_v^b = \{ s, s \equiv 0(b), v(s) \leq v \}. \]

Clearly \( Q_v[x] \) is a linear space, and by 2.4.6 its dimension is \( | U_v^b | \).

There are good reasons (Hughes and MacWilliams [12]) for not calling this linear space a G.R.M. of any sort unless \( b \) divides \((q - 1)\). We impose this restriction: A vector of \( HC_v(m, q) \) corresponding to a polynomial \( Q(x) \) of \( Q_v[x] \) will consist of \( b \) repetitions of the same vector

\[ Q(1), Q(\alpha), ..., Q(\alpha^{v-1}). \]
Set
\[ L_b(z) = \sum_{i=0}^{b-1} \frac{\alpha^{\beta i}}{v} \cdot z^v - 1 = z - \alpha^{\beta i}, \quad i = 0, 1, \ldots, a - 1. \] (39)

Let \( b \) be a divisor of \( q - 1 \). The nonprimitive G.R.M. code \( HC_v^b(m, q) \) is the image with respect to basis (39) of the polynomials \( Q_v^b[z] \). It has block length \( a = (q^m - 1)/b \) and dimension \( |U_v^b| \). In fact the vectors of \( HC_v^b(m, q) \) are the vectors (38), for \( Q(z) \in Q_v^b[z] \).

Since \( c \equiv w_q(c) \mod q - 1 \), \( w_q(\beta) \) is divisible by \( b \). We need consider only values of \( v \) which are divisible by \( b \), since the intervening values will not produce any new codes.

3.2. The Dual Code

The image of \( Q_v^b[z] \) with respect to basis (14) consists of vectors which are \( b \) repetitions of vectors of \( HC_v^b(m, q) \). If we concede that both this code and \( HC_v^b(m, q) \) are cyclic (an obvious fact which will be proved later), we have from (20) that the nonzeros of the larger code are \( \alpha^{v - \beta}, w_q(\beta) \leq v \). These are obviously also nonzeros of \( HC_v^b(m, q) \). We note with approval that \( \alpha^{v - \beta} \) has the desirable property of being a root of \( x^a - 1 = 0 \). Hence:

The nonzeros of \( HC_v^b(m, q) \) are \( \alpha^0 = 1 \) and \( \alpha^{v - \beta} \) where
\[ w_q(\beta) \leq v. \]

From the general theory of cyclic codes \( \alpha^b \) is a zero of the dual code of \( HC_v^b(m, q) \) in \( E[x]/x^a - 1 \) if and only if
\[ i = 0, \quad \text{or} \quad w_q(\beta) \leq v. \]

Set \( \beta = v - jb \). Then if \( \alpha^{v - \beta} \) is a zero of the dual,
\[ \nu \geq w_q(v - jb) = m(q - 1) - w_q(jb), \]
\[ w_q(jb) \leq m(q - 1) - \nu > m(q - 1) - \nu - b = \mu' \quad (\equiv 0 \mod b). \]

Thus, for the dual code, \( \epsilon_j = 0 \) whenever \( w_q(jb) > \mu' \), and \( \epsilon_0 = 0 \) since 1 is a zero. The dual code is almost \( HC_{\mu'}(m, q) \).

Thus

**Theorem 3.2.1.** The dual code of \( HC_v^b(m, q) \) is obtained from \( HC_{\mu'}^b(m, q) \) by removing the all-one vector.
3.3. \textit{m-Variable Approach}

Let $P_{v}^{b}(m, q)$ be the subset of $P_{v}(m, q)$ corresponding to $Q_{v}^{b}[x]$ by the mapping (25).

By 2.4.10, $P_{v}^{b}(m, q)$ is the set of polynomials

$$P(\bar{x}) = \sum_{i_1, \ldots, i_m} c_{i_1, \ldots, i_m} x_{1}^{i_1} \cdots x_{m}^{i_m} \quad \text{where} \quad 0 \leq i_k \leq q - 1,$$

$$\sum_{k=1}^{m} i_k \leq v, \quad \sum_{i=1}^{m} i_k \equiv 0 \pmod{b} \quad [\text{recalling that } u \equiv w_{q}(u) \pmod{b} \text{ since } b \text{ divides } q - 1].$$

Obviously $P_{v}^{b}(m, q)$ is the subset of polynomials of $P_{v}(m, q)$ with the property that

$$P(\bar{\alpha}) = P(\bar{\alpha} \xi), \quad \text{all } \bar{\alpha},$$

(40)

where $\xi = \alpha^{a} = \bar{e}S^{a}$ is a primitive $b$-th root of unity in $E$. The code $HC_{v}^{b}(m, q)$ then consists of vectors of the form [see (38)]

$$P(\bar{e}), P(\bar{e}S), \ldots, P(\bar{e}S^{a-1}),$$

for $P(\bar{x}) \in P_{v}^{b}(m, q)$.

3.4. \textit{Automorphism Group}

Divide the nonzero elements of $E^{m}$ into equivalence classes,

$$\{\bar{\alpha}, \bar{\alpha} \xi, \ldots, \bar{\alpha} \xi^{(a-1)}\}. \quad (41)$$

Let $\langle S^{a} \rangle$ be the subgroup of $H(m, q)$ generated by the matrix $S^{a} = \text{diag} [\xi, \ldots, \xi]$, which commutes with any matrix of $H(m, q)$, so that $\langle S^{a} \rangle$ is a normal (in fact central) subgroup.

