NOTICE: When government or other drawings, specifications or other data are used for any purpose other than in connection with a definitely related government procurement operation, the U. S. Government thereby incurs no responsibility, nor any obligation whatsoever; and the fact that the Government may have formulated, furnished, or in any way supplied the said drawings, specifications, or other data is not to be regarded by implication or otherwise as in any manner licensing the holder or any other person or corporation, or conveying any rights or permission to manufacture, use or sell any patented invention that may in any way be related thereto.
Scientific Report No. 5
Contract AF19(604)-7493
March 1963

On the Weights of the Elements
of Binary Group Codes

by

L. Calabi and E. Myrvaagnes

409595

Air Force Cambridge Research Laboratories
Office of Aerospace Research
United States Air Force
Bedford, Massachusetts

PARKE MATHEMATICAL LABORATORIES, Inc.
One River Road • Carlisle, Massachusetts
On the Weights of the Elements of Binary Group Codes

by

L. Calabi and E. Myrvaagnes
Requests for additional copies by Agencies of the Department of Defense, their contractors, and other Government agencies should be directed to the:

DEPARTMENT OF DEFENSE DOCUMENTATION CENTER (D.D.C.)
ARLINGTON HALL STATION
ARLINGTON 12, VIRGINIA

Department of Defense contractors must be established for ASTIA services or have their 'need-to-know' certified by the cognizant military agency of their project or contract.

All other persons and organizations should apply to the:

U.S. DEPARTMENT OF COMMERCE
OFFICE OF TECHNICAL SERVICES
WASHINGTON 25, D.C.

A limited number of copies are also available by writing to:

PARKE MATHEMATICAL LABORATORIES, INC.
ONE RIVER ROAD
CARLISLE, MASSACHUSETTS
Abstract

Various necessary and sufficient conditions are given for the existence of codes with preassigned weights. Some properties of the weight distribution are deduced.
Table of Contents

Introduction

1. Codes with preassigned weight vectors ........................................ 1
2. Further modifications of Theorem 1 ........................................... 5
3. Equivalence of weight vectors .................................................. 13
Introduction

In our study of the minimal weight that the elements of a $K$-dimensional binary group code $A(n,k)$ of length $n$ can have, one of us gave [6] an elementary, though long, proof of various existence theorems for binary group codes. We present here these and other similar results, relating and deriving them from a well known theorem. As is often the case, these necessary and sufficient conditions for the existence of codes are not easily applied: indeed they require the use of high-speed computers already for small values of $n$ and $K$. We have been able, however, to derive from them some special cases, and some necessary conditions, of practical utility. These are given in the last section. Further study in this direction would seem justified.
1. Codes with preassigned weight vectors.

Let \( x_1, x_2, \ldots, x_k \) be the elements of a group code \( A = A(n, k) \).
We shall always assume that \( x_n \) is the zero vector; that \( x_n, x_{n+1}, \ldots, x_{2^n-1} \)
are independent; and that the numeration is so chosen that \( \sum x_i 2^i = x_{2^n-1} \).
where the first summation is of vectors over the field of two elements.

Let \( W \) be the column vector whose \( i \)-th row is \( w_i \), the weight of \( x_i \);
notice that \( w_i = 0 \) is not in \( A \). \( W \) will be called the weight vector of \( A \).

More generally, let \( W \) be a \( (2^{k-1} \times 1) \) matrix whose elements are strictly positive integers \( w_i \). We will say that \( W \) is admissible if it is the weight vector of some code \( A \).

In order to formulate a well known criterion of admissibility we have to introduce the following \( (2^{k-1} \times 2^{k-1}) \) matrix \( C \). Its row number \( 2^i \) consists, from left to right, of \( 2^{k-1} \) zeros, followed by \( 2^{k-1} \) consecutive ones, then \( 2^{k-1} \) consecutive zeros, then \( 2^{k-1} \) consecutive ones..., to exhaustion; its row number \( \sum_{j=0}^{2^{k-1} - 2} 2^i \) is the sum mod. 2 of the rows number \( 2^i, 2^{i+1}, \ldots, 2^{k-1} \). It is easy to recognize that \( C \) is the matrix introduced by MacDonald [1] and used by Fontaine and Peterson [2]. If \( J \) denotes the \( n \times 2^{k-1} \) matrix of all ones, one has [1,2]

\[
C^T = 2^{k-1} (2^k - J).
\]

Theorem 1([1,2,3,7]): \( W \) is the weight vector of a code \( A(n, k) \) if, and only if

1) \( \sum w_i = n \cdot 2^{k-i} \)

2) the elements of \( N = C^T W \) are all non-negative integers.

