# A Theorem on the Distribution of Weights in a Systematic Code†

By JESSIE MACWILLIAMS

(Manuscript received September 4, 1962)

*A systematic code of word length n is a subspace of the vector space of all possible rows of n symbols chosen from a finite field. The weight of a vector is the number of its nonzero coordinates; clearly any given code contains a certain finite number of vectors of each weight from zero to n. This set of integers is called the spectrum of the code, and very little is known about it, although it appears to be important both mathematically and as a practical means of evaluating the error-detecting properties of the code.*

*In this paper it is shown that the spectrum of a systematic code determines uniquely the spectrum of its dual code (the orthogonal vector space). In fact the two sets of integers are related by a system of linear equations. Consequently there is a set of conditions which must be satisfied by the weights which actually occur in a systematic code. If there is enough other information about the code, it is possible to use this result to calculate its spectrum.*

In most systems of error correction by binary or multiple level codes the minimum distance between two code words is an important parameter. (The distance between two code words is the number of coordinate places in which they differ.) Much attention has been given to devising codes which have an assigned minimum distance.

The weight of a code word is its distance from the origin. The distance between two code words is the weight of the vector obtained by subtracting one from the other, coordinate by coordinate. If the code words form a vector space, this vector is itself a member of the code. Such codes are called systematic codes. The set of integers specifying the weight of each code word is then exactly the same collection of numbers as the set of integers specifying the distance between each pair of code words.

† This paper formed part of a thesis presented to the Department of Mathematics, Harvard University, in partial fulfillment of the requirements for the degree of Doctor of Philosophy.

Thus it is customary to talk about weight properties rather than distance properties of systematic codes.

In many cases, practically all that is known explicitly about the distribution of weights in a code is that the weight has a certain minimum value. Recent studies have shown that it would be useful (e.g., in the study of real life channels) to have more information. We would like to be able to answer questions of the following sort:

*i.* Given a method (implemented or theoretical) for constructing a systematic code, how many elements of each weight will be obtained? (It is a safe assumption that nobody will want to write out the code vectors and count them.)

*ii.* Given a set, $u_1, u_2, \cdots, u_s$, of positive integers, is it possible to construct a systematic code with elements of these weights only?

In theory there exists a method of answering these questions.[1,2,3] Unfortunately this method is quite difficult to apply. The purpose of this paper is to give a different method which is in some ways more useful.

We show that the spectrum of a systematic code determines uniquely the spectrum of the dual code (the orthogonal vector space). In fact, the two sets of integers are related by a system of linear equations. Our main theorem shows how to obtain this system of equations.

In Section I we give definitions and statements of the main theorem and of some corollaries. Section II contains proofs of these theorems. Section III describes how the results of Section I may be applied.

## I. DEFINITIONS, NOTATION AND A STATEMENT OF THE MAIN THEOREM

Let $F$ be a finite field of $q$ elements; $q$ is a prime power. Let $F^n$ denote the direct sum of $n$ copies of $F$. $F^n$ is the set of all possible row vectors of length $n$, in which each coordinate is an element of $F$. Addition of two vectors is defined coordinate by coordinate, under the rules prevailing in $F$.

$F^n$ is a vector space of dimension $n$ over $F$. Choose a basis consisting of the $n$ vectors

$$\epsilon_1 = (1, 0, 0, \cdots, 0)$$
$$\epsilon_2 = (0, 1, 0, \cdots, 0)$$
$$\cdots\cdots\cdots\cdots\cdots$$
$$\epsilon_n = (0, 0, 0, \cdots, 1).$$

An element $u$ of $F^n$ is then expressed uniquely as

$$u = \sum_{i=1}^{n} u_i \epsilon_i, \qquad u_i \epsilon F.$$

We write $u = (u_1, u_2, \cdots, u_n)$.

The weight of $u$ is defined to be the number of $u_i$ which actually appear in this sum — i.e., the number of nonzero coordinates in the vector $u$.

An alphabet is any subspace of $F^n$; a vector belonging to the alphabet $\mathfrak{A}$ is called a letter of $\mathfrak{A}$. It may happen that every letter of $\mathfrak{A}$ has zero as the $j$th coordinate — this case is not excluded.

The scalar product of two vectors,

$$u = \sum_{i=1}^{n} u_i \epsilon_i, \quad v = \sum_{i=1}^{n} v_i \epsilon_i, \qquad u_i, v_i \epsilon F,$$

is $u*v = \sum_{i=1}^{n} u_i v_i$, where the multiplication and addition are carried out in $F$. If $F$ is the field of two elements 0, 1, for example, the scalar product of $(1, 1, 0)$ with itself is $1 \cdot 1 + 1 \cdot 1 = 0$.

Two vectors $u$, $v$ are orthogonal if their scalar product is zero. In the example above, $(1, 1, 0)$ is orthogonal to itself.

The orthogonal complement of an alphabet $\mathfrak{A}$ is the set of all vectors of $F^n$ which are orthogonal to every vector of $\mathfrak{A}$. It is clear that these vectors also form an alphabet, say $\mathfrak{B}$, which is called the dual alphabet of $\mathfrak{A}$. If $k$ is the dimension of $\mathfrak{A}$, the dimension of $\mathfrak{B}$ is $m = n - k$.

The main result of this paper is as follows (the proof is given in Section II):

Let $\mathfrak{A}$ be an alphabet of dimension $k$, and $\mathfrak{B}$ the dual alphabet of dimension $m$. Let $A_i$, $B_i$ denote the number of letters of weight $i$ in $\mathfrak{A}$, $\mathfrak{B}$ respectively. Of course, $A_0 = B_0 = 1$. Set $\gamma = q - 1$. Let $z$ be an indeterminate.