\textbf{Lemma 3.4.1.} \textit{The factor group } $H^{b} = H/\langle S^{a} \rangle$ \textit{acts as a permutation group of degree \(a\) on the equivalence classes, and leaves the codes } $HC_{v}^{b}(m, q)$ \textit{invariant.}

\textbf{Proof.} For $M \in H$, $(\xi^{i} \bar{\alpha}) M = \xi^{i} (\bar{\alpha} M)$ so that any element of $H$, acting as a permutation on the points of $E^{m}$, transforms an equivalence class (41) into another; furthermore, the group $\langle S^{a} \rangle$ is the greatest subgroup of $H$ all of whose elements permute among themselves the elements of any given equivalence class. Now, let $P(\bar{x})$ belong to $P_{v}^{b}(m, q)$. Then, by (40), $P(\bar{x})$ is constant over the points of any class (41); on the other hand, the points $(\bar{e}, \bar{e}S, \ldots, \bar{e}S^{a-1})$ of $E^{m}$ belong to different classes. It is then obvious (by
Theorem 2.3.2) that any element of $H^b$, acting now as a permutation on the coordinates of $HC_v^b(m, q)$, leaves this code invariant.

**Corollary 3.4.2.** $HC_v^b(m, q)$ is a cyclic code. This is obvious since the group $H^b$ contains the element $S$ which acts as a cyclic permutation of degree and order $a$ on the equivalence classes of $E^m$ containing $e, eS, ..., eS^{a-1}$, respectively, and thus on the coordinates of $HC_v^b(m, q)$.

### 3.5. Minimum Weight

Let $v = r(q - 1) + cb$, $0 \leq cb < q - 1$.

**Theorem 3.5.1.** (i) $HC_v^b$ has minimum weight exactly

$$((q - cb)q^{m-r-1} - 1)/b,$$

(ii) all minimum weight vectors can be obtained from the vectors corresponding to (34) and satisfying (40), by the substitutions of the group $H^b$.

**Proof.** Part (i) follows from Kasami, Lin, and Peterson [15]. In order to prove (ii), we observe that the vector $(P(e), P(0), P(eS), ..., P(0))$, with $P(x) \in P_v^b(m, q)$, is a minimum weight vector of $HC_v^b(m, q)$ if and only if the vector $(P(0), P(e), P(eS), ..., P(0))$ has minimum weight in $C_v(m, q)$, with $P(0) \neq 0$. The proof then follows from Theorem 2.6.3. It must be noticed that the polynomial (34) does not belong to $P_v^b(m, q)$, unless $\omega_1 = \omega_2 = \cdots = \omega_r = 0$.

### 3.6. Geometric Properties

The case $b = q - 1$ is of special interest. In this case $\xi = \alpha^{a}$ is a primitive element of $E$, and it is well known that the $a = (q^m - 1)/(q - 1)$ equivalence classes (41) or their representatives, $e, eS, ..., eS^{a-1}$, may be regarded as the points of an $(m - 1)$-dimensional projective geometry, $PG(m - 1, q)$ over $E$. The points of $PG(m - 1, q)$ which satisfy $r$ linear independent homogeneous equations

$$\sum_{j=1}^{m} a_{ij}x_j = 0, \quad a_{ij} \in E \quad i = 1, ..., r,$$

form an $(m - r - 1)$-dimensional projective geometry $PG(m - r - 1, q)$.

The polynomial $S(x) = \prod_{e=1}^{r} (1 - x_i^{a-1})$ belongs to $P_{r(q-1)}^a(m, q)$, and $S(x) = 0$ unless $x_i = 0$, $i = 1, 2, ..., r$. The vector of $HC_v^b(m, q)$ defined by $S(x)$ is thus the incidence vector of the points of $PG(m - 1, q)$ with a $PG(m - r - 1, q)$. As a corollary of Theorem 3.5.1, we have
Theorem 3.6.1. The minimum weight vectors of the code $\text{HC}_b(m, q)$, with $b = q - 1$, $v = r(q - 1)$, are the incidence vectors of the projective geometries $\text{PG}(m - r - 1, q)$ with respect to the points of $\text{PG}(m - 1, q)$.

4. Subcodes which lie in subfields of $E$

4.1. Definition and General Properties of Subfield Subcodes

Let $E = GF(q)$, where $q = p^t$ is the power of a prime $p$. Then $F = GF(p)$ is a proper subfield of $E$. Given any linear code $A$ over $E$, the subset of code vectors of $A$, all of whose coordinates lie in $F$ is defined as the subfield subcode of $A$ over $F$, (Berlekamp [1]). One easily verifies the following properties:

(i) The subfield subcode of a linear code is a linear code.

(ii) A permutation of coordinate places which preserves $A$ also preserves the subfield code. (It may be the identity as a permutation of code vectors.)

4.2. Subfield Subcodes of the G.R.M. Codes

The subfield considered in this section is $F = GF(p)$, the smallest possible. The extension to intermediate nonprime fields is obvious, and will not be discussed.