If \( W \) is the weight vector of \( A \), \( N \) is called the modular (representation) vector of \( A \). If \( n_i \) is the integer in the \( i \)-th row of \( N \), and if \( \theta \) is the matrix whose \( i \)-th row is \( x_i \cdot 2^{-i} \), then \( \theta \) has \( n_i \) columns which represent in binary form the integer \( i \). In particular then \( \sum n_i = n \).
The matrix $C$ for $k=4$.

Letting $I$ denote the $(2^{k-1}) \times 1$ matrix of all ones, we can prove:

**Theorem 2:** $W$ is admissible if and only if there is a matrix $N$, all the elements of which are non-negative integers, such that

\[ CW = 2^{k-2} N + \left( \sum \omega_i \right) I. \]

Moreover, if 3) is satisfied, letting $n = \Sigma n_i$ one has $\Sigma \omega_i = n \cdot 2^{k-1}$; and then $W$ is the weight vector of a code $A(n, k)$.

To prove that 3) is necessary we use Theor. 1. From 2),

\[ N = 2^{k-1} \frac{C W - 2^{k-1} J V_j}{J W} \]

but 1) implies $J W = n \cdot 2^{k-1} I = \sum \omega_i I$.

To show that 3) is sufficient, let us first show that 3) implies $\Sigma \omega_i = 2^{k-1} \Sigma n_i$. Remembering that each column of $C$ has exactly $2^{k-1}$ ones [1], we have

\[ JC W = 2^{k-1} J W = 2^{k-1} \sum \omega_i I_j. \]
on the other hand
\[ 2^{k-2} J H + \left( \frac{1}{2} \Sigma \omega_i \right) J I = 2^{k-2} \Sigma n_i I + \left( \frac{1}{2} \Sigma \omega_i \right) K 2^{k-1} I. \]

Thus 3) implies
\[ 2^{k-2} \Sigma \omega_i = 2^{k-2} \Sigma n_i + \frac{1}{2} \left( 2^{k-1} \right) \Sigma \omega_i, \]

which yields 1) with \( n = \Sigma n_i \). Further
\[ C' I = 2^{k'-2} C W - 2^{k'-2} J W = \eta + 2^{k'-2} \Sigma \omega_i I - 2^{k'-2} \Sigma \omega_i I = \eta \]

which is 2); and hence 3) is sufficient. It may be interesting to note that the necessity of 3) follows also from the "mapping theorem" of Assmus and Mattson [4].

If we denote by \( C_j \) the \( j \)-th row of \( C \), 3) can be written
\[ C_j I = n_j 2^{k-2} + \frac{1}{2} \Sigma \omega_i, \quad j = 1, 2, \ldots, 2^{k-1}. \]

This relation gives a different interpretation to the integers \( n_j \).
If \( W \) is the weight vector of \( A(n, k) \), the weights not added in the sum \( C_j I \) correspond to the elements of a subcode (or subgroup) of \( A \) that we can denote \( A_j (n_j, k-i) \). In fact the \( k \)-th component of \( C_j \) can be considered as the value at \( x_i \) of the \( j \)-th character (with values \( \omega_i \) instead of \( j, -j \)). Thus \( \Sigma \omega_i - C_j I \) is the sum of the weights of the elements of \( A_j \); and hence
\[ \Sigma \omega_i - C_j I = m_j 2^{k-2}, \]

but also
\[ \Sigma \omega_i - C_j I = \frac{1}{2} \Sigma \omega_i - n_j 2^{k-2} = \left( n - n_j \right) 2^{k-2}. \]

**Corollary:** With the notation just introduced \( n_j = n - m_j \); that is \( n_j \) is the difference between the "length" of \( A \) and that of \( A_j \).

To introduce the next theorem, observe that 3) is equivalent to the statement: \( 2 C_j I - \Sigma \omega_i \) is a non-negative multiple of \( 2^{k-1} \), for all \( j \).
Theorem 3: \( W \) is admissible if and only if

4) \( \sum \omega_i \) is a multiple of \( 2^{K-1} \)

5) \( C_j W \) is a multiple of \( 2^{K-2} \), for \( j = 1, 2, \ldots, 2^{K-1} \)

6) \( 2C_j W \geq \sum \omega_i \) for \( j = 1, 2, \ldots, 2^{K-1} \).

Moreover, if 4) - 6) are satisfied and we set \( C_j W = a_j 2^{K-2} \), \( \sum \omega_i = n \cdot 2^{K-1} \), then \( N = \text{Ln}_j \) is the modular and \( W \) the weight vector of a code \( L(n, K) \).