*Theorem 1: The quantities defined above are related by the equation*

$$\sum_{i=0}^{n} A_i (1 + \gamma z)^{n-i} (1 - z)^i = q^k \sum_{i=0}^{n} B_i z^i.$$

*Remarks:*

*i.* The formula above is symmetric in the sense that, setting $(1 - z)/(1 + \gamma z) = \hat{z}$, we obtain by straightforward algebra

$$\sum_{i=0}^{n} B_i (1 + \gamma \hat{z})^{n-i} (1 - \hat{z})^i = q^m \sum_{i=0}^{n} A_i \hat{z}^i.$$

*ii.* Theorem 1 is a statement about equivalent classes;[3,4] it is still true if $\mathfrak{A}$, $\mathfrak{B}$ are replaced by equivalent alphabets.

An alphabet $\mathfrak{A}$ is said to be decomposable,[3,4] with respect to the basis

$\epsilon_1, \epsilon_2, \cdots, \epsilon_n$ of $F^n$, if it is the direct sum of two alphabets $\mathfrak{A}_1, \mathfrak{A}_2$, where $\mathfrak{A}_1$ contains $n$ columns of zeros and $\mathfrak{A}_2$ occupies these columns only. For example, the alphabet

$$\begin{matrix} 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{matrix}$$

is decomposable, with

$$\mathfrak{A}_1 = \begin{matrix} 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{matrix} \qquad \mathfrak{A}_2 = \begin{matrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1. \end{matrix}$$

In general, $\mathfrak{A}_1$ is a $k_1$-dimensional alphabet in $F^{n_1}$, and $\mathfrak{A}_2$ a $k_2$-dimensional alphabet in $F^{n_2}$, with $n_1 + n_2 = n$, $k_1 + k_2 = k$, $k_1 \leqq n_1$, $k_2 \leqq n_2$.

The dual alphabet of a decomposable alphabet is also decomposable; in fact $\mathfrak{B} = \mathfrak{B}_1 + \mathfrak{B}_2$, where $\mathfrak{B}_i$ is the dual alphabet of $\mathfrak{A}_i$ in $F^{n_i}$, $i = 1, 2$. (The example above is self-dual.)

*Corollary 1.1:* If $\mathfrak{A}$ is decomposable, say $\mathfrak{A} = \mathfrak{A}_1 + \mathfrak{A}_2$, the equation

$$\sum_{i=0}^{n} A_i(1 + \gamma z)^{n-i}(1 - z)^i = q^k \sum B_i z^i$$

is reducible in the obvious sense; the factors are the equations pertaining to $\mathfrak{A}_i$, $\mathfrak{B}_i$ in $F^{n_i}$, $i = 1, 2$.

For the example above we have

$$[(1 + z)^4 + (1 - z)^2]^2 = 2^2(1 + z^2)^2.$$

*Corollary 1.2:* A necessary condition for the existence of an alphabet containing letters of weights $w_i$, $i = 1, 2, \cdots, s$, and no other, is that there exists a set of integers $\alpha_i$, $i = 1, 2, \cdots, s$, such that the expression

$$(1 + \gamma z)^n + \gamma \sum_{j=1}^{s} \alpha_i(1 + \gamma z)^{n-w_i}(1 - z)^{w_i},$$

when expanded in powers of $z$, takes the form

$$q^k + \gamma q^k \sum_{i=1}^{n} \beta_i z^i,$$

where the $\beta_i$ are positive integers.

Unfortunately, this condition is not sufficient. For example,

$$(1 + z)^8 + 7(1 + z)^6(1 - z)^2 + 7(1 + z)^2(1 - z)^6 + (1 - z)^8 = 2^4(1 + 7z^2 + 7z^6 + z^8),$$

but it is not possible to construct a binary alphabet containing 7 letters of weight 2 and no letters of weight 4.

If $A_1 = A_2 = \cdots = A_{2j} = 0$, every vector of weight $\leqq j$ in $F^n$ appears as a coset leader for $\mathfrak{A}$, and conversely. Another way of saying this is that, for all pairs of distinct letters $a$, $a'$, of $\mathfrak{A}$ and any $i \leqq j$, the set of vectors at distance $i$ from $a$ is disjoint from the set of vectors at distance $i$ from $a'$. In this case we can enumerate these vectors by weights as follows:

Let $f_{s,i}$ denote the number of vectors of weight $s$ in $F^n$ which are at distance $i$ from some letter of $\mathfrak{A}$. Write

$$(1 + \gamma z)^{n-i}(1 - z)^i = \sum_{i=0}^{n} \Psi(i, j) z^j$$

*Corollary 1.3:* If $\mathfrak{A}$ contains no letter of weight $< 2j + 1$, then

$$\sum_{s=1}^{n} f_{s,j} x^s = \sum_{i=0}^{n} B_i \Psi(i, j)(1 + \gamma x)^{n-i}(1 - x)^i.$$

The proofs of corollaries 1.1 to 1.3 are given in Section II.

## II. PROOFS

If $\mathfrak{A}$ is an alphabet of $F^n$ and $\mathfrak{B}$ the orthogonal complement of $\mathfrak{A}$, the weights of the letters of $\mathfrak{B}$ are, of course, uniquely determined by the letters of $A$. However, a much stronger statement can be made: the set of integers specifying the number of letters of each weight in $\mathfrak{B}$ is related by a system of linear equations to the set of integers similarly defined for $\mathfrak{A}$. This section will consist of proofs of this statement and of some of its consequences.

Two proofs are given. The first is short and easy; the second is longer and more sophisticated. However, it incidentally produces a more general result and gives some insight into what is going on.

We make the following conventions for notation: $\mathfrak{A}$ shall be a $k$-dimensional alphabet in $F^n$; $\mathfrak{B}$ shall be the orthogonal complement of $\mathfrak{A}$ of dimension $m = n - k$; $\gamma$ shall denote the quantity $q - 1$. $A_i$, $B_i$ denote the number of letters of weight $i$ in $\mathfrak{A}$, $\mathfrak{B}$ respectively. The binomial coefficient $\binom{r}{s}$ is understood to be zero if $s > r$.