4.2.1. According to the results of 2.4.8, the $\nu$-th order G.R.M. code $C_{\nu}(m, q)$ of length $q^m$ over $E$ can be defined as the set of vectors $Q(0), Q(1), Q(\alpha),..., Q(\alpha^{\nu-1})$ where $Q(\alpha)$ is any polynomial of $Q_{\nu}[\alpha]$, i.e.,

$$Q(\alpha) = \sum_{u \in U_\nu} c_u \alpha^u$$

with

$$U_\nu = \{u; 0 \leq u \leq q^m - 1, \nu(u) \leq \nu\}$$

and $c_u \in K = GF(q^m)$ with the property that

$$c_{uq} = c_u q.$$

4.2.2. The subfield subcode of $C_{\nu}(m, q)$, denoted by $B_{\nu}(m, q)$, consists of vectors corresponding to polynomials $R(\alpha)$ of $Q_{\nu}[\alpha]$ where

$$R(\alpha^e) \in F, \quad R(0) \in F.$$ (42)
We denote this subset of $Q_\nu[z]$ by $R_\nu[z]$. If

$$R(z) = \sum_{u \in V_\nu} c_u z^u,$$

property (42) is equivalent to

$$c_{up} = c_u \alpha^p.$$

Let $V_\nu = \{u; 0 \leq u \leq q^m - 1, w_\nu(u \alpha^j) \leq \nu, j = 0, 1, \ldots, t - 1\}$. Then $R_\nu[z]$ consists of polynomials

$$R(z) = \sum_{u \in V_\nu} c_u z^u, \quad c_u \in K, \quad c_{up} = c_u \alpha^p. \quad (43)$$

By Lemma 2.4.6 the dimension of $B_\nu(m, q)$ over $F$ is $|V_\nu|$. We point out that, as in the case of nonprimitive G.R.M. codes, increasing the size of $\nu$ does not necessarily increase the size of $B_\nu(m, q)$.

From Theorem 2.6.1 $B_\nu(m, q)$ contains the incidence vectors of any $EG(m - r, q)$. The minimum weight $d_\nu$ of $B_\nu(m, q)$ is bounded by

$$(q - s) q^{m-r-1} \leq d_\nu \leq q^{m-r}.$$ 

And, according to Theorem 2.6.2, $d_\nu = (q - s) q^{m-r-1}$ if and only if there exist $s$ distinct elements $\omega_j'$ in $E$ such that the elements $c_k$ of (37) belong to $F$.

4.3. The Dual Code

Let $B_\nu^*(m, q)$ be the dual code over $F$ of $B_\nu(m, q)$, from 2.2.1 $B_\nu^*(m, q)$ contains, usually properly, the subfield subcode $B_\nu^*(m, q)$ where

$$\mu = m(q - 1) - \nu - 1 = (m - r - 1)(q - 1) + q - 2 - s.$$ 

If $d_\nu^*$ denotes the minimum weight of $B_\nu^*(m, q)$ we have

$$d_\nu^* \leq d_\mu \leq q^{r+1}.$$ 

A lower bound on $d_\nu^*$ can be obtained from the BCH bound: $d_\nu^* \geq u_\nu^* + 1$ if $u_\nu^*$ is the smallest power of $\alpha$ which is not a root of $B_\nu(m, q)$, that is, such that

$$w_\nu(u_\nu^* \alpha^j) \geq v + 1 \quad \text{for some } j.$$ 

We give without proof the values of $u_\nu^*$, for $r \geq 1$, in the following theorem.

**Theorem 4.3.1.** Let $s = s_0 + s_1 \alpha + \cdots + s_{l-1} \alpha^{p-1}$, with $0 \leq s_i \leq p - 1$, be the $p$-ary expansion of $s$. 

(i) If \( s_{t-1} < p - 1 \), \( u_\ast = (p(s + 1) + q) q^{r-1} - 1 \). Otherwise, assume \( s_i = s_{i+1} = \cdots = s_{t-1} = p - 1 \), with \( i \leq t - 1 \) and \( s_{i-1} < p - 1 \). Then

(ii) if \( s_0 < p - 2 \), and \( s_1 = \cdots = s_{t-1} = 0 \), \( u_\ast = (s_0 + 2) p^t q^r - 1 \);

(iii) if \( \sum_{k=0}^{t-1} s_k p^k \geq p - 2 \), \( u_\ast = (p^{t-i+1}(s + 1) + q) q^{r-1} - 1 \).

Partial results were obtained by Chow [4], Kasami, Lin, and Peterson [15] and Lin [17]. Proofs of the results given here can be found in Delsarte [7].

4.4. The Automorphism Group

It is well known that the substitution

\[ \theta : z \rightarrow z^p, \]

belongs to the automorphism group of any cyclic or extended cyclic code over \( GF(p) \). This substitution is a collineation of the points of \( EG(m, q) \) (Carmichael [2]).

From 2.5.1 \( \theta \in G(m, q) \), and it is easy to verify that \( \theta G(m, q) \theta^{-1} = G(m, q) \). Thus the order of the group \( \langle G(m, q), \theta \rangle \) is

\[ t | G(m, q)|. \]

**Theorem 4.4.1.** If \( \nu = r(q - 1) + s \), the automorphism group of \( B_v(m, q) \) contains a group isomorphic to \( \langle G(m, q), \theta \rangle \), and \( \langle G(m, q), \theta \rangle \) acts as a nontrivial permutation group on the code vectors, when \( r \geq 1 \).

**Proof.** By 4.1.1 (ii) the automorphism group of \( B_v(m, q) \) contains an isomorphic image of this group. It remains to show that only the identity of \( \langle G(m, q), \theta \rangle \) is the identity permutation on \( B_v(m, q) \), when \( r \geq 1 \).

\( B_v(m, q) \) contains the incidence vectors of all \( EG(m - r, q) \). If \( M \) is the identity on \( B_v(m, q) \), it is a collineation which stabilizes every \( EG(m - r, q) \). Hence it must stabilize the intersection of two \( EG(m - r, q) \) (there are two since \( r \geq 1 \)) and finally stabilizes every point. Thus \( M \) is the identity of \( \langle G(m, q), \theta \rangle \).

