BOUND FOR UNRESTRICTED CODES,
BY LINEAR PROGRAMMING

by P. DELSARTE

Abstract
The paper describes a problem of linear programming associated with
distance properties of unrestricted codes. As a solution to the problem,
one obtains an upper bound for the number of words in codes having
a prescribed set of distances.

1. Introduction

Important information about a code is contained in its Hamming distance
distribution, defined as follows: for a q-ary code C of length n, it is the \((n + 1)\)-
tuple \((A_0(C), A_1(C), \ldots, A_n(C))\), where \(A_i(C)\) denotes the mean number of
codewords being at Hamming distance \(i\) from a fixed codeword. For linear
codes over the field \(GF(q)\), the distance distribution reduces to the classical
weight distribution. In that case the distributions of a code \(C\) and of its dual \(C'\)
are related by the MacWilliams identities \((1)\), i.e., by linear equations of the form

\[ |C| A_k(C') = \sum_{i=0}^{n} A_i(C) P_k(i), \quad 0 \leq k \leq n, \quad (1) \]

where the \(P_k(i)\) are constant integers, only depending on \(n\) and \(q\). It turns out
that \(P_k(x)\) can be identified with a Krawtchouk polynomial of degree \(k\), for a
suitable normalization (cf. Szegö \(^{16}\)).

The present paper starts from the observation that the distance distribution
of an unrestricted code (over an unrestricted alphabet) yields nonnegative
numbers when substituted to the right-hand member of (1). This theorem leads
in a natural way to a problem of linear programming, the solution of which
gives an upper bound for the number of words in codes having a designed set
of distances. Some characteristic properties of codes meeting that bound are
also derived from the well-known theory of duality in linear programming;
for this we refer to Simonnard \(^{14}\).

When only the minimum distance is specified, these results imply, as par-
ticular cases, some classical theorems such as the Plotkin, Singleton and
Hamming bounds (cf. Berlekamp \(^1\)). In the latter case, the codes meeting the
bound are the perfect codes and the characterization one obtains for them is
the Lloyd theorem (cf. Van Lint \(^9\)) which is shown to hold for any alphabet.
The same result has been recently discovered by Lenstra \(9\)), in a very different way.

For group codes over an Abelian group, called *additive codes* in this paper, one defines a duality relation that reduces to the classical concept for linear codes over a prime field. If \(C'\) is the dual of any additive code \(C\), it is shown that the MacWilliams identities on the weight distributions are still satisfied.

A basic tool in this paper is the theory of group characters of an Abelian group, used in a similar way as in Van Lint \(9\)). Mapping the \(q\)-ary alphabet onto an Abelian group of order \(q\), one defines the *characteristic matrices* of a code by means of the characters of that group. These matrices appear to be very useful in the study of distance properties of a code.

2. Definitions and preliminaries

Let \(V = F^n\) be the set of \(n\)-tuples over a finite alphabet \(F\) of order \(q\), with \(q \geq 2\), \(n \geq 1\). Then \(V\) is made a metric space by definition of the *Hamming distance* \(d\) over it: for any two points \(a, b\) of \(V\), we set

\[
d(a, b) = |\{i \mid 1 \leq i \leq n, \alpha_i \neq \beta_i\}|,
\]

where \(\alpha_i\) denotes the \(i\)th component of \(a\). An \((n, M)\) code over \(F\) is a subspace of cardinality \(M\) of the metric space \((V, d)\). The elements of a code are called the *codewords*.

In order to be able to calculate with codes, we now map the alphabet \(F\) onto a given "additive" Abelian group of order \(q\), in an arbitrary way. Then the points of \(V\) are considered as elements of the group \((F, +)^n\), and \(V\) is made a normed space by means of the *Hamming weight* \(w\), where \(w(a)\) is defined to be the number of nonzero components of \(a\). Comparing this with the definition of \(d\), we have

\[
d(a, b) = w(a - b), \quad \forall a, b \in V.
\]

Let \(v\) be the *period* of the group \((F, +)\), i.e., the smallest integer \(v\) such that \(vf = 0, \forall f \in F\). We shall now introduce a symmetric *inner product* \(\langle \cdot, \cdot \rangle\) of \(V\) over the cyclotomic field \(Q_v\) of complex \(v\)th roots of unity. The notations are the same as in the author's paper on Abelian codes \(2\)). Let

\[
f_0 = 0, f_1, f_2, \ldots, f_\lambda, \quad \text{with} \quad \lambda = q - 1,
\]

be the elements of \(F\) and let \(\phi_0, \phi_1, \ldots, \phi_\lambda\) be the group characters of \((F, +)\), i.e., the homomorphic mappings of \((F, +)\) into the multiplicative group of \(Q_v\). It is always possible to choose the numbering in such a way that \(\phi_j(f_\lambda) = \phi_j(f_1)\). In particular, \(\phi_0\) is the principal character: \(\phi_0(f_j) = 1 \forall j\). Then, for \(a, b \in V\), we define

\[
\langle a, b \rangle = \prod_{i=1}^{n} \phi_{f_i}(a_i), \quad \text{with} \quad f_{t_1} = b_{t_1}.
\]
For fixed $a$ in $V$, the mapping $b \rightarrow \langle a, b \rangle$ is a character of $(F, +)^n$, as can be easily verified. Some useful properties of the inner product are examined in the appendix.