Let $\epsilon_1, \epsilon_2, \cdots, \epsilon_n$ be the usual basis of $F^n$. Let $s = (s_1, s_2, \cdots, s_\nu)$ be a set of $\nu$ different indices, $1 \leqq s_i \leqq n$, and let $t = (t_1, t_2, \cdots, t_{n-\nu})$ be the complementary set of indices. Denote by $F_s^\nu$, $F_t^{n-\nu}$ the spaces generated by $\epsilon_{s_1}, \cdots, \epsilon_{s_\nu}$ and $\epsilon_{t_1}, \cdots, \epsilon_{t_{n-\nu}}$. Clearly, $F_s^\nu$, $F_t^{n-\nu}$ are orthogonal complements in $F^n$. Let $| H |$ stand for the number of vectors in a space $H$.

*Lemma 2.0:*

$$| \mathfrak{A} \cap F_t^{n-\nu} | = q^{k-\nu} | \mathfrak{B} \cap F_s^{\nu} |.$$

*Proof:* The orthogonal complement of $\mathfrak{A} \cap F_t^{n-\nu}$ is the smallest space containing $\mathfrak{B}$ and $F_s^{\nu}$. This is the lattice theoretic union of $\mathfrak{B}$ and $F_s^{\nu}$, which we write $\mathfrak{B} \cup F_s^{\nu}$. Then

$$| \mathfrak{B} \cup F_s^{\nu} | \cdot | \mathfrak{A} \cap F_t^{n-\nu} | = q^n = q^{m+k}.$$

The number of vectors in $\mathfrak{B} \cup F_s^{\nu}$ is $q^m q^{\nu} / | \mathfrak{B} \cap F_s^{\nu} |$.
Hence

$$q^{m+\nu} | \mathfrak{A} \cap F_t^{n-\nu} | = q^{m+k} | \mathfrak{B} \cap F_s^{\nu} |$$

or

$$| \mathfrak{A} \cap F_t^{n-\nu} | = q^{k-\nu} | \mathfrak{B} \cap F_s^{\nu} |.$$

Denote by $\{(\epsilon_{s_1}, \cdots, \epsilon_{s_\nu}), a\}$ a pair consisting of $\nu$ basis vectors of $F^n$ and a vector $a$ of $\mathfrak{A}$ which is orthogonal to each of $\epsilon_{s_1}, \cdots, \epsilon_{s_\nu}$.

*Lemma 2.1:*

*i. For a fixed set of indices $s_1, \cdots, s_\nu$ the number of pairs*

$$\{(\epsilon_{s_1}, \cdots, \epsilon_{s_\nu}), a\} \quad \textit{is} \quad | \mathfrak{A} \cap F_t^{n-\nu} |.$$

*ii. The total number of such pairs for all choices of $\nu$ distinct basis vectors is* $\sum_{i=0}^{n} A_i \binom{n-i}{\nu}$.

*Proof:*

*i.* $F_t^{n-\nu}$ consists of exactly those vectors of $F^n$ which are orthogonal to $\epsilon_{s_1}, \cdots, \epsilon_{s_\nu}$; hence $\mathfrak{A} \cap F_t^{n-\nu}$ consists of exactly those vectors of $\mathfrak{A}$ which are orthogonal to $\epsilon_{s_1}, \cdots, \epsilon_{s_\nu}$.

*ii.* If $a \in \mathfrak{A}$ is of weight $i$, then $a$ is orthogonal to $n - i$ of the vectors $\epsilon_1, \cdots, \epsilon_n$. A set of $\nu$ vectors may be chosen from these $n - i$ in $\binom{n-i}{\nu}$ ways. Hence the total number of pairs

$$\{(\epsilon_{s_1}, \cdots, \epsilon_{s_\nu}), \quad a\} \text{ is } \sum_{i=0}^{n} A_i \binom{n-i}{\nu}.$$

Let $\sum_s$ indicate summation over all possible choices of $\nu$ indices $s_1, \cdots, s_\nu$; similarly, $\sum_t$ denotes summation over all the complementary sets $t_1, \cdots, t_{n-\nu}$. Lemma 2.1 is equivalent to

$$\sum_t | \mathfrak{A} \cap F_t^{n-\nu} | = \sum_{i=0}^{n} A_i \binom{n-i}{\nu}.$$

Replace $\mathfrak{A}$ by $\mathfrak{B}$, $\nu$ by $n - \nu$ and $s$ by $t$. The same argument then gives

$$\sum_s |\mathfrak{B} \cap F_s^{\nu}| = \sum_{i=0}^{n} B_i \binom{n-i}{n-\nu}.$$

*Lemma 2.2*

$$\sum_{i=0}^{n} A_i \binom{n-i}{\nu} = q^{k-\nu} \sum_{i=0}^{n} B_i \binom{n-i}{n-\nu}.$$

*Proof:* For a fixed set $s$ (which determines, of course, a fixed set $t$) we have by 2.0

$$|\mathfrak{A} \cap F_t^{n-\nu}| = q^{k-\nu} |\mathfrak{B} \cap F_s^{\nu}|.$$

Thus

$$\sum_t |\mathfrak{A} \cap F_t^{n-\nu}| = q^{k-\nu} \sum_s |\mathfrak{B} \cap F_s^{\nu}|,$$

which, by 2.1 is the same thing as

$$\sum_{i=0}^{n} A_i \binom{n-i}{\nu} = q^{k-\nu} \sum_{i=0}^{n} B_i \binom{n-i}{n-\nu}.$$

The equation of 2.2 holds for $\nu = 0, 1, \cdots, n-1$. This is, in fact, one form of the promised set of linear equations between the quantities $A_i$, $B_i$.