Notice that 5) and 6) do not imply 4), as the following example shows:

\[
W = \begin{bmatrix}
1 \\
2 \\
3 \\
4
\end{bmatrix}, \quad K = 3.
\]

Similarly

\[
W = \begin{bmatrix}
1 \\
2 \\
3 \\
4
\end{bmatrix}, \quad K = 3.
\]

shows that 4) and 5) do not imply 6). And finally 4) and 6) do not imply 5) because of the example

\[
W = \begin{bmatrix}
1 \\
2 \\
3 \\
4
\end{bmatrix}, \quad K = 3.
\]
The necessity of 4) - 6) is an immediate consequence of 1) and 3). Conversely, 4) and 5) enable us to write \( C_i W = \gamma_i 2^{n-2} + \frac{1}{2} \sum \omega_j \) and 6) to conclude \( n_2 \geq n \). Hence 4) - 6) imply 3). The "Moreover" part of the theorem is now clear.

2. Further modifications of Theorem 1.

It is natural to check whether the 2 \( ^\omega \) conditions of, say, Theorem 2 are independent and thus all have to be checked. Unfortunately the answer is yes: the second example above fails to satisfy Theorem 2 only for \( j = \omega \) (and fails to satisfy Theorem 3 only for condition 6) with \( j = \omega \) ). Convenient permutations allow us to modify this example so that it fails Theorem 2 for any single given value of \( j \).

In this context, the following result may be of interest:

Proposition 1: Given \( W \), let \( W' \) be the \( (2^{n-1}) \times 1 \) matrix consisting of the first \( 2^{n-1} \) rows of \( W \). Then \( W \) is admissible if and only if

a) \( W' \) is admissible

b) \( \sum \omega_j \) (over \( W \) ) is a multiple of \( 2^{n-2} \)

c) \( C_i W \) is a multiple of \( 2^{n-2} \) for \( 2^{n-2} < j < 2^n \).

The proof is an immediate consequence of Theorem 3 and of the dependency of \( C \) on \( k \) as described in [1].

Let us extend the use of a "prime" to differentiate the symbols referring to the subcode generated by the first \( k \) generators. If \( \tilde{C} \) denotes the matrix obtained from \( C \) by substituting 1 for 0 and 0 for 1, then we know from [1] that
Let $C'$ denote the matrix obtained from $C$ by substituting 1 for 0 and -1 for 1. Then clearly

$$C' = \begin{pmatrix} C' & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \end{pmatrix}$$

We set

$$H = \begin{pmatrix} \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \end{pmatrix}$$
\[ \tilde{W} = \frac{\mu_0}{W} \quad \mu_0 = 0 \]

\[ \tilde{N} = \frac{n_0}{N} \quad n_0 = n = -\sum_{i=1}^{k} \eta_i \]

\[ R = \begin{bmatrix} \mu_0 \\ \mu_{i-1} \\ \vdots \\ \mu_{k-1} \\ \mu_{k-1} \end{bmatrix} \quad S = \begin{bmatrix} \mu_0 \\ \mu_{k-1} \\ \vdots \\ \mu_{k-1} \end{bmatrix} \]

\[ T = \begin{bmatrix} \eta_0 \\ \eta_1 \\ \vdots \\ \eta_{k-1} \end{bmatrix} \quad Y = \begin{bmatrix} \eta_{k-1} \\ \vdots \\ \eta_{k-1} \end{bmatrix} \]

Then

\[ \tilde{W} = \begin{bmatrix} R \\ S \end{bmatrix} \quad \tilde{W}' = R \quad \tilde{N} = \begin{bmatrix} T \\ Y \end{bmatrix} \]

\[ H = \begin{bmatrix} H' & H' \\ H' & -H' \end{bmatrix} \]
Lemma 1: \( \widetilde{N}^1 = T + V \).

Observe that the generator matrix \( \tilde{G} \) has \( n_c \) columns representing the binary number \( 1 \leq i \leq 2^{k-1} - 1 \), and \( n_{k_{-1}} \) columns representing the number \( 2^{k-1} + i \), and that both types are identical except in the last row, which is the \( k \)-th generator. Hence, \( n_{i} = n_{i} + n_{k_{-1}} \).

Further,

\[
\begin{align*}
\sum_{i=1}^{2^{k-1}} n_{i} &= -\sum_{i=1}^{2^{k-1}} n_{i}' \\
&= -\sum_{i=1}^{2^{k-1}} (n_{i} + n_{k_{-1}}) \\
&= -\sum_{i=1}^{2^{k-1}} n_{i} - \sum_{i=2^{k-1}}^{2^{k-1}} n_{i} \\
&= n_{k_{-1}} - \sum_{i=1}^{2^{k-1}} n_{i} = n_{k_{-1}} + n_{0},
\end{align*}
\]

terminating the proof.