A code $C$ of length $n$ over $F$ will be called an additive code, with respect to $(F, +)$, if its words form a subgroup of $(F, +)^n$. By use of the inner product (3), let us now define a duality among additive codes: the dual code $C'$ of $C$ is defined to be

$$C' = \{ b \in V | \langle a, b \rangle = 1, \forall a \in C \}.$$

When $q$ is a prime, an additive code is merely a linear code over the Galois field $GF(q)$ and the dual is the classical one: the orthogonal complement. When $q$ is a prime power and when $(F, +)$ is chosen to be the elementary Abelian group (= additive group of $GF(q)$), then any linear code over $GF(q)$ is additive, but the converse is not true. The following theorem is a generalization to additive codes of a well-known result in the case of linear codes.

Theorem 1. Let $C$ be an additive code over $(F, +)$. Then its dual $C'$ is also an additive code which, as a subgroup of $G = (F, +)^n$, is isomorphic to the factor group $G/C$. Moreover, the dual of $C'$ is $C$ itself.

Proof. These properties are classical results on characters of Abelian groups (cf. for instance Hall 6), p. 195). However, since coding theorists might be not familiar with this subject, an elementary proof is given in the appendix (theorems 18 and 19).

3. Krawtchouk polynomials and MacWilliams transform

For fixed positive integers $n$ and $\lambda$, the Krawtchouk polynomial $P_k(x)$ of degree $k$ is defined by

$$P_k(x) = \sum_{j=0}^{k} (-1)^j \lambda^{k-j} \binom{n}{k} \binom{x-j}{k-j}, \quad 0 \leq k \leq n, \quad (4)$$

with $\binom{\ell}{j} = x(x-1) \ldots (x-j+1)/j!$. These polynomials were defined by Krawtchouk (cf. Szegö 16), p. 35) by means of the following orthogonality conditions:

$$\sum_{i=0}^{n} v_i P_r(i) P_s(i) = q^n v_r \delta_{r,s}, \quad (5)$$

where $\delta_{r,s}$ is the Kronecker symbol, $q = \lambda + 1$, and

$$v_i = (\binom{i}{\ell}) \lambda^i, \quad 0 \leq i \leq n. \quad (6)$$

The first (implicit) use of these polynomials in coding theory was made by
MacWilliams\(^\text{10}\)). The next theorem shows how they arise naturally from the definitions of sec. 2. For elementary Abelian groups, an equivalent statement was first given by Van Lint\(^9\).

**Theorem 2.** Let \(a\) be an element of \(V\) of weight \(w(a) = i\). Then one has

\[
\sum_{h \in Y_k} \langle a, h \rangle = P_k(i),
\]

where \(P_k(x)\) is the Krawtchouk polynomial (4), with \(\lambda = q - 1\), and \(Y_k\) is the set of elements of weight \(k\) in \(V\).

**Proof.** For a \(k\)-tuple \((s_1, \ldots, s_k)\) of integers, \(1 \leq s_1 < \cdots < s_k \leq n\), let us calculate the contribution \(c(s_1, \ldots, s_k)\) to the left-hand member of (7) of all elements \(h \in Y_k\) with \(h_{s_1}, \ldots, h_{s_k} \neq 0\). Using (3) we obtain

\[
c(s_1, \ldots, s_k) = \sum_{t=1}^{\lambda} \phi_t(a_{s_1}) \cdots \sum_{t=1}^{\lambda} \phi_t(a_{s_k}),
\]

by elementary calculation. On the other hand, it is well known that group characters satisfy

\[
\sum_{t=1}^{\lambda} \phi_t(f) = \begin{cases} 
\lambda, & f = 0, \\
-1, & f \neq 0,
\end{cases}
\]

for \(f \in F\). Substituting this in the right-hand member of (8), we deduce

\[
c(s_1, \ldots, s_k) = (-1)^j \lambda^{k-j},
\]

where \(j\) is the number of nonzero components of \(a\) among \(a_{s_1}, \ldots, a_{s_k}\). If \(a\) has weight \(i\), there are exactly \(\binom{n}{j}\binom{k-j}{i-j}\) choices for \((s_1, \ldots, s_k)\) corresponding to a given \(j\). Hence the sum \(\sum \langle a, h \rangle\) where \(h\) runs through all elements of weight \(k\) is equal to

\[
\sum_{j=0}^{n} (-1)^j \lambda^{k-j} \binom{n}{j} \binom{k-j}{i-j},
\]

i.e., to \(P_k(i)\), and the theorem is proved.

To the polynomials \(P_0, P_1, \ldots, P_n\), we associate the **Krawtchouk matrix** \(P\) of order \(n + 1\), over the integers, defined as follows:

\[
P = [P_k(i); \; 0 \leq i, \; k \leq n],
\]

i.e., the matrix whose \((i, k)\) entry is \(P_k(i)\).

Let us also recall the definition of the set \(Y_i\) (cf. theorem 2): for a given \(i\), it denotes the subset of all elements of weight \(i\) in \(V\), i.e.,

\[
Y_i = \{a \in V \mid w(a) = i\}.
\]
Theorem 3. The Krawtchouk matrix satisfies the two equations

\[ \Delta P = P^T \Delta, \]  

(11)

and

\[ P^2 = q^n I, \]  

(12)

with \( \Delta = \text{diag}(v_0, v_1, \ldots, v_n) \).

**Proof.** Observing that \( Y_i \) has cardinality \( v_i \), by (6), we can write, using theorem 2,

\[ \sum_{a \in Y_i} \sum_{h \in Y_k} \langle a, h \rangle = v_i P_k(i). \]

Hence \( v_i P_k(i) \) equals \( v_k P_i(k) \), for \( 0 \leq i, k \leq n \), which proves (11). Then (12) is a consequence of (11) and the orthogonality relations (5), since these can be written as \( P^T \Delta P = q^n \Delta \).