We now give the second proof.

Let $\mathfrak{G}$ be a finite Abelian group. A character $\chi$ of $\mathfrak{G}$ is a homomorphism of $\mathfrak{G}$ into the multiplicative group of complex numbers of absolute value 1. The characters of $\mathfrak{G}$ form a group $\mathfrak{G}^*$ which is isomorphic to $\mathfrak{G}$, there being in general no canonical isomorphism.†

If $\mathfrak{A}$ is a subgroup of $\mathfrak{G}$, the characters such that $\chi(a) = 1$ for all $a$ of $\mathfrak{A}$ form a subgroup $\mathfrak{B}^*$ of $\mathfrak{G}^*$. $\mathfrak{B}^*$ is precisely the character group of $\mathfrak{G}$ *mod* $\mathfrak{A}$.

Suppose now that $\mathfrak{G}$ is the additive group of a finite field. $\mathfrak{G}^*$ is just a multiplicative copy of $\mathfrak{G}$, and the characters can be labeled by the elements of $\mathfrak{G}$ in a symmetric way; that is, if $r$, $s$, $\cdots$ are elements of $\mathfrak{G}$ we have

$$\chi_r(s) = \chi_s(r) = \chi(r, s).$$

If $\mathfrak{G}$ is the additive group of a prime field of order $q$, we take $r$, $s$ etc.

† For prime fields, the proof can be given without mentioning the word character. The presentation here is an uneasy compromise with conscience — we wish to indicate possible extensions to nonprime fields without doing too much work.

to be the integers *mod* $q$, and set $\chi(r, s) = \zeta^{rs}$ where $\zeta$ is a primitive $q$th root of unity.

We have from the general theory of characters

$$\chi(r, 0) = \chi(0, s) = 1,$$

$$\sum_{r=1}^{\gamma} \chi(r, s) = -1 \qquad \text{if } s \not\equiv 0.$$

Let $\epsilon_1, \epsilon_2, \cdots, \epsilon_n$ be the fixed basis of $F^n$, and $u = (u_1, u_2, \cdots, u_n)$ the coordinates of a vector of $F^n$ with respect to this basis. The character group of $F^n$ is, of course, a multiplicative copy of $F^n$. We label the characters by elements of $F^n$ as follows:

$$\psi_u(v) = \prod_{i=1}^{n} \chi(u_i, v_i) = \psi_v(u) = \psi(u, v).$$

Let $\mathfrak{A}$ be a subspace of $F^n$. The characters such that $\psi_b(a) = 1$ for all $a$ of $\mathfrak{A}$ form a subgroup $\mathfrak{B}^*$ of the character group. $\mathfrak{B}^*$ is exactly the character group of $F^n$ *mod* $\mathfrak{A}$. The elements $b$ which label these characters form a subspace $\mathfrak{B}$ of $F^n$, isomorphic to $F^n$ *mod* $\mathfrak{A}$. In our notation, the equation $\psi(a, b) = 1$ holds for all $a$ of $\mathfrak{A}$ and all $b$ of $\mathfrak{B}$, and given either $\mathfrak{A}$ or $\mathfrak{B}$, the other is uniquely† determined by this condition.

*Lemma 2.3: Let $\mathfrak{A}$, $\mathfrak{B}$ be related as above. Then*

*i.* $$\sum_{a \in \mathfrak{A}} \psi(v, a) = q^k \text{ if } v \in \mathfrak{B}.$$

*ii.* $$\sum_{a \in \mathfrak{A}} \psi(v, a) = 0 \text{ if } v \notin \mathfrak{B}.$$

*Proof:* Part *i* is obvious, since by definition $\psi(v, a) = 1$ if $v \in B$. For *ii* we observe that for $a \in \mathfrak{A}$, $\psi(v, a) = \psi_a(v)$ is a character of $F^n$ *mod* $\mathfrak{B}$. If $\bar{v}$ denotes a coset of $F^n$ *mod* $\mathfrak{B}$, $\sum_{a \in \mathfrak{A}} \psi_a(\bar{v}) = 0$ for $\bar{v} \not\equiv \mathfrak{B}$. Now $\psi_a(v) = \psi_a(\bar{v})$ for any $v$ in $\bar{v}$; hence

$$\sum_{a \in \mathfrak{A}} \psi(v, a) = \sum_{a \in \mathfrak{A}} \psi_a(\bar{v}) = 0 \quad \text{if} \quad v \notin \mathfrak{B}.$$

*Lemma 2.4: If $F$ is a prime field, then $\mathfrak{A}$, $\mathfrak{B}$ are related as in* 2.3 *if and only if they are orthogonal complements.*

*Proof:* $\psi(a, b) = \zeta^{\Sigma a_i b_i}$ where $\zeta$ is a primitive $q$th root of unity. Hence $\psi(a, b) = 1$ implies that $a$ is orthogonal to $b$. Since $\mathfrak{A}$ is isomorphic to $F^n$ *mod* $\mathfrak{B}$ the dimensions of $\mathfrak{A}$, $\mathfrak{B}$ add up to $n$. Thus $\mathfrak{B}$ is the orthogonal complement of $\mathfrak{A}$.

---

† That is, if $F$ is a prime field. Otherwise we must fix the basis of $F$ over its prime field before we claim uniqueness.

Let $f(i, s)$ denote a function of the integers $i$, $s$ with values in a ring $R$. The values of $f(i, s)$ may be added and multiplied, and these operations obey the two distributive laws. $f(i, v_i)$ denotes the same function of $i$ and the $i$th coordinate of $v$.

*Lemma 2.5:*

$$\sum_{v \in F^n} \prod_{i=1}^{n} f(i, v_i) = \prod_{i=1}^{n} \sum_{r=0}^{\gamma} f(i, r).$$

*Proof:* If $n = 1$ the statement is

$$\sum_{s=0}^{\gamma} f(1, s) = \sum_{r=0}^{\gamma} f(1, r),$$

which is obvious. Assume the truth of the lemma for $F^{n-1}$.