Lemma 2: Condition 3) in Theorem 2 is equivalent to each one of the following:

7) \( C^*W + 2^{k-1}N = 0 \):

8) \( H \tilde{W} + 2^{k-1}N = 0 \).

That 7) and 8) are equivalent is clear. To show that 3) and 7) are equivalent observe that \( C^* = J - 2C \). Thus, since \( JW = (\Sigma\omega_I)I \), 7) yields

\[
\Sigma\omega_I I - 2CW + 2^{k-1}N = 0
\]

which is, essentially, 3). This proves also the converse.
We can rewrite 8):

\[
\begin{bmatrix}
H' & H' \\
H' & -H'
\end{bmatrix}
\begin{bmatrix}
R \\
S
\end{bmatrix} + 2^{K-1}
\begin{bmatrix}
T \\
V
\end{bmatrix} = 0,
\]

obtaining

\[
\begin{cases}
\alpha) & H'(R+S) + 2^{K-1}T = 0 \\
\beta) & H'(R-S) + 2^{K-1}V = 0.
\end{cases}
\]

Adding \( \alpha \) and \( \beta \) yields

\[
H'R + 2^{K-2}(T+V) = 0
\]

\[
H'\tilde{R} + 2^{K-2}\tilde{N} = 0
\]

which is 8) for \( n-1 \). The matrix \( H \) is a Hadamard matrix (see, for example, [8]), and hence \( H' = 2^{-K}H \).

Thus \( \beta \) becomes:

\[
H'(S-R) = 2^{K-1}V
\]

or

\[
S - R = H'V.
\]

We have:

**Theorem 4:** \( W \) is admissible if and only if there is a matrix \( V \) whose elements are non-negative integers, such that:

a) \( W' \) is admissible

b) \( S-R = H'V \)

c) \( \tilde{N}' - V \) is non negative, except in the first row.
The "if" part has been shown above. To prove the "only if" part, assume that a) and b) are satisfied. Retracing the steps above we have

from a) \( H'(R - S) + \alpha K^{-1} \tilde{N}' = 0 \)

and from b) \( H'(R - S) + \alpha K^{-1} \tilde{V} = 0 \),

which is \( \beta \). Subtracting,

\[
H'(R - S) + \alpha K^{-1} (\tilde{N}' - \tilde{V}) = 0
\]

or
\[
H'(R - S) + \alpha K^{-1} (\tilde{N} - \tilde{V}) = 0,
\]

which is \( \gamma \) because of c). But \( \alpha \) and \( \beta \) give us \( \delta \) and hence \( \mathcal{W} \) is admissible by Theorem 2 and Lemma 2.

Notice that a) and b) do not imply c), as the following example shows.

Let
\[
\mathcal{W} = \begin{bmatrix}
7 \\
3 \\
3 \\
6 \\
3
\end{bmatrix}, \quad \mathcal{W}' = \begin{bmatrix}
7 \\
3 \\
3
\end{bmatrix}
\]

Theorem 2 shows that
\[
\mathcal{W}' = \begin{bmatrix}
7 \\
3 \\
4
\end{bmatrix}
\]

is admissible and that the corresponding modular vector is
\[
\tilde{N}' = \begin{bmatrix}
4 \\
0 \\
3
\end{bmatrix}
\]
By definition

\[
R = \begin{bmatrix} 0 \\ 7 \\ 3 \\ 4 \end{bmatrix} \quad \text{and} \quad s = \begin{bmatrix} 3 \\ 6 \\ 2 \\ 3 \end{bmatrix}.
\]

If we set

\[
V = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \end{bmatrix}
\]

then also b) is satisfied: \( S - R = H'V \). But c) is not:

\[
\bar{N} - V = \begin{bmatrix} -7 \\ 3 \\ -1 \\ 2 \end{bmatrix}.
\]

Theorem 4 has a natural intuitive interpretation which we shall illustrate by an example for \( K = 3 \). Suppose part a) of Theorem 4 is satisfied. That is, there exists a code \( A' = \{ x_1, x_2, x_3 \} \)

with weight vector \( W' = \begin{bmatrix} \omega_1 \\ \omega_2 \\ \omega_3 \end{bmatrix} \) and modular vector \( N' = \begin{bmatrix} \eta_1 \\ \eta_2 \\ \eta_3 \end{bmatrix} \). We wish
to determine whether \( W = \begin{bmatrix} w_1 \\ w_2 \\ w_3 \\ w_4 \\ w_5 \\ w_6 \\ w_7 \end{bmatrix} \) is admissible. The admissibility of \( W \),
given that \( W' \) is admissible, clearly implies that we can add a generator \( x_j \) to \( A \), satisfying four conditions:

i) the weight of \( x_j \) is \( w_j \),

ii) the weight of \( x_j = x_i + x_j \) is \( w_i \),

iii) the weight of \( x_i = x_i + x_j \) is \( w_i \),

and iv) the weight of \( x_j = x_i + x_k + x_l \) is \( w_j \).