To an \((n+1)\)-tuple \( A = (A_0, A_1, \ldots, A_n) \) of rational numbers, we associate the homogeneous polynomial

\[ A(y, z) = \sum_{i=0}^{n} A_i y^i z^{n-i}. \]

Then the *MacWilliams transform* \(^{11}\) of \( A(y, z) \) is defined to be the polynomial

\[ A'(y, z) = A(z - y, z + \lambda y). \]

In order to calculate the expansion \( A'(y, z) = \sum A'_k y^k z^{n-k} \), we observe that \((z - y)^i (z + \lambda y)^{n-i}\) is the generating function of the Krawtchouk polynomials at point \( i \) (cf. Szegö\(^{16}\), p. 36):

\[ (z - y)^i (z + \lambda y)^{n-i} = \sum_{k=0}^{n} P_k(i) y^k z^{n-k}. \]

This clearly yields the formula

\[ A'_k = \sum_{i=0}^{n} A_i P_k(i), \quad 0 \leq k \leq n, \]  

(13)

for the coefficient \( A'_k \) of \( y^k z^{n-k} \) in \( A'(y, z) \). In the rest of this paper, we shall call MacWilliams transform the resulting correspondence (13) between the \((n + 1)\)-tuples \( A = (A_0, \ldots, A_n) \) and \( A' = (A'_0, \ldots, A'_n) \), i.e., in matrix form:

\[ A \rightarrow A' = A P, \]  

(14)
where $P$ is the Krawtchouk matrix (9). According to theorem 3, this mapping is one-to-one and is an involution up to the constant factor $q^n$:

$$ (A')' = q^n A, \quad \text{for any } A. $$

(15)

It will also be useful to associate the polynomial

$$ \alpha(x) = \alpha_0 P_0(x) + \alpha_1 P_1(x) + \ldots + \alpha_n P_n(x) $$

(16)
to the $(n + 1)$-tuple $\alpha = (\alpha_0, \alpha_1, \ldots, \alpha_n)$ of rational numbers $\alpha_i$. The components $\alpha_i$ of a polynomial $\alpha(x)$ of degree not exceeding $n$ in the basis of Krawtchouk polynomials can be calculated from the values assumed at the integral points $k$, $0 \leq k \leq n$, by the formula

$$ q^n \alpha_i = \sum_{k=0}^{n} \alpha(k) P_k(i), $$

(17)

which readily follows from (16) and (12). Another interesting identity, satisfied by any two $(n + 1)$-tuples $A$ and $\alpha$, is

$$ \sum_{k=0}^{n} A'_{k} \alpha(k) = q^n \sum_{i=0}^{n} A_i \alpha_i, $$

(18)

where $A'$ is the MacWilliams transform of $A$; this is an immediate consequence of (13) and (17).

For $A = (A_0, A_1, \ldots, A_n)$, let $s(A)$ denote the number of nonzero components $A_i$, $1 \leq i \leq n$, of $A$ and let $d(A)$ denote the least integer $k$, $1 \leq k \leq n$, for which $A_k$ is not zero. A useful property of the MacWilliams transform is the following.

**Theorem 4.** See ref. 10. Let $A$ be an $(n + 1)$-tuple with $A_0 \neq 0$, and let $A'$ be the MacWilliams transform of $A$. Then $d(A)$ and $s(A')$ are related by

$$ s(A') \geq [(d(A) - 1)/2]. $$

**Proof.** From (18) and the definition of $d(A)$, we deduce

$$ \sum_{k=0}^{n} A'_{k} \alpha(k) = q^n A_0 \alpha_0, $$

(19)

for any polynomial (16) of degree not exceeding $d(A) - 1$. Let us assume $s(A') < t$, with $t = [(d(A) - 1)/2]$. Then there exists a polynomial $\beta(x)$ of degree $t$ vanishing at each point $x = k$ such that $A'_{k} \neq 0$, $0 \leq k \leq n$. With $\alpha(x) = (\beta(x))^2$, eq. (19) becomes (cf. (17))

$$ 0 = A_0 \sum_{k=0}^{n} P_k(0) (\beta(k))^2. $$

(20)
Since \( P_k(0) = v_k \) is positive, the right-hand member of (20) cannot be zero for \( A_0 \neq 0 \). The theorem follows from this contradiction.

4. Characteristic matrices of a code

For an \((n, M)\) code \( C \) over \( F \) and for an integer \( k, 0 \leq k \leq n \), we define the \((M \times v_k)\) matrix \( H_k \), over the field \( \mathbb{Q}_v \) of complex \( v \)th roots of unity, by

\[
H_k = [\langle a, h \rangle; \; a \in C, \; h \in Y_k],
\]

for some numbering of \( C \) and \( Y_k \) (cf. (10)). The matrix \( H_k \) will be called the \( k \)th characteristic matrix of \( C \). The following theorem relates the characteristic matrices of a code and its distance properties.

**Theorem 5.** The \( k \)th characteristic matrix of a code satisfies

\[
H_k \tilde{H}_k = [P_k(d(a, b)); \; a, b \in C],
\]

where \( P_k(x) \) is the Krawtchouk polynomial of degree \( k \) and \( d \) is the Hamming distance.

**Proof.** For \( a, b \in C \), let us calculate the element numbered by \( (a, b) \) in the matrix product \( H_k \tilde{H}_k \). Using (21) and theorem 2, we obtain

\[
(H_k \tilde{H}_k)(a, b) = \sum_{h \in Y_k} \langle a - b, h \rangle = P_k(w(a - b)).
\]

Hence the theorem is proved, by (2).