4.5. The \( m \)-variable Approach

A polynomial \( R(z) \) of \( R_v[z] \) is made up of terms of the form

\[ \sum_j \sum_k (z^{q^k z^{uq^k} q^j}) \alpha^j, \quad w_\alpha(\alpha^j) \leq \nu \quad j = 0, \ldots, t - 1. \]

(The summation is over all distinct values of \( uq^k \mod q^m - 1 \).) Let \( l_i = \sum_{s=0}^{t-1} l_{i,s} p^s; \) define

\[ [pl_i] = l_{i,t-1} + l_{i,0} p + \cdots + l_{i,t-2} p^{t-2}; \]
that is, 
\[ [p^l_i] = \begin{cases} p^l_i \text{ mod } q - 1 & \text{if } i < q - 1 \\ q - 1 & \text{if } i = q - 1. \end{cases} \]

By Lemma 2.4.10, the reduced form of the image of the above polynomial is

\[ \sum_{j} \sum_{l_1 \cdots l_m} d^{v'}(l_1 \cdots l_m) x_1^{[p^l_1]} \cdots x_m^{[p^l_m]}, \]

with

\[ 0 \leq [p^l_i] \leq q - 1, \quad \sum_{i=1}^{m} [p^l_i] \leq \nu. \]

**Theorem 4.5.1.** The code \( B_s(m, q) \) is the image with respect to basis (3) of the set of polynomials

\[ T(\bar{x}) = \sum_{l_1 \cdots l_m} d(l_1 \cdots l_m) x_1^{l_1} \cdots x_m^{l_m}, \]

where

(i) \( \sum_{i=1}^{m} [p^l_i] \leq \nu \quad j = 0, 1, \ldots, t - 1, \)

(ii) \( d([p^l_1], \ldots, [p^l_m]) = d^{v'}(l_1 \cdots l_m). \)

In fact it is easy to check directly that (i) and (ii) are equivalent to the statement that \( [T(\bar{\omega})]^p = T(\bar{\omega}), \) (that is \( T(\bar{\omega}) \in F \)) for all \( \bar{\omega} \in E^m, \) (Kasami, Lin, and Peterson [15]).

**4.5.2.** In the \( m \)-variable language, the group \( \langle G(m, q), \theta \rangle \) consists of transformations

\[ x_i \rightarrow y_i = \sum_{j=1}^{m} a_{ij} x_j^\tau + \omega_{0,i}, \]

where \( (a_{ij}) \) is an invertible matrix over \( E, \bar{\omega}_0 \) a point of \( E^m, \) and \( 0 \leq \tau < t. \)

This is the full collineation group on the points of \( EG(m, q). \)

## 5. Geometric Codes

### 5.1. Euclidean Geometry Codes

A particularly interesting class of codes is obtained, when \( \nu = r(q - 1), \) \( (s = 0). \) The minimum weight vectors of \( B_s(m, q) \) then are the incidence
vectors of the $EG(m - r, q)$. The dual code $B^*_r(m, q)$ has, according to Theorem 4.3.1 (i), minimum weight $d^*_r$ at least

$$d^*_r + 1 = (p + q) q^{r-1}.$$ 

These codes $B^*_r(m, q)$ are equivalent to the codes introduced by Weldon [26] as Euclidean geometry codes, and are majority logic decodable for a number of independent errors not exceeding $[J/2]$, where

$$J = \frac{q^{r+1} - 1}{q - 1} = q^r + q^{r-1} + \cdots + q + 1,$$

is the order of the "orthogonal check sets" (Massey [19]) that can be constructed from the incidence vectors of the $EG(m - r, q)$. We emphasize that the majority decoding algorithms do not use the full error-correcting ability of the code, since

$$d^*_r \geq (p + q) q^{r-1} > J + 1,$$

unless $q = p = 2$; or $p = 2$, $r = 1$.

These codes have a further interesting property, namely

**Theorem 5.1.1.** The code $B_{r(q-1)}(m, q)$ is generated as a vector space over $F$ by the incidence vectors of the $EG(m - r, q)$. This result can be derived (not easily) from a theorem of Delsarte [5].

**Corollary 5.1.2.** The p-rank of the incidence matrix of points and $EG(m - r, q)$ of $EG(m, q)$ is $| V_{r(q-1)} |$ defined by (43).

It is clear that 5.1.1 cannot be extended to codes over nonprime fields between $F$ and $E$. By arguments parallel to those of 4.2.2 the dimension of such a code is found to be greater than $| V_{r(q-1)} |$.

5.2. Projective Geometry Codes

Define $HB_{r(q-1)}^{(q-1)}(m, q)$ as the subfield subcode of the nonprimitive G.R.M. code $HC_{r(q-1)}^{(q-1)}(m, q)$ discussed in 3.6. Equivalently, it is the set of $(q^{m} - 1)/(q - 1) -$ periodic vectors of the code $HB_{r(q-1)}(m, q)$. The following property is fairly obvious (see Theorem 3.6).

5.2.1. The minimum weight of $HB_{r(q-1)}^{(q-1)}(m, q)$ is $(q^{m-r} - 1)/(q - 1)$, and the minimum weight vectors are the incidence vectors of the projective
geometries $PG(m - r - 1, q)$ with respect to the points of $PG(m - 1, q)$. Hence, the number of minimum weight vectors is

$$(p - 1) \frac{(q^m - 1)(q^{m-1} - 1) \cdots (q^{r+1} - 1)}{(q^{m-r} - 1)(q^{m-r-1} - 1) \cdots (q - 1)}.$$

5.2.2. The dual code is the set of $(q^m - 1)/(q - 1)$ — periodic vectors of $[HB_{r(q-1)}(m, q)]^*$ and is equivalent to the projective geometry code introduced by Rudolph [23]. It can be decoded by majority logic (Goethals, Delsarte [10]), correcting a number of errors not exceeding $[K/2]$, where

$$K = (q^{r+1} - 1)/(q - 1)$$

is the number of $PG(m - r - 1, q)$ which contain a given $PG(m - r - 2, q)$.