Let \( \alpha_i^j (i \neq j, k, l) \) be the number of positions in which \( x_j \) has ones in common with only those generators \( x_i \), \( x_k \), \( x_l \) such that \( i = \sum x_i \). That is, \( x_j \) has \( \alpha_i^j \) ones in positions vacant in both \( x_i \), and \( x_k \), \( \alpha_k^j \) ones in positions common to \( x_i \) but not \( x_j \), \( \alpha_k^l \) ones in positions common to \( x_l \) but not \( x_j \), and \( \alpha_l^j \) ones in positions which contain ones in both \( x_i \), and \( x_k \); and this clearly exhausts \( x_j \). Recalling that \( \alpha_k^j = 0 \), we can translate the four conditions i) - iv) into equations:

\[
\begin{align*}
\alpha_1^j + \alpha_2^j + \alpha_3^j + \alpha_4^j + \alpha_5^j = w_j \\
\alpha_1^j + \alpha_2^j - \alpha_3^j + \alpha_4^j - \alpha_5^j = w_i \\
\alpha_1^j + \alpha_2^j + \alpha_3^j - \alpha_4^j - \alpha_5^j = w_i \\
\alpha_1^j + \alpha_2^j - \alpha_3^j - \alpha_4^j + \alpha_5^j = w_j \\
\end{align*}
\]

11.1
Collecting the $\mathcal{M}_i$'s and setting $V = \begin{bmatrix} \mathcal{N}_0 \\ \nu_1 \\ \mathcal{N}_2 \\ \nu_3 \end{bmatrix}$, we obtain

\[
\begin{bmatrix}
\mathcal{M}_\gamma - \mathcal{M}_0 \\
\mathcal{M}_z - \mathcal{M}_1 \\
\mathcal{M}_1 - \mathcal{M}_2 \\
\mathcal{M}_0 - \mathcal{M}_3
\end{bmatrix} = \begin{bmatrix}
1 & 1 & 1 & 1 \\
1 & -1 & 1 & -1 \\
1 & 1 & -1 & -1 \\
1 & -1 & -1 & 1
\end{bmatrix} V.
\]

The left-hand member is $S - \mathcal{R}$, and the matrix of coefficients of $V$ is $H'$, so this equation is precisely part b) of Theorem 4. The requirement in Theorem 4 that $V$ be of non-negative integers follows here directly from the definition of the $\mathcal{N}_i$. Moreover, since each $\mathcal{M}_i$ counts positions from among those counted by the corresponding $\mathcal{N}_i$, it is clear that for $i > 0$, $\mathcal{N}_i \leq \mathcal{N}_i$, which is part c) of Theorem 4. It can be seen quite easily that these conditions on the $\mathcal{N}_i$ are both necessary and sufficient for the admissibility of $\mathcal{W}$. They can be shown by induction to hold for any $\kappa$. In fact, it was this elementary approach of comparing a new generator with each previous generator that first suggested Theorem 4 to us.
3. Equivalence of weight vectors.

Because of the numeration involved in associating \( W \) to a code \( A \), different weight vectors correspond to one and the same code. On the other hand if \( W \) is the weight vector of \( A \) (with a given numeration), \( W \) is also the weight vector of any code equivalent to \( A \). We have thus a "many-to-many" correspondence between admissible vectors \( W \) and codes.

To obtain a one-to-one correspondence we consider only equivalence classes of codes and equivalence classes of vectors, defined as follows. Two admissible vectors \( W, W' \) are called equivalent if they are weight vectors of equivalent codes. The remark above enables us immediately to say also that \( W \) and \( W' \) are equivalent if and only if they are weight vectors of one and the same code \( A \) (for two numerations of its elements).