The distance distribution of an \((n, M)\) code \( C \) is defined to be the \((n+1)\)-tuple \( A(C) = (A_0(C), A_1(C), \ldots, A_n(C)) \) of nonnegative rational numbers

\[
A_i(C) = \frac{1}{M} \left| \{ (a, b) \mid a, b \in C, d(a, b) = i \} \right|.
\]

In other words, \( A_i(C) \) is the mean number of codewords at distance \( i \) from a fixed codeword. In particular, \( A_0(C) \) always equals unity. The following result plays a central role in this paper.

**Theorem 6.** The MacWilliams transform of the distance distribution \( A(C) \) of any code \( C \) is nonnegative. More precisely, one has

\[
A'_k(C) \geq 0, \; k = 0, 1, \ldots, n.
\]

**Proof.** Let \( C \) be an \((n, M)\) code over \( F \) and let \( j \) stand for the all-one vector of order \( M \). Denoting by \( ||y|| = (\bar{y} y)^{1/2} \) the Hermitian norm of a complex
vector $y$ and using theorem 5, eqs (22) and (13), successively, we obtain

$$
\|\tilde{H}_k\| = \sum_{a,b \in C} P_k(d(a, b))
$$

$$
= M \sum_{i=0}^{n} A_i(C) P_k(i)
$$

$$
= M A_k'(C).
$$}

Since the left-hand member of (23) is nonnegative, the theorem is proved.

**Corollary 7.** Let $A(C)$ be the distance distribution of a code $C$. Then the $k$th component of the MacWilliams transform of $A(C)$ is zero if and only if the sum of rows of the $k$th characteristic matrix of $C$ is zero. In other terms, one has

$$
(A_k'(C) = 0) \iff (j^T H_k = 0).
$$

**Proof.** This is an immediate consequence of (23) and a well-known property of the norm.

We conclude this section with a generalization of the MacWilliams equations relating the weight distribution of a linear code and that of its dual. Let $C$ be an additive $(n, M)$ code over an Abelian group. Then it is easily seen that the distance distribution of $C$ reduces to its weight distribution. In other words, we have (cf. (10))

$$
A_k(C) = |C \cap Y_k|, \quad 0 \leq i \leq n.
$$

**Theorem 8.** The weight distribution of the dual $C'$ of an additive code $C$ is, up to a constant factor, the MacWilliams transform of the weight distribution of $C$ itself. More precisely, one has

$$
|C| A_k(C') = A_k'(C), \quad 0 \leq k \leq n.
$$

**Proof.** Let $H_k$ be the $k$th characteristic matrix of the given $(n, M)$ code $C$. Since $C$ is additive, we deduce from (21)

$$
\|\tilde{H}_k j\| = \sum_{h \in X_k} \sum_{a,b \in C} \langle a - b, h \rangle
$$

$$
= M \sum_{h \in Y_k} [ \sum_{u \in C} \langle u, h \rangle ],
$$

with $M = |C|$. Now, as shown in the appendix (theorem 17), the term between square brackets in (25) is equal to $M$ or to zero, according to whether $h$
belongs to \( C' \) or not. Hence (25) becomes
\[
||\tilde{R}_k||^2 = M^2 |C' \cap Y_k| \\
= M^2 A_k(C'),
\]
by (24). Comparing this with (23), we have the desired result.

5. A linear-programming problem

For a positive integer \( n \), let \( D \) be a subset of \( N = \{1, 2, \ldots, n\} \). Then \( \bar{I}(D) \) is defined to be the set of codes of length \( n \), over a given alphabet, whose distance distribution satisfies
\[
(A_i(C) \neq 0, \ i \in N) \Rightarrow (i \in D).
\]
(26)
In other terms, a code belongs to \( \bar{I}(D) \) whenever the distance between any two distinct codewords belongs to the given "distance set" \( D \). We are interested in the following problem: to find a "realistic" upper bound for the number of words in a code of \( \bar{I}(D) \). To this, we associate the problem \( P-I \) of linear programming (cf. for instance Simonnard 14)), with \( m (= |D|) \) variables \( A_i \) and \( n \) inequalities:

\[
P-I \left\{ \begin{array}{ll}
\sum_{i \in D} A_i P_k(i) & \geq -v_k, \ \ k \in N, \\
A_i & \geq 0, \ \ i \in D, \\
\text{maximize } z = \sum_{i \in D} A_i,
\end{array} \right.
\]
(27) (28) (29)

where \( P_k(x) \) is the Krawtchouk polynomial (4) and \( v_k \) is defined as in (6).
Any \( m \)-tuple \( (A_i, \ i \in D) \) of rational numbers \( A_i \) will be called a program of \( P-I \) if it satisfies (27) and (28); it will be called a maximal program if (in addition to this) it maximizes \( z \) and the maximum value of \( z \) will be denoted by \( \bar{z}(D) \).

Theorem 9 implies the existence of at least one maximal program and theorem 10 shows the connection between \( P-I \) and the coding problem stated above.

Theorem 9. Problem \( P-I \) admits at least one program. Moreover, any program \( (A_i) \) is bounded by
\[
A_i \leq v_i, \ \forall \ i \in D.
\]
(30)

Proof. First, it is obvious that the zero \( m \)-tuple is a program. In order to prove (30), we embed the given program \( (A_i) \) into an \((n + 1)\)-tuple \( A \) by defining \( A_0 = 1 \) and \( A_i = 0 \) for \( i \in N - D \). Since \( v_k = P_k(0) \), inequalities (27) are equivalent to
\[
A'_k \geq 0, \ \ k \in N,
\]
(31)

where $A'$ is the MacWilliams transform of $A = (A_0, A_1, \ldots, A_n)$. On the other hand, using (14) and (15), we obtain

$$\sum_{k=0}^{n} (v_i - P_i(k)) A'_k = q^n (v_i - A_i),$$

for $i = 0, 1, \ldots, n$. Hence (30) follows from (31) and the obvious consequence $(v_i \geq P_i(k))$ of theorem 2.