5.2.3. The code $HB_{r(q-1)}(m, q)$ is generated as a vector space over $F$ by the incidence vectors of the $PG(m - 1 - r, q)$.

Proofs of 5.1.1 and 5.2.3, which at present are complicated, are not given in this paper. The proof of 5.2.3 can be derived from Goethals and Delsarte [10].

5.3. The Case $v = r(q - 1) + (q - 2)$.

Consider the polynomial

$$g(y) = \prod_{\omega} (y - \omega),$$

where $\omega \in E, \omega \neq 0, 1$.

$$g(y) = \frac{y^q - y}{y(y - 1)} = \sum_{i=0}^{q-2} y^i.$$

Then

$$P(x) = \prod_{i=1}^{r} (1 - (x_i - \omega_i)^{q-1}) g(x_{r+1})$$

(44)

describes a minimum weight vector of $B_v(m, q)$. Thus $B_v(m, q)$ has minimum weight exactly $2q^{m-r-1}$. The vectors described by (44) are the union of the incidence vectors of two parallel $EG(m - r - 1, q)$, multiplied by the factors $g(0) = 1, g(1) = q - 1 = -1$, respectively.

The dual code $B_v^*(m, q)$ has by Theorem 4.3.1 (iii) minimum weight exactly $q^{r+1}$, and is decodable by majority logic, as described below.
Let $X$ be the incidence vector of a fixed $EG(m - r - 1, q)$, and $Y_i$ the incidence vector of a parallel $EG(m - r - 1, q)$. $X$ and $Y_i$ are of course disjoint vectors—no coordinate place is in both $X$ and $Y_i$. $B_i(m, q)$ contains all vectors $X - Y_i$, and the number of such vectors is $(q^{r+1} - 1)$. (There are $(q^{r+1} - 1)/(q - 1)$ $EG(m - r, q)$ containing the $EG(m - r - 1, q)$ corresponding to $X$, and in each of these $(q - 1)$ choices for $Y_i$.) The vectors $X - Y_i$ of $B_i(m, q)$ form an orthogonal check set of order $J_1 = q^{r+1} - 1$ over $X$. Furthermore, a fixed $EG(m - r - i, q)$ $(2 \leq i \leq m - r)$ is contained in exactly $J_i = (q^{r+i} - 1)/(q - 1)$ distinct $EG(m - r - i + 1, q)$ belonging to $EG(m, q)$, so that the usual multi-step majority logic procedure will correct up to $[J/2]$ errors, with $J = \min(J_1, J_2, ..., J_{m-r})$. (The $i$-th step of the algorithm gives the sum of the errors in the positions corresponding to the coordinates of the given $EG(m - r - i, q)$, so that the $(m - r)$-th step gives the error in the position corresponding to the point $EG(0, q)$.) Since $J_1 < J_2 < \cdots < J_{m-r}$, one has $J = J_1 = q^{r+1} - 1$ and the decoding method uses the full capability of the code $B_i^*(m, q)$ [$B_i^*(m, q)$ is said to be completely orthogonalizable in $m - r$ steps] (Massey [19])

5.4. Relations between Geometric Codes

Let $b = q - 1$, $v = r(q - 1)$ and consider the following codes over $F = GF(p)$:

$$\begin{align*}
\Gamma &= HB^b_1(m + 1, q); \\
\Gamma' &= HB^b(m, q) \\
\Gamma'' &= C_v(m, q); \\
\Gamma_0' &= HB^{b-1}_v(m, q) \\
\Gamma_0'' &= C_{v-1}(m, q).
\end{align*}$$

We now examine how these codes (which are the dual of some "geometric codes") are related to each other. Let the coordinate places of $\Gamma$ be considered as the $v = (q^{m+1} - 1)/b$ points of a projective geometry $PG(m, q)$ over $E$. Moreover, let $V' = PG(m - 1, q)$ be any hyperplane in $V$ and $V'' = V - V'$ the complementary set of $V'$ with respect to $V$; so that $V'$ and $V''$ have cardinality $v' = (q^n - 1)/b$ and $v'' = q^m$, respectively. This partition of $V$ induces the following obvious partition of the vectors $a$ of $\Gamma$:

$$a = [a', a''],$$

where $a'$ (resp. $a''$) denotes the restriction of $a$ to $V'$ (resp. $V''$).

**Theorem 5.4.1.** (i) The code $\Gamma'$ (resp. $\Gamma''$) is the set of all distinct vectors $a'$ (resp. $a''$), for which $[a', a'']$ is a vector of $\Gamma$. 
(ii) The code $\Gamma'_0$ (resp. $\Gamma''_0$) is the set of vectors $a'$ (resp. $a''$), for which $[a', 0]$ (resp. $[0, a'']$) is a vector of $\Gamma$.

The proof of this theorem, which can be obtained from the $m$-variable approach to G.R.M. codes, will not be given in the present paper. It can be found in Delsarte [6]. As a corollary of Theorem 5.4.1, one has the following relation between the respective dimensions $k, k', k'', k'_0, k''_0$ of the codes $\Gamma, \Gamma', \Gamma'', \Gamma'_0, \Gamma''_0$:

$$k' + k'' = k'' + k'_0 = k.$$

APPENDIX. PROOF OF THEOREM 2.6.3.