Let $F_r{}^n$, $0 \leqq r \leqq \gamma$, denote the set of vectors of $F^n$ which have last coordinate $r$. Clearly the $F_r{}^n$ are a partition of $F^n$. Then

$$\begin{aligned}
\sum_{v \in F^n} \prod_{i=1}^{n} f(i, v_i) &= \sum_{r=0}^{\gamma} \sum_{v \in F_r{}^n} \left[ \prod_{i=1}^{n-1} f(i, v_i) f(n, r) \right] \\
&= \sum_{r=0}^{\gamma} f(n, r) \sum_{v \in F^{n-1}} \prod_{i=1}^{n-1} f(i, v_i) \\
&= \sum_{r=0}^{\gamma} f(n, r) \prod_{i=1}^{n-1} \sum_{r=0}^{\gamma} f(i, r) \quad \text{(by induction)} \\
&= \prod_{i=1}^{n} \sum_{r=0}^{\gamma} f(i, r).
\end{aligned}$$

Let $z^{(r)}$ be a set of (commuting) indeterminates, $r = 0, 1, \cdots, \gamma$. To each vector $v = (v_1, v_2, \cdots, v_n)$ of $F^n$ associate a monomial $\prod_{i=1}^{n} z^{(v_i)}$. The monomial associated with $v$ describes how many times each field element appears as a component of $v$. Let $R$ be the ring of polynomials in $z^{(0)}, z^{(1)}, \cdots, z^{(\gamma)}$ over the complex numbers. Let $u = (u_1, u_2, \cdots, u_n)$ be a fixed vector of $F^n$.

*Lemma 2.6:*

$$\sum_{v \in F^n} \psi(u, v) z^{(v_1)} z^{(v_2)} \cdots z^{(v_n)} = \prod_{j=1}^{n} \sum_{r=0}^{\gamma} \chi(u_j, r) z^{(r)}.$$

*Proof:* Set $f(j, v_j) = \chi(u_j, v_m) z^{(v_j)}$, which is in $R$. Then

$$\psi(u, v) z^{(v_1)} z^{(v_2)} \cdots z^{(v_n)} = \prod_{j=1}^{n} f(j, v_j).$$

By 2.5,

$$\sum_{v \in F^n} \psi(u, v) z^{(v_1)} z^{(v_2)} \cdots z^{(v_n)} = \prod_{j=1}^{n} \sum_{r=0}^{\gamma} f(j, r)$$

$$= \prod_{j=1}^{n} \sum_{r=0}^{\gamma} \chi(u_j, r) z^{(r)}.$$

*Lemma 2.7: Let* $\mathfrak{A}$, $\mathfrak{B}$ *be orthogonal complements in* $F^n$, *as usual. Then*

$$\sum_{u \in \mathfrak{A}} \prod_{j=1}^{n} \sum_{r=0}^{\gamma} \chi(u_j, r) z^{(r)} = q^k \sum_{v \in \mathfrak{B}} z^{(v_1)} z^{(v_2)} \cdots z^{(v_n)}$$

*Proof:* We evaluate the quantity

$$F(u, v) = \sum_{u \in \mathfrak{A}} \sum_{v \in F^n} \chi(u, v) z^{(v_1)} z^{(v_2)} \cdots z^{(v_n)}$$

in two ways, which give the two sides of the equation.
By 2.6

$$F(u, v) = \sum_{u \in \mathfrak{A}} \prod_{j=1}^{n} \sum_{r=0}^{\gamma} \chi(u_j, r) z^{(r)}.$$

Also

$$F(u, v) = \sum_{v \in F^n} z^{(v_1)} z^{(v_2)} \cdots z^{(v_n)} \sum_{u \in \mathfrak{A}} \psi(u, v).$$

By 2.4 and 2.3

$$\sum_{u \in \mathfrak{A}} \psi(u, v) = \begin{cases} q^k \text{ if } v \in \mathfrak{B} \\ 0 \text{ if } v \notin \mathfrak{B}. \end{cases}$$

Hence

$$F(u, v) = q^k \sum_{v \in \mathfrak{B}} z^{(v_1)} z^{(v_2)} \cdots z^{(v_n)}.$$

*Theorem 2.8: Let* $\mathfrak{A}$ *be a* $k$*-dimensional alphabet of* $F^n$, *and* $\mathfrak{B}$ *the orthogonal complement of dimension* $m = n - k$. *Let* $A_i$, $B_i$ *denote the number of letters of weight* $i$ *in* $\mathfrak{A}$, $\mathfrak{B}$. *Then*

$$\sum_{i=0}^{n} A_i (1 + \gamma z)^{n-i} (1 - z)^i = q^k \sum_{i=0}^{n} B_i z^i.$$

*Proof:* In 2.7 set $z^{(r)} = \begin{cases} z & \text{if } r \neq 0 \\ 1 & \text{if } r = 0. \end{cases}$

If $u_j = 0$, $\chi(u_j, r)$ is 1 and $\sum_{r=0}^{\gamma} \chi(u_j, r) z^{(r)}$ becomes $(1 + \gamma z)$.

If $u_j \neq 0$ $\sum_{r=1}^{\gamma} \chi(u_j, r)$ is $-1$, and $\sum_{r=0}^{\gamma} \chi(u_j, r) z^{(r)}$ becomes $(1 - z)$.

Let $| u |$ denote the number of nonzero $u_j$.