**Theorem 10.** The number $\bar{M}(D) = 1 + \bar{z}(D)$ is an upper bound for the number of words in any code belonging to $\Gamma(D)$.

**Proof.** Let $C$ be an $(n, M)$ code of $\Gamma(D)$. According to theorem 6, the distance distribution $A = A(C)$ of $C$ satisfies (31) or, equivalently, (27). Hence $(A_i, i \in D)$ is a program of $P-I$ and the theorem follows from the fact that $M = 1 + z$ for such a program (cf. (29)).

**Example.** Let $q = 2, n = 14, D = \{6, 8, 10, 12, 14\}$. Problem $P-I$ can be solved by hand, by means of the simplex algorithm. It turns out that the optimal solution of $P-I$ is unique, with

$\bar{M}(D) = 64, A_6 = 42, A_8 = 7, A_{10} = 14,$

and $A_{12} = A_{14} = 0$. In fact there actually exists a binary $(14, 64)$ code in $\Gamma(D)$; such a code can be derived from the extended $(16, 256)$ Nordstrom–Robinson code (cf. Goethals 4) in an easy manner. So, according to theorem 10, we have shown the maximality of any $(14, 64)$ code in $\Gamma(D)$, as well as the uniqueness of the distance distribution of such a code.

Unfortunately, the bound $\bar{M}(D)$ resulting from theorem 10 is not always as good as in the preceding example: for $q = 2, n = 13, D = \{6, 8, 10, 12\}$, problem $P-I$ yields $\bar{M}(D) = 40$, while the Johnson bound 7 insures $M \leq 35$ for any $(n, M)$ code in $\Gamma(D)$ and while the best known code of $\Gamma(D)$ has $M = 32$ codewords.

6. The dual problem

To problem $P-I$ we associate its dual problem $P-II$, with $n$ inequalities in the $m$ variables $\alpha_k$, defined as follows:

$$\begin{align*}
\sum_{k \in N} \alpha_k P_k(i) &\leq -1, \quad i \in D, \\
\alpha_k &\geq 0, \quad k \in N, \\
\text{minimize } \zeta &\triangleq \sum_{k \in N} \alpha_k v_k.
\end{align*}$$

A program and a minimal program of $P-II$ are defined in a similar manner as
in sec. 5. As an immediate application of the well-known properties of duality in linear programming (cf. Simonnard\textsuperscript{14}, pp. 88–95), and using theorem 9, with the definitions (13), (16), we have the following results.

Theorem 11. (i) Both problems P-I and P-II admit at least one optimal program (maximal for P-I, minimal for P-II). Moreover, the optimal values of $z$ and of $\zeta$ are equal to $\bar{z}(D)$, so one has

$$z \leq \bar{z}(D) \leq \zeta,$$

for any pair $(A_i, (\alpha_k))$ of programs of P-I and P-II, respectively.

(ii) For any pair of optimal programs $(A_i)$ of P-I and $(\alpha_k)$ of P-II, one has the two sets of equations

$$\alpha_k A'_k = 0, \quad \forall \ k \in N,$$

and

$$A_i \alpha(i) = 0, \quad \forall \ i \in D,$$

with $A_0 = \alpha_0 = 1$ and $A_i = 0, \forall \ i \in N - D$. Conversely, if programs $(A_i)$ of P-I and $(\alpha_k)$ of P-II satisfy these equations, then both are optimal.

Before applying this result to coding theory, we need a definition. For a subset $D$ of $N$, we shall denote by $p(D)$ the set of polynomials $\alpha(x)$ of degree not exceeding $n$, over the rational numbers, satisfying

$$\alpha_0 = 1, \quad \alpha_k \geq 0, \quad \forall \ k \in N,$$

$$\alpha(i) \leq 0, \quad \forall \ i \in D,$$

where $\alpha_0, \alpha_1, \ldots, \alpha_n$ are the components of $\alpha(x)$ in the basis of Krawtchouk polynomials (cf. (16)).

Theorem 12. For any $(n, M)$ code in $\Gamma(D)$ and any polynomial $\alpha(x)$ in $p(D)$, one has

$$M \leq \alpha(0).$$

Moreover, if $M = \alpha(0)$, then the distance distribution of the code satisfies (35) and (36) with $A = A(C)$.

Proof. Conditions (37) are equivalent to (32) and (33); hence $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ is a program of P-II. On the other hand, by (16) and (34), one has $\alpha(0) = 1 + \zeta$. Therefore, theorem 11-(i) yields

$$\bar{M}(D) = \min_{\alpha \in p(D)} (\alpha(0)),$$

with $\bar{M}(D) = 1 + \bar{z}(D)$, and (38) is a consequence of theorem 10. The second part of the theorem follows from theorem 11 and the fact that the distance distribution $(A_i(C), i \in D)$ of a code $C$ in $\Gamma(D)$ is a program of P-I.
An \((n, M)\) code \(C\) in \(\Gamma(D)\) will be called maximal if it satisfies \(M = \bar{M}(D)\) or, equivalently, if there exists a polynomial \(\alpha(x)\) in \(p(D)\) for which \(M = \alpha(0)\). As will be seen in sec. 7, the characteristic identities (35) and (36) satisfied by the distance distribution \((A_i(C))\) of maximal codes are very useful in the theory of these codes.