The authors hasten to point out that it would be very desirable to find a more sophisticated and shorter proof.

**Lemma A1.1.** If $P(x) = 0$ whenever $x_1 = a$, then $P(x) = (x_1 - a) \hat{P}(x)$, where the right hand side is in reduced form; that is the exponent of $x_1$ in $\hat{P}(x)$ is at most $q - 2$.

**Proof.** $P(a, x_2, \ldots, x_m) = 0$ for all $x_2 \cdots x_m$. Set

$$P(x) = \sum_{i} g_i x^{q-1} + g_1 x_1^{q-2} + \cdots + g_{q-1}, \quad g_i = g_i(x_2, \ldots, x_m).$$

Use the equations $P(x) = P(x) - P(a, x_2, \ldots, x_m)$.

**Corollary A1.2.** If $P(x) = 0$ unless $x_1 = b$, then

$$P(x) = (1 - (x_1 - b)^{q-1}) \hat{P}(x_2, \ldots, x_m).$$

**Proof.** 1.1 and A1.1.

**Lemma A1.3.** Let $S$ be a set of points of $EG(m, q)$, where $|S| = tq^n < q^m$, $0 < t < q$. Let $S$ have the property that for any hyperplane $H$, either $|S \cap H| = 0$ or $|S \cap H| \geq tq^{n-1}$. Then there exists a hyperplane which does not meet $S$.

**Proof.** Suppose the converse. Considering the intersection of $S$ with $q$ parallel hyperplanes we see that $|S \cap H| = tq^{n-1}$ for every $H$. Considering the $(q + 1)$ hyperplanes through a fixed $EG(m - 2, q)$, we see that $S$ meets every $EG(m - 2, q)$ in $tq^{n-2}$ points. Iterating this argument, $S$ meets every $643/16/5-3$
DELSARTE, GOETHALS, AND MACWILLIAMS

\( \text{EG}(m - n + 1, q) \) in \( tq \) points and every \( \text{EG}(m - n, q) \) in \( t \) points, \( (m - n \geq 1) \).

Let \( L_1 \) be a fixed \( \text{EG}(m - n + 1, q) \), and \( L_0 \) a fixed \( \text{EG}(m - n - 1, q) \) of \( L_1 \) which meets \( S \) in \( k \) points. Consider the \( (q + 1) \) \( \text{EG}(m - n, q) \) of \( L_1 \) through \( L_0 \). Then

\[
t \cdot q = |S \cap L_1| = k + (q + 1)(t - k) = qt + t - qk,
\]

\[
t = qk \quad \text{which is impossible.}
\]

**Lemma A1.4.** Let \( P(\bar{x}) \) correspond to a minimum weight vector of \( \text{C}_r(m, q) \). Let \( S \) be the set of points \( \bar{\omega} \in E^m \) such that \( P(\bar{\omega}) \neq 0 \). Then there is a hyperplane which does not meet \( S \).

**Proof.** Let \( v = r(q - 1) + s \); then \( |S| = (q - s) q^{m-r-1} \). The intersection of \( S \) with a hyperplane \( H \) consists of the nonzero coordinates of a vector of \( \text{C}_v(m, q) \), \( \nu' = v + (q - 1) \nu \). Thus

\[
|S \cap H| = 0 \quad \text{or} \quad |S \cap H| \geq (q - s) q^{m-r-2}.
\]

\( S \) satisfies the hypotheses of A1.3.

Henceforth we suppose that the coordinate system is chosen so that the hyperplane \( x_1 = 0 \) does not meet \( S \). Then by A1.1 \( P(\bar{x}) = x_1 \hat{P}(\bar{x}) \), and the highest power of \( x_1 \) which appears in \( \hat{P}(\bar{x}) \) is \( q - 2 \).

**Lemma A1.5.** Let \( v = s \leq q - 1 \). Let \( P(\bar{x}) \) correspond to a minimum weight vector of \( \text{C}_s(m, q) \). Then there exists \( z = \sum_{i=1}^{m} \epsilon_i x_i \), such that

\[
P(\bar{x}) = \begin{cases} 
\epsilon \prod_{j=1}^{s} (z - b_j), & \text{if } s < q - 1, \\
\epsilon [1 - (z - a)^{q-1}], & \text{if } s = q - 1,
\end{cases}
\]

where the \( b_j \) are distinct elements of \( E \).

**Proof.** The lemma is true for \( s = 1 \) since every vector of \( \text{C}_1(m, q) \) is described by a polynomial of the form \( \epsilon_0 + \sum_{i=1}^{m} \epsilon_i x_i \). We proceed by induction on \( s \). Set \( \hat{P}(\bar{x}) = x_1 \hat{P}(\bar{x}) \). Let \( [P(\bar{x}) = 0]_m \) denote the number of \( \bar{\omega} \in E^m \) for which \( P(\bar{\omega}) = 0 \). Since \( \hat{P}(\bar{x}) \) describes a vector of \( \text{C}_{s-1}(m, q) \),

\[
[P(\bar{x}) = 0]_m \leq q^m - (q - s + 1) q^{m-1} = (s - 1) q^{m-1}.
\]

\[
sq^{m-1} = [P(\bar{x}) = 0]_m \leq [x_1 = 0]_m + [\hat{P}(\bar{x}) = 0]_m \leq q^{m-1} + (s - 1) q^{m-1}.
\]

1 In the following we always suppose \( r < m - 1 \); the proofs are similar if \( r = m - 1 \).
Thus \([P(\bar{x}) \neq 0]_m = (q - s + 1)q^{m-1}\), and by induction

\[ P(\bar{x}) = c \prod_{j=1}^{s-1} (x - b_j), \]

\[ P(\bar{x}) = cx_1 \prod_{j=1}^{s-1} (x - b_j). \]

It is easy to check that this expression has \((q - s)q^{m-1}\) nonzeros if and only if \(x = x_1\) and no \(b_j\) is zero.