Then $\prod_{j=1}^{n} \sum_{r=0}^{\gamma} \chi(u_j, r) z^{(r)}$ goes into $(1 + \gamma z)^{n-|u|}(1 - z)^{|u|}$; $| u |$ is of course the weight of $u = (u_1, u_2, \cdots, u_n)$, so that the left-hand side of 2.7 becomes

$$\sum_{i=0}^{n} A_i (1 + \gamma z)^{n-i}(1 - z)^i.$$

The right-hand side of 2.7 is clearly

$$q^k \sum_{i=0}^{n} B_i z^i,$$

which proves the theorem.

Innumerable sets of linear equations between the quantities $A_i$, $B_i$ may be obtained from theorem 2.8. The following two are sometimes useful.

*Lemma 2.9: For* $\nu = 0, 1, \cdots, n$,

*i.*
$$\sum_{i=0}^{n-\nu} A_i \binom{n-i}{\nu} = q^{k-\nu} \sum_{i=0}^{n} B_i \binom{n-i}{n-\nu}.$$

(*These are the equations of* 2.2.)

*ii.*
$$\sum_{i=\nu}^{n} A_i \binom{i}{\nu} = q^{k-\nu} \sum_{i=0}^{\nu} (-1)^i B_i \gamma^{\nu-i} \binom{n-i}{n-\nu}.$$

*i.* is obtained by setting $(1 + \gamma z)/(1 - z) = 1 + y$,

*ii.* by setting $(1 - z)/(1 + \gamma z) = 1 + y$. The algebraic details are easy to verify.

This process is reversible, i.e., (*i*) or (*ii*) imply 2.8. Before exploring the consequences of theorem 2.8, we give a different specialization of 2.7.

*Theorem 2.10: Let* $B_s^{(1)}$ *be the number of letters of* $\mathfrak{B}$ *which contain* $s$ *coordinates equal to* 1. *Let* $A_{0s}$ *be the number of letters* $u$ *in* $\mathfrak{A}$ *of weight* $s$ *for which* $\sum_{i=1}^{n} u_i = 0$. *Let* $A_{1s}$ *be the number of letters* $u$ *in* $\mathfrak{A}$ *of weight* $s$ *for which* $\sum_{i=1}^{n} u_i \neq 0$. (*Clearly* $A_s = A_{0s} + A_{1s}$).
*Then*

$$\sum_{s=0}^{n} B_s^{(1)} z^s = (A_{0s} - A_{1s}/\gamma)(z - 1)^s (z + \gamma)^{n-s}.$$

*Proof:* In 2.7 set

$$z^{(r)} = \begin{cases} z & \text{if } r = 1 \\ 1 & \text{if } r \neq 1. \end{cases}$$

Then

$$q^k \sum_{\nu \in \mathfrak{B}} z^{(\nu_1)} z^{(\nu_2)} \cdots z^{(\nu_n)} \text{ becomes } q^k \sum_{s=0}^{n} B_s^{(1)} z^s,$$

$$\sum_{r=0}^{\gamma} \chi(u_i, r) z^{(r)} \text{ becomes } \chi(u_i, 1) z + \sum_{r=0}^{\gamma} \chi(u_i, r) - \chi(u_i, 1)$$

$$= \chi(u_i, 1)(z - 1) + \sum_{r=0}^{\gamma} \chi(u_i, r)$$

$$= \begin{cases} \chi(u_i, 1)(z - 1) & \text{if } u_i \neq 0 \\ z + \gamma & \text{if } u_i = 0 \end{cases}$$

$$\prod_{i=1}^{n} \sum_{r=0}^{\gamma} \chi(u_i, r) z^{(r)} \quad \text{becomes} \quad (z + \gamma)^{n-|u|} (z - 1)^{|u|} \prod_{u_i \neq 0} \chi(u_i, 1).$$

Now if $u$ is a letter of $A$, so are also the letters $2u, \cdots, \gamma u$, and these have the same weight as $u$. We sum first over these letters

$$\sum_{s=1}^{\gamma} \prod \chi(su_i, 1) = \sum_{s=1}^{\gamma} \chi(s \Sigma u_i, 1)$$

$$= \begin{cases} -1 & \text{if } \Sigma u_i \neq 0 \\ \gamma & \text{if } \Sigma u_i = 0 \end{cases}$$

The sum of

$$(z + \gamma)^{n-|u|} (z - 1)^{|u|} \prod_{u_i \neq 0} \chi(u_i, 1)$$

over all letters in $\mathfrak{A}$ of the same weight as $u$ is thus

$$(A_{0|u|} - (A_{1|u|}/\gamma))(z + \gamma)^{n-|u|} (z - 1)^{|u|}.$$

Hence the left-hand side of 2.7 becomes

$$\sum_{s=0}^{n} (A_{0s} - (A_{1s}/\gamma))(z + \gamma)^{n-s} (z - 1)^s.$$

We return now to the consequences of theorem 2.8. As remarked in the proof of 2.10, if $\mathfrak{A}$ contains a letter $u$, it contains also the letters $2u, \cdots, \gamma u$; that is, the number of letters of weight $i$ in $\mathfrak{A}$ is divisible by $\gamma$ for $i > 0$. We have then

*Lemma 2.11: A necessary condition for the existence of an alphabet containing letters of weights $w_i$, $i = 1, 2, \cdots, s$, and no other, is the existence of a set of integers $\alpha_i$, $i = 1, 2, \cdots, s$, such that the expression*

$$(1 + \gamma z)^n + \gamma \sum_{j=1}^{s} \alpha_i (1 + \gamma z)^{n-w_i}(1 - z)^{w_i},$$

*when expanded in powers of* $z$, *takes the form*

$$q^k + \gamma q^k \sum_{i=1}^{n} \beta_i z^i,$$

*where the* $\beta_i$ *are positive integers.*

It has been pointed out before that this condition is not sufficient.