**Example.** Let \(q = 2\), \(n = 47\) and
\[
D = [12, 16] \cup [20, 24] \cup [28, 32] \cup [36, 47],
\]
with \([s, t] = \{s, s + 1, \ldots, t\}\). Let us consider the polynomial \(\hat{\alpha}(x)\) of degree 7 vanishing at points \(x = 12, 16, 20, 24, 28, 32, 36\) and satisfying \(\alpha(0) = 2^{23}\). Elementary calculation gives the following values for the components \(\alpha_i\) of \(\hat{\alpha}(x)\):
\[
\alpha_0 = \ldots = \alpha_3 = 1, \quad \alpha_4 = \ldots = \alpha_7 = 1/9,
\]
and, by definition, \(\alpha_i = 0\) for \(i > 7\). Hence \(\alpha(x)\) satisfies (37) and, therefore, belongs to \(p(D)\). Using theorem 12, we have \(M \leq 2^{23}\) for any code \(C\) in \(\Gamma(D)\).

Now there is a well-known \((47, 2^{23})\) linear code in \(\Gamma(D)\), namely the expurgated quadratic residue code \(QR(47)\), for which the nonzero weights (or distances) are precisely the zeros (12, 16, \ldots, 36) of \(\alpha(x)\) (cf. Pless 13)).

By theorem 12, this code is maximal in \(\Gamma(D)\). Moreover, any maximal code (i.e., satisfying \(M = \bar{M}(D) = 2^{23}\)) has the same distance distribution as \(QR(47)\).

Indeed, eqs (35) and (36) imply
\[
A'_0(C) = 2^{23}, \quad A'_1(C) = \ldots = A'_7(C) = 0, \quad (40)
\]
respectively, for any such maximal code \(C\), and (39) gives a unique solution for \((A_i(C), i \in \bar{D})\).

The maximality of \(QR(47)\) in \(\Gamma(D)\) is a particular instance of a more general result, which we shall prove by using characteristic matrices, although it is in fact an easy consequence of theorem 11-(ii):

**Theorem 13.** Let \(D\) be a subset of \(N\) and \(\alpha(x)\) a polynomial in \(p(D)\). On the other hand, let \(C\) be an \((n, M)\) code in \(\Gamma(D)\) whose distance distribution satisfies
\[
(A_i(C) \neq 0) \Rightarrow (\alpha(i) = 0), \quad \forall i \in D,
\]
and \(A'_1(C) = A'_2(C) = \ldots = A'_{r}(C) = 0\), with \(r = \deg(\alpha(x))\). Then \(C\) is maximal in \(\Gamma(D)\).

**Proof.** Let \(H_k\) be the \(k\)th characteristic matrix of \(C\). According to theorem 5, we have
\[
\sum_{k=0}^{r} \alpha_k H_k \bar{H}_k = \alpha(0) I. \quad (41)
\]
Indeed, for \( a, b \in C \), the \((a, b)\)-entry in the left-hand member of (41) is equal to \( \alpha(d(a, b)) \) and, by (40), this is zero for \( a \neq b \). Multiplying both members of (41) by \( j^T \), the all-one row vector of order \( M \), we obtain, using corollary 7,

\[
\alpha_0 j^T H_0 \bar{H}_0 = \alpha(0) j^T.
\]

Now, since \( H_0 = j \) and \( \alpha_0 = 1 \), this implies \( M = \alpha(0) \) and the theorem is proved.

**Example.** Let us assume there exists a self-dual \((26, 2^{13})\) binary linear code in \( \Gamma(D) \), with \( D = \{8, 10, 12, 14, 16, 18, 26\} \). Then any such code would be maximal in \( \Gamma(D) \). In order to prove this, it is sufficient to verify that the polynomial

\[
\beta(x) = \prod_{i \in D} (1 - x/i)
\]

has positive components in the basis of Krawtchouk polynomials. With \( \alpha(x) = \beta(x)/\beta_0 \), the maximality of \( C \) then follows from theorem 13. We observe that the MacWilliams identities completely determine the distance (or weight) distribution of the code: \( A_0 = A_{26} = 1 \), \( A_8 = A_{18} = 650 \), \( A_{10} = A_{16} = 845 \), \( A_{12} = A_{14} = 2600 \).

7. Codes with a specified minimum distance

One of the most important problems in coding theory is to find good codes having a given length \( n \) and minimum distance at least a given \( \delta \), i.e., codes in \( \Gamma(D) \) with

\[
D = \{\delta, \delta + 1, \ldots, n\},
\]

having as many words as possible. Therefore, coding theorists were interested in upper bounds for the number of codewords in a code belonging to \( \Gamma(D) \). For the state of affairs concerning the important binary case \((q = 2)\), we refer to Johnson 7).

Applying theorems 11 and 12, we will now obtain three of the most classical bounds, as well as a characterization of codes meeting them. First, we have the Plotkin bound (cf. Berlekamp 1), p. 315).

**Theorem 14.** For any \( q \)-ary \((n, M)\) code of designed minimum distance \( \delta \), with \( \delta > n \lambda/q, \lambda = q - 1 \), one has

\[
M \leq \frac{q \delta}{q \delta - n \lambda}.
\]

(43)

Moreover, any code satisfying equality in (43) is equidistant, with distance \( \delta \).

**Proof.** Let us consider the polynomial

\[
\alpha(x) = 1 + \frac{P_1(x)}{q \delta - n \lambda}.
\]

(44)
Since \( P_0(x) = 1 \) and \( P_1(x) = n \lambda - q x \), it follows from (37) and (44) that \( \alpha(x) \) belongs to \( p(D) \), when \( D \) is defined by (42). Hence (43) is a consequence of theorem 12, since \( \alpha(0) = q \delta / (q \delta - n \lambda) \). Next, let \( C \) be an \((n, M)\) code, with \( M = \bar{M}(D) = \alpha(0) \). By theorem 12, and (36), the distance distribution of \( C \) satisfies \( A_i(C) = 0 \), for \( i > \delta \); this concludes the proof.