Proposition 2  \( W_1 = [\omega_{11}] \) and \( W_2 = [\omega_{21}] \) are equivalent if and only if there is a permutation \( \sigma \) of \( \{1, 2, \ldots, 2^n - 1\} \) such that \( \omega_{1k} = \omega_{2\sigma(k)} \) and such that if \( \sigma(2^j) = \sum_{k=0}^{2^n-1} a_{i,k} 2^k \), then

\[
\sigma(\Xi a_i 2^j) = \sum_{k=0}^{2^n-1} (\Xi a_{i,k} 2^k),
\]

where \( \Xi \) denotes sum modulo 2. It is enough to prove that these properties characterize the changes in allowable numerations of the elements of a code \( A \). Let then \( x_1, x_2, \ldots \), \( \tilde{x}_1, \tilde{x}_2, \ldots \) denote the elements of \( A \), in two different orders, but such that

\[
X_{\tilde{x}_j} x^j = \sum_j x_i x^i, \quad X_{x_i} x^j = \sum_j x_i x^i.
\]

For some permutation \( \sigma \) we have \( \tilde{x}_i = x_{\sigma(i)} \).

In particular

\[
X_{\tilde{x}_j} x^j = x_{\sigma(2^j)}, \quad x_{\tilde{x}_j} x^j = \sum_{k=0}^{2^n-1} a_{\tilde{x},k} x^k.
\]

\[
X_{\tilde{x}_j} x_{\tilde{x}_j} x^j = X_{\tilde{x}_j} x^j = \sum_{k=0}^{2^n-1} a_{\tilde{x},k} x^k, \quad x_{\tilde{x}_j} x^j = \sum_{k=0}^{2^n-1} x_{\tilde{x},k} x^k, \quad x_{\tilde{x}_j} x_{\tilde{x}_j} = \sum_{k=0}^{2^n-1} x_{\tilde{x},k} x^k.
\]
Conversely, let \( x_1, x_2, \ldots \) be an allowable numeration of the elements of \( A \), and let \( \sigma \) have the properties of the proposition. Set \( \Phi_i = x_{\sigma(i)} \).

To prove that \( \Phi_1, \Phi_2, \ldots, \Phi_n \) are independent, assume \( \sum \frac{1}{i} a_{i} = 0 \). Then

\[
\check{0} = x_{\sigma(i)} \frac{1}{i} a_{i} = \frac{1}{j} \sum_{j} x_{\sigma(i)} a_{j} \check{1} = \frac{1}{j} \sum_{j} x_{\sigma(i)} a_{j} \check{1} = \frac{1}{j} \sum_{j} x_{\sigma(i)} \check{1} = \frac{1}{j} \check{1}.
\]

Since \( x_1, x_2, \ldots, x_n \) are independent, \( \sum_{j} a_{j} = \check{0} \) for each \( \check{1} \), and

\[\check{1} = \check{1} \quad \text{which is not possible since} \quad \check{1} \quad \text{is a permutation. Thus indeed the vectors} \quad \Phi_i \quad \text{are independent.}
\]

Moreover

\[
\check{1} = \frac{1}{j} \sum_{j} x_{\sigma(i)} \frac{1}{j} a_{j} = \frac{1}{j} \sum_{j} x_{\sigma(i)} a_{j} \check{1} = \frac{1}{j} \sum_{j} x_{\sigma(i)} \check{1} = \frac{1}{j} \check{1}.
\]

If we denote by \( T_\sigma \) the \( (x_i^j) \times (x_i^j) \) permutation matrix corresponding to the permutation \( \sigma \) of Prop. 2, we can write \( W_i = T_\sigma W_i \). The matrices \( T_\sigma \) so obtained have been denoted \( P_\sigma \) in [2]; our Prop. 2 can also be obtained from the definition of \( P_\sigma \). Moreover, in [2] it has been shown that to every \( \sigma \) there corresponds a \( \tau \), also with the properties of Prop. 2, such that

\[T_\sigma \check{1} = \check{1} T_\sigma.
\]

If then \( W_i = T_\sigma W_i \) and \( N = \check{1} W_i \), \( N_\sigma = \check{1} W_i \), we obtain

\[N_\sigma = \check{1} W_i = \check{1} T_\sigma \check{1} W_i = \check{1} \check{1} T_\sigma \check{1} W_i = T_\sigma \check{1} W_i.
\]

This establishes the

**Corollary [2]** Let \( A_1, A_2 \) be two codes, \( W_i, W_i \) and \( N_i, N_i \) their weight and modular vectors. Then the following propositions are equivalent:

a) \( A_1 \) and \( A_2 \) are equivalent codes;

b) There exists a permutation \( \sigma \) as in Prop. 2 such that \( W_2 = T_\sigma W_i \);

c) There exists a permutation \( \sigma \) as in Prop. 2 such that \( N_2 = T_\sigma N_i \).
From this one can easily deduce the following almost obvious result:

**Proposition 3.** Let \( N = [n_i] \) be a \((2^k-1) \times 1\) matrix whose elements are non-negative integers; then \( N \) is the modular vector of some code \( \Lambda(0, \lambda, \kappa) \) if and only if there exists a permutation \( \sigma \) as in Prop. 2 such that \( n_{e_i(\sigma i)} \neq 0 \) for \( i = 0, 1, \ldots, \kappa-1 \).