Suppose now that $\mathfrak{A} = \mathfrak{A}_1 + \mathfrak{A}_2$ is a decomposable alphabet. $\mathfrak{A}_j$ is a $k_j$-dimensional alphabet in $F^{n_j}$, $j = 1, 2$, with orthogonal alphabet $B_j$. $k_1 + k_2 = k$, and $n_1 + n_2 = n$. Let $A_i^{(1)}$, $A_i^{(2)}$ and $B_i^{(1)}$, $B_i^{(2)}$ be the number of letters of weight $i$ in $\mathfrak{A}_1$, $\mathfrak{A}_2$, $\mathfrak{B}_1$, $\mathfrak{B}_2$.

*Lemma 2.12:*

$$\sum_{i=0}^{n} A_i (1 + \gamma z)^{n-i}(1 - z)^i$$

$$= \left[\sum_{i=0}^{n_1} A_i^{(1)}(1 + \gamma z)^{n_1-i}(1 - z)^i\right]\left[\sum_{i=0}^{n_2} A_i^{(2)}(1 + \gamma z)^{n_2-i}(1 - z)^i\right]$$

$$= \sum_{i=0}^{n}\left[q^{k_1}\sum_{i=0}^{n_1} B_i^{(1)} z^i\right]\left[q^{k_2}\sum_{i=0}^{n_2} B_i^{(2)} z^i\right].$$

*Proof:* The number of letters of weight $s$ in $\mathfrak{B}_1 + \mathfrak{B}_2$ is

$$\sum_{\sigma+\rho=s} B_\sigma^{(1)} B_\rho^{(2)},$$

which is the coefficient of $z^s$ in $\sum_{i=0}^{n_1} B_i^{(1)} z^i \sum_{i=0}^{n_2} B_i^{(2)} z^i$. Similarly,

$$\sum_{\sigma+\rho=s} A_\sigma^{(1)} A_\rho^{(2)}$$

is the coefficient of $(1 + \gamma z)^{n-s}(1 - z)^s$ in

$$\left[\sum_{i=0}^{n_1} A_i^{(1)}(1 + \gamma z)^{n_1-i}(1 - z)^i\right]\left[\sum_{i=0}^{n_2} A_i^{(2)}(1 + \gamma z)^{n_2-i}(1 - z)^i\right].$$

We define the coset leader of a coset of $\mathfrak{A}$ in $F^n$ to be an element of least weight in the coset. The weight of a coset is defined to be the weight of its coset leader.

If $A_i = 0$ for $i = 1, 2, \cdots, 2e$ every vector of weight $\leqq e$ in $F^n$ appears as a coset leader for $\mathfrak{A}$ and conversely. Another way of saying this is: for all pairs of distinct letters $a$, $a'$ of $\mathfrak{A}$, the set of vectors at distance $i \leqq e$ from $a$ is disjoint from the set of vectors at distance $i$ from $a'$.

Let $c_1^{(i)}, c_2^{(i)}, \cdots, c_\nu^{(i)}$ be the cosets of $A$ of weight $i$; we assume that

$\nu = \gamma^i \binom{n}{i}$, i.e., that all vectors of weight $i$ appear as coset leaders. Let $f_{s,i}$ be the number of vectors of weight $s$ contained in the set-theoretic union $\bigcup_{j=1}^{\nu} c_j^{(i)}$. The polynomial $\sum_{s=0}^{n} f_{s,i} x^s$ is called the enumerator (by weight) of this set of vectors. We propose to show that theorem 2.8 gives a convenient expression for this enumerator. We need the following preliminary lemma.

*Lemma 2.13: Let $u$ be a fixed vector of weight $i$. Let $d_{st}$ be the number of vectors of weight $s$ which are at distance $t$ from $u$. Then*

$$\sum_{s=0}^{n} \sum_{t=0}^{n} d_{st} x^s y^t = (1 + \gamma xy)^{n-i}[x + y + (\gamma - 1)xy]^i.$$

*Proof:* Suppose first that $u = (u_1, u_2, \cdots, u_i)$ is a vector of weight $i$ in $F^i$. We show that under these circumstances

$$\sum_{s=0}^{i} \sum_{t=0}^{i} d_{st} = [x + y + (\gamma - 1)xy]^i.$$

This is obvious for $i = 1$; we suppose it true for $i - 1$. Let $v = (v_1, v_2, \cdots, v_{i-1})$ be a vector of weight $s$ distant $t$ from $(u_1, u_2, \cdots, u_{i-1})$ in $F^{i-1}$. From $v$ we obtain:

*i.* One vector $(v_1, v_2, \cdots, v_{i-1}, 0)$, weight $s$, distant $t + 1$ from $u$.

*ii.* One vector $(v_1, v_2, \cdots, v_{i-1}, u_i)$ weight $s + 1$ distant $t$ from $u$.

*iii.* $\gamma - 1$ vectors $(v_1, v_2, \cdots, v_{i-1}, v_i)$ $v_i \neq 0$, $v_i \neq u_i$ which have weight $s + 1$, and are distant $t + 1$ from $u$.

Hence the enumerator for $i$ is obtained by multiplying that for $i - 1$ by $[x + y + (\gamma - 1)xy]$, and the lemma is proved for $n = i$.

We now apply induction to $n - i$. Let $u$ be a vector of weight $i$ in $F^n$, and $u'$ a vector of weight $i$ in $F^{n-1}$ obtained from $u$ by omitting one zero coordinate. Let $v'$ be a vector of $F^{n-1}$ which has weight $s$ and is distant $t$ from $u'$. From $v'$ we obtain in $F^n$

*i.* One vector of weight $s$, distant $t$ from $u$, by adding a zero coordinate to $v'$.

*ii.* $\gamma$ vectors of weight $s + 1$, distant $t + 1$ from $u$, by adding a non-zero coordinate to $v'$.

This corresponds to multiplication by $(1 + \gamma xy)$. Hence the lemma is proved.