Next, we obtain the Singleton bound and the distance distribution of codes meeting that bound, i.e., the so-called "maximum distance separable codes" (cf. Singleton 15), and Berlekamp 1), pp. 309 and 429). The first derivation of the distance distribution for unrestricted codes seems to be due to Mar- guinaud 12).

**Theorem 15.** For any \( q \)-ary \((n, M)\) code of designed minimum distance \( \delta \), one has

\[
M \leq q^{n-\delta+1}.
\]

Moreover, the distance distribution of any code \( C \) satisfying equality in (45) is given by

\[
A_{n-j}(C) = \sum_{i=j}^{n-\delta} (-1)^{i-j} \binom{n}{i} (q^{n-\delta+1-i} - 1),
\]

for \( j = 0, 1, \ldots, n - \delta \).

**Proof.** Let us consider the polynomial

\[
\alpha(x) = q^{n-\delta+1} \prod_{i=\delta}^{n} (1 - x/i).
\]

Using (17) and identity (61) of the appendix, with \( j = \delta - 1 \), we obtain the following formula for the components of \( \alpha \):

\[
\alpha_k = \binom{n-k}{n-\delta-1}, \quad 0 \leq k \leq n - \delta + 1,
\]

and \( \alpha_k = 0 \), for \( k > n - \delta + 1 \). Hence \( \alpha(x) \) belongs to \( p(D) \) and (45) results from theorem 12. Next, let \( C \) be an \((n, M)\) code in \( T(D) \) with \( M = \bar{M}(D) = q^{n-\delta+1} \). By (35), the distance distribution \( (A_i) \) of \( C \) satisfies

\[
A'_0 = q^{n-\delta+1}, \quad A'_1 = A'_2 = \ldots = A'_{n-\delta+1} = 0.
\]

It remains to be shown that eqs (47) admit as their unique solution (with \( A_0 = 1, A_1 = \ldots = A_{\delta-1} = 0 \)) the numbers \( A_i = A_i(C) \) defined by (46); this has been implicitly proved by Goethals 3).

Finally, we derive the sphere-packing bound and the Lloyd theorem for perfect codes over unrestricted alphabets. A proof of this theorem is given
by Van Lint \(^9\)), when \( q \) is a prime power. The general result has also been obtained by Lenstra \(^9\)) using different methods.

**Theorem 16.** For any \( q \)-ary \((n, M)\) code of designed minimum distance \( \delta \), one has

\[
M \leq q^n \left/ \sum_{i=0}^{t} v_i \right.
\]

with \( t = [(\delta - 1)/2] \). Moreover, if there exists a perfect \( t \)-error-correcting code (i.e., a code of \( I(D) \) satisfying equality in (48)), then the *Lloyd polynomial*

\[
Q_t(x) = \sum_{k=0}^{t} P_k(x)
\]

of degree \( t \) has \( t \) distinct integral zeros in the set \( N = \{1, 2, \ldots, n\} \).

**Proof.** Let us define \( M_t = v_0 + v_1 + \ldots + v_t \) and

\[
\alpha_k = \left( \frac{Q_t(k)}{M_t} \right)^2,
\]

for \( k = 0, 1, \ldots, n \), where \( Q_t(x) \) is the Lloyd polynomial. From (11), (16) and (49) we deduce the following formula for the value of \( \alpha(x) \) at point \( i \):

\[
M_t^2 v_t \alpha(i) = \sum_{k=0}^{n} v_k P_i(k) (Q_t(k))^2.
\]

Since \((Q_t(x))^2\) has degree less than \( \delta \), the orthogonality relations (5) show that the right-hand member of (50) vanishes for \( i = \delta, \delta + 1, \ldots, n \). Accordingly, one has \( \alpha(i) = 0 \), \( \forall \ i \in D \), so that \( \alpha(x) \) belongs to \( p(D) \). On the other hand, adding up both members of (5) for \( r \) and \( s \) running through \( \{0, 1, \ldots, t\} \), we obtain

\[
\sum_{k=0}^{n} v_k (Q_t(k))^2 = q^n M_t.
\]

Comparing this with (50), we have \( \alpha(0) = q^n/M_t \). Hence (48) is a consequence of theorem 12.

Next, let us denote by \( C \) a perfect \( t \)-error-correcting code. By definition, \( C \) is maximal in \( I(D) \) with \( |C| = M(D) = q^n/M_t \), \( t = (\delta - 1)/2 \). Consequently, using theorem 12, we obtain

\[
Q_t(k) A'_k(C) = 0, \quad \forall \ k \in N,
\]
from (35) and (49), where \( A_k(C) \) is the distance distribution of \( C \). On the other hand, by theorem 4, the number \( s(A') \) of integers \( k \) with \( k \in N, A'_k(C) \neq 0 \), is at least \( t \). Since \( Q_t(x) \) has degree \( t \), it follows from (51) that \( s(A') \) equals \( t \) and that \( Q_t(k) \) vanishes for each \( k \in N \) such that \( A'_k(C) \neq 0 \). Hence the theorem is proved.

**Remarks.** (i) When \( C \) is a perfect additive code over an Abelian group, it results from theorem 8 that the \( t \) zeros of \( Q_t(x) \) are the nonzero distances of the dual code \( C' \) of \( C \), i.e., the integers \( k \in N \) such that \( A_k(C') \neq 0 \). This result is due to MacWilliams \(^{10}\) for perfect linear codes over finite fields.