Let \(v = r(q - 1) + s, v > q - 1\). Let \(P(\bar{x})\) describe a minimum weight vector of \(C_s(m, q)\). Set \(\bar{x} = (x_1, \bar{x}')\), and

\[ P(x_1, \bar{x}') = g_1x_1^{q-1-i} + g_{i+1}x_1^{q-2-i} + \cdots + g_{q-2}x_1, \]

where \(g_j = g_j(\bar{x}')\) and \(g_s(\bar{x}') \neq 0\).

Let \(\eta(j)\) be the number of \(\bar{\omega}'\) of \(E^{m-1}\) for which \(P(x_1, \bar{\omega}') = 0\) for \(j\) distinct values of \(x_1\) in \(E\). Clearly \(\eta(j) = 0\) for \(q - 1 - i < j < q\), and \(\eta(q)\) is the number of \(\bar{\omega}'\) for which all coefficients \(g_j\) are zero.

**Lemma A1.6.** Let \(v = r(q - 1) + s\) \((0 < s \leq q - 1)\).

(i) \(\eta(q) \geq q^{m-1} - (q - s/1 + i)q^{m-r-1}\)

(ii) Equality in (i) implies that \(j = q - 1 - i\) is the only value of \(j\) less than \(q\) for which \(\eta(j) \neq 0\), and \(\eta(q - 1 - i) = (q - s/1 + i)q^{m-r-1}\).

**Proof.**

\[ q\eta(q) + \sum_{j=1}^{q-1-i} j\eta(j) = [P(\bar{x}) = 0]_m = q^m - (q - s)q^{m-r-1}. \]

\[ \eta(q) + \sum_{j=0}^{q-1-i} \eta(j) = |E^{m-1}| = q^{m-1}. \]

From these equations

\[ (i + 1)\eta(q) = \sum_{j=0}^{q-2-i} (q - 1 - i - j)\eta(j) + (i + 1)q^{m-1} - (q - s)q^{m-r-1}. \]

The terms under \(\sum\) are nonnegative, thus

\[ \eta(q) \geq q^{m-1} - \frac{q - s}{i + 1}q^{m-r-1}. \]
Equality implies $\sum = 0$, so each term is separately zero. Then

$$\eta(q - 1 - i) = \frac{q - s}{1 + i} q^{m-r-1}.$$  

**Lemma A1.7.** The only possible values of $i$ are zero, and $(q - 1 - s)$.

**Proof.** (i) Suppose $s + i \geq q - 1$, say $s + i = q - 1 + \epsilon$, $\epsilon \geq 0$. Then $g_s(x')$ is of degree at most $r(q - 1) + \epsilon$, which implies

$$[g_s(x') \neq 0]_{m-1} \geq (q - \epsilon) q^{(m-1)-r-1}.$$  

Clearly $\eta(q) \leq [g_s(x') = 0]_{m-1}$, thus

$$q^{m-1} - \frac{q - s}{q - s + \epsilon} q^{m-r-1} \leq \eta(q) \leq q^{m-1} - (q - \epsilon) q^{m-r-2},$$

$$\frac{q - s}{q - s + \epsilon} \geq q - \epsilon.$$  

The only possibilities are $s = \epsilon$, that is $i = q - 1$, which is impossible by (45), or $\epsilon = 0$, $i = q - 1 - s$.

(ii) $s + i < q - 1$. Then $g_s(x')$ is of degree at most $(r - 1)(q - 1) + s + i$, as before,

$$q^{m-1} - \frac{q - s}{1 + i} q^{m-r-1} \leq \eta(q) \leq q^{m-1} - (q - s - i) q^{m-r-1},$$

$$\frac{q - s}{1 + i} \geq q - s - i,$$

and the only possibility is $i = 0$.

**Proof of 2.6.3.** We now suppose Theorem 2.6.3 true for $\nu \leq r(q - 1)$ (Lemma A1.5 establishes the case $r = 1$) and proceed by induction on $\nu$. There are two cases.

(i) $\nu = r(q - 1) + s \quad 0 < s \leq q - 1$.

$$P(x) = g_{q-1-s}(x') x_1^s + g_{q-s}(x') x_1^{s-1} + \cdots + g_{q-2}(x') x_1.$$  

From the proof of A1.7 (i) with $\epsilon = 0$ we have

$$[g_{q-1-s}(x') = 0]_{m-1} = \eta(q) = q^{m-1} - q^{m-r-1},$$

$$[g_{q-1-s}(x') \neq 0]_{m-1} = q^{m-r-1}.$$
Thus \( g_{v-1-s}(\bar{x}') \) is of degree \( v' = r(q - 1) \), and represents a minimum weight vector of \( C_{v'}(m - 1, q) \). By induction there is a linear transformation

\[
y_i = \sum_{j=2}^{m} e_{i,j} x_j, \quad i = 2, \ldots, r + 1
\]
such that \( g_{v-1-s}(\bar{x}') \) becomes

\[
r(y_2, \ldots, y_{r+1}) = c \prod_{i=2}^{r+1} (1 - (y_i - a_i)^{q-1}).
\]