*Lemma 2.14: Suppose that $A_i = 0$, $i = 1, 2, \cdots, 2e$, and take $t \leqq e$. Then the enumerator, $\sum_{s=0}^{n} f_{s,i} x^s$, of vectors in cosets of weight $t$ of $F^n$ mod $\mathfrak{A}$ is the coefficient of $y^t$ in*

$$\sum_{i=0}^{n} A_i (1 + \gamma xy)^{n-i}(x + y + (\gamma - 1)xy)^i.$$

*Proof:* The cosets of weight $t$ in $F^n$ *mod* $\mathfrak{A}$ are disjoint, and contain all vectors of $F^n$ which are at distance $t$ from some letter of $\mathfrak{A}$.

Set $(1 + \gamma z)^{n-i}(1 - z)^i = \sum_{r=0}^{n} \Psi(i, n, r) z^r$. Let $\mathfrak{B}$, $B_i$ have their usual meaning. Assume the conditions of 2.14.

*Lemma 2.15:*†

$$q^m \sum_{s=0}^{n} f_{s,t} x^s = \sum_{i=0}^{n} B_i \Psi(i, n, t)(1 + \gamma x)^{n-i}(1 - x)^i$$

*Proof:* Set

$$z = \frac{x + y + (\gamma - 1)xy}{1 + \gamma xy},$$

then

$$1 + \gamma z = \frac{(1 + \gamma x)(1 + \gamma y)}{(1 + \gamma xy)}, \qquad 1 - z = \frac{(1 - x)(1 - y)}{1 + \gamma xy}.$$

Make this substitution in the equation

$$\sum_{i=0}^{n} B_i (1 + \gamma z)^{n-i}(1 - z) = q^m \sum_{i=0}^{n} A_i z^i$$

we obtain

$$\sum_{i=0}^{n} B_i (1 + \gamma x)^{n-i}(1 - x)^i (1 + \gamma y)^{n-i}(1 - y)^i$$
$$= q^m \sum_{i=0}^{n} A_i (1 + \gamma xy)^{n-i}(x + y + (\gamma - 1)xy)^i.$$

Equating coefficients of $y^t$ gives us

$$\sum_{i=0}^{n} B_i \Psi(i, n, t)(1 + \gamma x)^{n-i}(1 - x)^i = q^m \sum_{s=0}^{n} f_{s,t} x^s$$

## III. APPLICATIONS

The easiest application of theorem 1 is to a generalized Hamming alphabet, that is, a close-packed 1-error correcting alphabet over a field of $q$ elements. Such an alphabet exists for $n = (q^m - 1)/\gamma$, all $m > 1$.[3]

The dual alphabet is of dimension $m$, and contains $(q^m - 1)$ letters of weight $q^{m-1}$. The spectrum of a generalized Hamming alphabet is thus given by the expansion of

$$(1 + \gamma z)^n + (q^m - 1)(1 + \gamma z)^{n-u}(1 - z)^u$$

where $n = (q^m - 1)/\gamma$, $u = q^{m-1}$

† A similar formula ($q = 2$) is found by Lloyd[5] for close-packed codes which are not assumed to be group codes.

TABLE I — DISTRIBUTION OF WEIGHTS IN THE TWO GOLAY CODES

The first table is for the 3-error-correcting (23, 12) alphabet over $Z_2$, the second for the 2-error-correcting (11, 6) alphabet over $Z_3$. In both cases, $i$ stands for weight, $B_i$ for the number of letters of weight $i$ in the dual alphabet, $A_i$ for the number of letters of this weight in the Golay alphabet.

| $i$ | $B_i$ | $A_i$ |
|---|---|---|
| 0 | 1 | 1 |
| 7 | 0 | 23 × 11 |
| 8 | 23 × 22 | 23 × 22 |
| 11 | 0 | 23 × 56 |
| 12 | 23 × 56 | 23 × 56 |
| 15 | 0 | 23 × 22 |
| 16 | 23 × 11 | 23 × 11 |
| 23 | 0 | 1 |

| $i$ | $B_i$ | $A_i$ |
|---|---|---|
| 0 | 1 | 1 |
| 5 | 0 | 2 × 66 |
| 6 | 2 × 66 | 2 × 66 |
| 8 | 0 | 2 × 165 |
| 9 | 2 × 55 | 2 × 55 |
| 11 | 0 | 2 × 12 |

Theorem 1 may, in fact, be used to calculate the number of letters of each weight in any close-packed code. The results for the two Golay[6] codes are given in Table I.

Anything which is known about the structure of an alphabet or its dual may be used with theorem 1 to limit the number of possible weight distributions. Such items of information are a very diversified character, and no general method has been developed. However, the results obtained by hand calculation indicated that it is probably worthwhile to make a systematic computer study of the known classes of alphabets.

ACKNOWLEDGMENTS

The author would like to thank her friends and associates for their consistently helpful suggestions; and is especially indebted to H. E. Elliott for the elegant proof of lemma 2.5 and to J. B. Kruskal for theorem 2.10. The criticisms and suggestions of Professor A. M. Gleason of Harvard University produced new and better proofs of practically every other theorem in this paper.

REFERENCES

1. Slepian, D., A Class of Binary Signaling Alphabets, B.S.T.J., **35,** January, 1956, pp. 203–234.
2. Bose, R. C., and Kuebler, R. R., Jr., A Geometry of Binary Sequences Associated with Group Alphabets in Information Theory, Ann. Math. Stat. **31,** 1960, p. 113.
3. MacWilliams, F. J., Error-correcting Codes for Multiple-Level Transmission, B.S.T.J., **40,** January, 1961, pp. 281–308.
4. Slepian, D., Some Further Theory of Group Codes, B.S.T.J., **39,** September, 1960, pp. 1219–1252.
5. Lloyd, S. P., Binary Block Coding, B.S.T.J., **36,** March, 1957, pp. 517–535.