(ii) Recently, extending results of Van Lint \(^9\), Tietäväinen \(^{17}\) proved the nonexistence of perfect \( t \)-error-correcting \( q \)-ary codes, for \( t \geq 2 \) and \( q = \text{prime power} \), other than the two Golay codes and the binary repetition codes of odd length.

(iii) The Grey bound \(^5\) for complementary binary codes can also be derived from theorem 12.

8. **Appendix**

Let \( G \) be a finite Abelian group of order \( m \) and period \( v \). A *character* of \( G \) is a homomorphic mapping of \( G \) into the multiplicative group of the cyclotomic field \( Q_v \). It is well known that there are \( m \) distinct characters. Moreover, the characters \( \psi(x) \) can be numbered with the elements \( x \) of \( G \) in such a way that the mapping of \( G \times G \) into \( Q_v \) defined by

\[
\langle x, y \rangle = \psi_x(y), \quad x, y \in G,
\]

becomes symmetric. This mapping will be called an *inner product* of \( G \). If \( + \) stands for the group operator, then the inner product satisfies the two relations

\[
\langle x, y + z \rangle = \langle x, y \rangle \langle x, z \rangle \quad (52)
\]

and

\[
(\langle x, u \rangle = \langle y, u \rangle, \quad \forall u \in G) \iff (x = y), \quad (53)
\]

for any \( x, y, z \) in \( G \). In fact these properties, together with \( \langle x, y \rangle = \langle y, x \rangle \), can be taken as axioms for an inner product.

For any subgroup \( H \) of \( G \), we define the *dual of \( H \)* to be the following subset of \( G \):

\[
H' = \{ x \in G \mid \langle u, x \rangle = 1, \quad \forall u \in H \}. \quad (54)
\]

From (52) it immediately follows that \( H' \) is itself a subgroup of \( G \).

**Theorem 17.** If \( H' \) is the dual of a subgroup \( H \) of \( G \), then one has

\[
\sum_{x \in H'} \langle u, x \rangle = \begin{cases} |H|, & \text{for } x \in H', \\ 0, & \text{for } x \in G - H'. \end{cases} \quad (55)
\]
Proof. Let $h_1, h_2, \ldots, h_k$ be independent generators of $H$, of order $m_1, m_2, \ldots, m_k$, respectively. For a fixed $x$ in $G$, we set

$$\omega_i = \langle h_i, x \rangle, \quad 1 \leq i \leq k. \tag{56}$$

Then $\omega_i$ is a complex $m_i$th root of unity. From (54) and (56) it follows that $x$ belongs to $H'$ if and only if $\omega_1 = \omega_2 = \ldots = \omega_k = 1$. Now using (52) we obtain

$$\sum_{u \in H} \langle u, x \rangle = \prod_{i=1}^k (1 + \omega_1 + \ldots + \omega_i^{-m_i-1}). \tag{57}$$

Hence $x$ belongs to $H'$ if and only if the right-hand member of (57) is not zero, and the theorem is proved.

Theorem 18. Duality among subgroups of $G$ satisfies

$$|H| \cdot |H'| = |G| \quad \text{and} \quad (H')' = H.$$

Proof. By summation of the two members of (55) for $x$ running through $G$, we readily obtain the first equality. As a consequence, we have $|(H')'| = |H|$, from which the second equality follows, since, by (54), $H$ is a subgroup of $(H')'$.

Theorem 19. Let $H$ be a subgroup of $G$. Then the subgroup $H'$ of $G$ is isomorphic to the factor group $G/H$.

Proof. Let $x$ be an element of $G$. Then the mapping

$$u \rightarrow \langle u, x \rangle, \quad u \in H,$$

of $H$ into $Q_v$, is a character of $H$. Hence there exists a unique element $h(x)$ in $H$ such that

$$\langle u, x \rangle = \langle u, h(x) \rangle_H, \quad u \in H, \tag{58}$$

where $\langle , \rangle_H$ stands for the inner product of $H$. From the properties (52), (53) of the inner product and from theorem 18, it follows that the mapping $h$ of $G$ into $H$, defined by (58), is a homomorphism whose kernel is $H'$ and whose range is $H$. Hence the theorem is proved.

Finally, we quote, without detailed proof, some properties of the Krawtchouk polynomials introduced in sec. 3:

$$(k + 1) P_{k+1}(x) = ((n - k) \lambda + k - q x) P_k(x) - \lambda (n - k + 1) P_{k-1}(x), \tag{59}$$

$$P_k(x) = \sum_{t=0}^k (-q)^t \lambda^{k-t} \binom{k}{k-t} \binom{n-k}{q-t}, \tag{60}$$

$$\sum_{k=0}^n \binom{n-k}{q-t} P_k(i) = q^i \binom{n-1}{q-1}, \tag{61}$$
with \( q = \lambda + 1 \), for any \( i, j, k \) with \( 0 \leq i, j, k \leq n \). Recurrence formulas (59) are useful for computation. Such formulas are classical in theory of orthogonal polynomials (cf. Szegö \(^{16}\), p. 42). Equations (60) express the Krawtchouk polynomials in the basis of polynomials \((\cdot)\); they can be derived from (4) by elementary combinatorial identities. Finally, (61) follows from (60).

Acknowledgment

The author is indebted to Dr J. M. Goethals for many interesting discussions during the preparation of this paper.

MBLE Research Laboratory

REFERENCES

8) H. W. Lenstra, Jr., Two theorems on perfect codes, Discrete Mathematics (to appear).
13) V. Pless, Information and Control 6, 147-152, 1963.
17) A. Tietäväinen, On the nonexistence of perfect codes over finite fields, to be published.