Let \( R(x_1, \bar{y}') \) be the reduced form of \( P(x_1, \bar{x}') \) in the new coordinates. From the definition of \( \eta(q) \), \( R(x_1, \bar{y}') = 0 \) unless \( y_i = a_i \), \( i = 2, \ldots, r + 1 \). By A1.2

\[
R(x_1, \bar{y}') = r(y_2, \ldots, y_{r+1}) \bar{R}(x_1, y_{r+2}, \ldots, y_m).
\]

\( \bar{R} \) is of total degree \( s \), and

\[
R(x_1, a_2, \ldots, a_{r+1}, y_{r+2}, \ldots, y_m) = c \bar{R}(x_1, y_{r+2}, \ldots, y_m).
\]

Thus

\[
[R(x_1, y_{r+2}, \ldots, y_m) \neq 0]_{m-r} = \eta(q) = (q - s) q^{m-r-1}.
\]

Then by A1.5

\[
\bar{R}(x_1, y_{r+2}, \ldots, y_m) = \begin{cases} c' \prod_{j=1}^{s} (x_1 - b_j), & \text{if } s < q - 1, \\ c'[1 - (x_1 - a_1)^{q-1}], & \text{if } s = q - 1. \end{cases}
\]

(ii) \( v = r(q - 1) + s, \quad 0 < s < q - 1 \).

\[
P(x_1, \bar{x}') = g_0(\bar{x}') x_1^{q-1} + g_1(\bar{x}') x_1^{q-2} + \cdots + g_{q-2}(\bar{x}') x_1.
\]

From the proof of A1.7 (ii) with \( i = 0 \) we have

\[
[g_0(\bar{x}') = 0]_{m-1} = \eta(q) = q^{m-1} - (q - s) q^{m-r-1},
\]

\[
[g_0(\bar{x}') \neq 0]_{m-1} = (q - s) q^{m-r-1}.
\]

Thus \( g_0(\bar{x}') \) is of degree \( v' = (r - 1)(q - 1) + s \) and represents a minimum
weight vector of $C_v(m - 1, q)$. As before there exists a coordinate system $x_1, y_2, ..., y_m$ in which $g_0(\bar{x}')$ becomes

$$r(y_2, ..., y_{r+1}) = c \prod_{i=2}^{r} (1 - (y_i - a_i)^{q-1}) \prod_{j=1}^{s} (y_{r+1} - b_j).$$

Let $P(x_1, \bar{y}')$ become $R(x_1, \bar{y}')$. As before

$$R(x_1, \bar{y}') = r(y_2, ..., y_{r+1}) \hat{R}(x_1, y_{r+1}, y_{r+2}, ..., y_m),$$

where $\hat{R}$ is of total degree $(q - 1)$ and of degree at most $(q - 1 - s)$ in $y_{r+1}$.

Let $c_1, c_2, ..., c_{q-s}$ be the elements of $E$ other than the $b_j$. Then for each $c_i$

$$R(x_1, a_1, ..., a_r, c_i, y_{r+2}, ..., y_m) = c \prod_{j=1}^{s} (c_j - b_j) \hat{R}(x_1, c_i, y_{r+2}, ..., y_m),$$

and

$$\sum_{i=1}^{q-s} [\hat{R}(x_1, c_i, y_{r+2}, ..., y_m) \neq 0]_{m-r} = (q - s) q^{m-r-1}. \tag{i}$$

From A1.6, $\eta(q - 1) = (q - s) q^{m-r-1}$. For each $c_i$ and any $y_{r+2}, ..., y_m$ there is one value of $x_1$ such that $\hat{R} \neq 0$. This implies

$$[\hat{R}(x_1, c_i, y_{r+2}, ..., y_m) \neq 0]_{m-r} \geq q^{m-r-1},$$

so that we must have

$$[\hat{R}(x_1, c_i, y_{r+2}, ..., y_m) \neq 0]_{m-r} = q^{m-r-1}. \tag{ii}$$

By A1.5

$$\hat{R}(x_1, c_i, y_{r+2}, ..., y_m) = 1 - (x_1 - a(c_i))^{q-1}. \tag{iii}$$

Set

$$\hat{R}(x_1, y_{r+1}, y_{r+2}, ..., y_m) = -x_1^{q-1} + f_1 x_1^{q-2} + \cdots + f_{q-s} x_1^1,$$

where $f_i$ is a polynomial of degree $\leq i$ in $y_{r+1}, ..., y_m$.

Set $f_1 = dy_{r+1} + h$ where $a \in E$ and $h$ of degree 1 in $y_{r+2}, ..., y_m$. Then

$$dc_i + h = -a(c_i)$$

so that $h$ is a constant and one has

$$\hat{R}(x_1, c_i, y_{r+2}, ..., y_m) = 1 - (x_1 + dc_i + h)^{q-1}. \tag{iv}$$
Hence, by Lemma A1.1

\[ \hat{R}(x_1, y_{r+1}, y_{r+2}, \ldots, y_m) \equiv 1 - (y_1 - a_1)^{q-1} \mod \prod_{i=1}^{q-2} (y_{r+1} - c_i) \]

with \( y_1 = x_1 + dy_{r+1} \), \( a_1 = -h \).

This concludes the proof of Theorem 2.6.3.

REFERENCES

6. P. Delsarte, On linear codes which are invariant under some permutation groups, Report R-105, MBE Research Laboratory, Brussels, Belgium, 1969.
12. D. R. Hughes and F. J. MacWilliams, A result in Group Theory, with applications to Geometric Codes, (to be published.)