4. Some consequences of Theorems 1 to 4.

Given \( W = [\omega_c^k] \); let \( d, \omega_c^k \) be non-negative integers verifying

\[
 d = \min \omega_c^k, \quad \omega_c^k = \omega_c^k - d
\]

and set

\[
 D = W - dI = [d_i].
\]

In general only the case \( d = \min \omega_c^k \) will be of interest. However, we need establish the results below also for \( d < \min \omega_c^k \) so as to obtain more flexibility and, in particular, to be able to use induction arguments.

The relations 1') - 7') yield equivalent relations:

1') \( \sum d_i - d = (n - 2d) 2^k - 1 \).

2') the elements of \( C^*D + 2^{k-1}dI \) are all non-negative integers.

3') \( C_D = 2^{k-2}N + (Z d_i - d)I \).

4') \( \Sigma_d = d \) is a multiple of \( 2^{k-2} \).

5') \( C_d \) is a multiple of \( 2^{k-2} \) for \( j = 1, 2, \ldots, 2^{k-2} \).

6') \( 2C_d \geq Z d_i - d \) for \( j = 1, 2, \ldots, 2^{k-1} \).

7') \( C_d = dI + 2^{k-1}N = 0 \).

Relation 8') and Theorem 4 can also be rewritten in terms of \( d_i \) with very little change.

It may be interesting to point out the substitution of \( Z \omega_c^k \) with \( Z d_i - d \). We shall say that \((C, d)\) is admissible if and only if \( W = D + dI \) is admissible.
Proposition 4. Let $d_i \neq 0$ for at most two subscripts $i_1', i_2'$. Then $(D, d)$ is admissible if and only if $d + d_{i_1'} + d_{i_2'}, d - d_{i_1'} + d_{i_2'}, d + d_{i_1'} - d_{i_2'},$ and $d - d_{i_1'} - d_{i_2'}$ are non-negative multiples of $2^{k - r}$.

Without loss of generality we can assume $i_1' = 1, i_2' = 2$ by taking an equivalent weight vector. Then (see the definition of $C$) $C, D = d, C_1 D = d_1', C_2 D = d_2'$, and $C_3 D = 0$. Moreover all other $C_j D$ have one of these four values.

We can write $3')$ as

$$-d_i - d_{i_1'} + d_{i_2'} + \alpha C_j D = n_j 2^{k - r}.$$ 

Hence the proposition, which has the known

Corollary The only codes $A(n, k)$ with all elements of equal weight ($d_i = 0$ for all $i$) satisfy $d = \mathcal{L} 2^{k - r}, n = \mathcal{L} (2^{k - r}).$

Proposition 5 Let $k > 3$ and $d_i \neq 0$ only for $i_1', i_2', i_3'$. Then $(D, d)$ is admissible if and only if $d - d_{i_1'} + d_{i_2'} + d_{i_3'}, d + d_{i_1'} - d_{i_2'} + d_{i_3'}, d + d_{i_1'} - d_{i_2'} - d_{i_3'},$ and $d - d_{i_1'} - d_{i_2'} - d_{i_3'}$ are non-negative multiples of $2^{k - r}$.

We can reduce the general case to either of two special ones:

a) $i_1' = 1, i_2' = 2, i_3' = 3$; or b) $i_1' = 1, i_2' = 2, i_3' = 4$.

In case a), $C_1 D = d_1', C_2 D = d_2', C_3 D = d_3', C_4 D = 0$, and all other $C_j D$ have one of these values. Our result then follows as above from $3')$. In case b) we have $C_1 D = d_1', C_2 D = d_2', C_3 D = d_3', C_4 D = 0$; hence, again from $3')$, the conditions of the proposition are necessary; by a) we know already that they are sufficient.

The assumption $k > 3$ is required to insure the existence of $C_4$. Similar results can be obtained for increasing, but always small, number of non-zero $d_i$'s. They can all be considered as particular cases of $7')$.

The function $\Sigma d_i$ has some interesting properties. The first is a generalization of the Corollary to Prop. 4, which considered the case $\Sigma d_i = 0$.

Proposition 6 Let $A(n, k)$ be a code with weights $(b, d)$. Then, for
some integer \( \ell \), \( \eta = 2\sum j_i + 2^\ell (2^{K-1}) \) and \( d = \sum d_i + 2^{K-1} \). Moreover \( \ell \geq 0 \) if and only if \( \sum d_i = 2^{K-1} \).

From 1') we obtain \( d = \sum d_i + 2 \sum j_i \) and then from 1') \( \eta = 2d + \frac{\sum d_i - d}{2^{K-1}} = 2\sum d_i + (\sum j_i - 2^{K-1}) \). Solving the first relation for \( \sum d_i \) we obtain \( \sum d_i = d - \sum j_i \). Thus \( \sum d_i = 2^{K-1} \) is equivalent to \( \ell \geq 0 \). Since \( \eta - 2d = \ell \), we have also:

**Corollary** \( \eta \geq 2d \) if and only if \( \sum d_i \leq 2^{K-1} \).

The relation \( \sum d_i = 2^{K-1} \) restricts considerably the possible values of \( \sum d_i \).

**Proposition 7** If \( (D,j) \) is admissible and \( \sum d_i = 2^{K-1} \), then \( \sum d_i = 0 \) or \( \sum d_i = 2^r \) for some \( r \geq 0 \).

Assume \( \omega \leq \sum d_i \). Then, for some \( j \), \( \omega \leq j \sum d_i \). Since \( (D,j) \) is a multiple of \( 2^{K-2} \), \( \sum d_i \leq 2^{K-2} \). If the equality sign holds, we are through. Similarly if \( \omega \leq \sum d_i \). So assume \( \omega \leq 2^{K-2} \). We have then \( \omega \leq \sum d_i - C_j D \leq 2^{K-2} \). But the middle term is the sum of the \( j_i \)'s for the subgroup \( \mathcal{D}_j \). Using induction we have then

\[
\sum d_i - C_j D = \sum \frac{1}{r} \sum j_i \leq 2^{r-1} \sum j_i = \sum \frac{1}{r} \sum j_i
\]

To complete the proof, let \( K = 2 \). Then the proposition states \( \sum d_i = 0 \) or \( \sum d_i = 2 \) : a triviality. Relation 1') yields:

**Corollary 1**

\[
d \leq \left[ \frac{2^{K-1} - 2^{K-2}}{2^{K-1}} \right].
\]

This is an improvement on Plotkin's upper bound \( \left[ \frac{2^{K-1}}{2^{K-1}} \right] \); however both bounds agree "almost everywhere".

Because of Proposition 6 we obtain also:

**Corollary 2** If \( \sum d_i \leq 2^{K-1} \), then \( \eta \geq 2^{K-1} \).
Thus, if \( n < 2^{k'} \), the \( \delta \) of Prop. 6 is strictly negative:

**Corollary:** If \( n < 2^{k'} \), then \( d \leq \left\lfloor \frac{n-1}{2} \right\rfloor \).

That the values of \( \Sigma d_j \) given in Prop. 7 are actually taken (and then \( n \) and \( d \) are given by Prop. 8) is shown by the codes described by MacDonald [1] and McCluskey [1], among others.

It is possible to prove, in parallel to Prop. 7, that \( \Sigma d_j = 2^{k'-1} + \sum_{i=r}^{n-r} 2^z \)

for some \( r \leq n \), if \( 2^{k'-1} < \Sigma d_j < 2^{k'-1} + 2^{k'-2} \).

But this result does not seem interesting; the application of Prop. 6 in this case does not determine \( n \) and \( \Sigma d_j \); can, and often does, exceed \( 2^{k'-1} \) also for small values of \( n \).
References


<table>
<thead>
<tr>
<th>Parke Mathematical Laboratories, Inc. Carlisle, Massachusetts</th>
<th>UNCLASSIFIED</th>
<th>Parke Mathematical Laboratories, Inc. Carlisle, Massachusetts</th>
<th>UNCLASSIFIED</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>On The Weights Of The Elements Of Binary Group Codes</strong></td>
<td>1. Information Theory</td>
<td><strong>On The Weights Of The Elements Of Binary Group Codes</strong></td>
<td>1. Information Theory</td>
</tr>
<tr>
<td>by L. Calabi and E. Myrvaauges</td>
<td>2. Linear Algebra</td>
<td>by L. Calabi and E. Myrvaauges</td>
<td>2. Linear Algebra</td>
</tr>
<tr>
<td>(Scientific Report No. 5; AFCRL-63-95) (Contract AF 19(604)-7493)</td>
<td>II. Air Force Cambridge Research Laboratories, Office of Aerospace Research</td>
<td>(Scientific Report No. 5; AFCRL-63-95) (Contract AF 19(604)-7493)</td>
<td>II. Air Force Cambridge Research Laboratories, Office of Aerospace Research</td>
</tr>
</tbody>
</table>

Various necessary and sufficient conditions are given for the existence of codes with pre-assigned weights. Some properties of the weight distribution are deduced.