A GEOMETRY OF BINARY SEQUENCES ASSOCIATED WITH GROUP ALPHABETS IN INFORMATION THEORY[1]

By R. C. Bose and Roy R. Kuebler, Jr.

University of North Carolina

1. The group alphabet. When a piece of information, or *letter* is transmitted over a symmetric binary channel [14], the letter is presented to the channel in the form of a sequence of n binary digits. Because of *noise* on the channel, there is a positive probability p that a transmitted symbol will be received in error, that is, a transmitted 0 will be received as 1 or transmitted 1 received as 0. It is assumed that $0 < p < \frac{1}{2}$, and that the noise on the channel operates independently on each symbol that is presented for transmission. If the collection of all distinct pieces of information—the *alphabet*—consists of $K = 2^k$ letters, it is customary to take $n > k$, and in some manner use the additional digit positions to "correct" errors in transmission. Slepian [14] has introduced the *n-place group alphabet*, or, briefly, the (n, k)*-alphabet*, and an associated decoding scheme. The 2^n possible binary sequences form an Abelian group B_n wherein the group operation is addition modulo 2 of vectors given by the sequences. An (n, k)-alphabet is a 2^k-letter n-place binary signaling alphabet whose letters form a subgroup of B_n.

Let us designate the letters of the alphabet by

$$U_0 = I = (000 \cdots 0), U_1, U_2, \cdots, U_\mu, \mu = 2^k - 1.$$

The group B_n can be developed according to the alphabet and its cosets:

$$(1) \qquad \begin{array}{lllll} I = U_0 = L_0, & U_1, & U_2, & \cdots & U_\mu, \\ L_1 \quad, & L_1 + U_1, & L_1 + U_2, & \cdots & L_1 + U_\mu, \\ L_2 \quad, & L_2 + U_1, & L_2 + U_2, & \cdots & L_2 + U_\mu, \\ \cdots & \cdots & \cdots & & \cdots \\ L_\nu \quad, & L_\nu + U_1, & L_\nu + U_2, & \cdots & L_\nu + U_\mu, \end{array}$$

where $\nu = 2^{n-k} - 1$, and L_l is an n-place binary sequence which has not appeared in cosets led by $L_0, L_1, \cdots, L_{l-1}$. The group elements L_l are called *coset leaders*.

The *weight* $w(T_j)$ of an element T_j of B_n is defined as *the number of ones in the n-place binary sequence* T_j.

Because of the group property, any coset is repeated, with elements in a

Received December 1, 1958; revised May 25, 1959.

[1] This research was supported by the United States Air Force through the Air Force Office of Scientific Research of the Air Research and Development Command, and by the United States Public Health Service through a grant to support a research fellowship in biostatistics.

different order, if the coset leader is replaced by any other element of the coset. It is then agreed that L_l will be taken as that element (or any one of these elements) of the coset l whose weight is least. The detection scheme is then the following: if the element of B_n which is received from the channel output lies in column i of the coset array, the detector prints the letter U_i.

The following is an example ($k = 3$, $n = 5$) of such an array.

(2)

	I	U_1	U_2	U_3	U_4	U_5	U_6	U_7
Alphabet:	00000	00111	11101	00011	11010	00100	11110	11001
Cosets	10000	10111	01101	10011	01010	10100	01110	01001
	01000	01111	10101	01011	10010	01100	10110	10001
	00010	00101	11111	00001	11000	00110	11100	11011

For such a code, given p and setting $q = 1 - p$,

$$(3) \quad Q_1 = Pr(\text{transmitted letter } U_i \text{ be correctly produced by the detector}) = \sum_{l=0}^{\nu} p^{w(L_l)} q^{n-w(L_l)}.$$

Since $p^w q^{n-w}$ is a monotonically decreasing function of w, one sees the motivation for taking as L_l an element of minimal weight in coset l.

As Slepian has observed [14]: "Two important questions regarding (n, k)-alphabets naturally arise. What is the maximum value of Q_1 possible for a given n and k and which of the $\cdots$ different subgroups [alphabets] give rise to this maximum Q_1? The answers to these questions for general n and k are not known. For many special values of n and k the answers are known." The present paper is directed towards developing a geometry which can give an additional tool for use in studies on group alphabets. To the reader interested in other aspects of the coding problem there may be cited, as representative of analyses of the problem and methods of approach, papers of Hamming [10], Gilbert [8], Golay [9], Elias [5, 6], Reed [13], Lloyd [11], Calabi and Haefeli [4], MacDonald [12], Fontaine and Peterson [7].

2. An algebra of binary sequences.

We introduce an algebra of binary sequences, defined as follows. The *elements* of the algebra are the n-place binary sequences $T_1, T_2, \cdots, T_{2^n}$, where $T_j = (a_{j1}, a_{j2}, \cdots, a_{jn})$, each a_{ji} being either zero or one. In the present case, all letters of the alphabet and all elements of cosets are binary sequences of this nature.

Addition is defined by

$$(4) \qquad T_i + T_j = (a_{i1} + a_{j1}, a_{i2} + a_{j2}, \cdots, a_{in} + a_{jn}),$$

where the addition is vector addition modulo 2. This addition clearly has all the usual properties: commutativity, associativity, inversion. We note a special property of this addition: for any n-place binary sequence T, $2T = T + T = (0\ 0\ 0 \cdots 0)$, the null sequence.

The *product* T_iT_j is defined as

$$(5) \qquad T_iT_j = (a_{i1}a_{j1}, a_{i2}a_{j2}, \cdots, a_{in}a_{jn});$$

that is, the coordinates of the product are the products of matching coordinates of the factors. This multiplication of course has all the usual multiplicative properties: commutativity, associativity, distributivity. However, inversion is not satisfied; that is, division is not unique. We shall not perform the division operation. Since

$$a_{iu}a_{ju} = \begin{cases} 1 \text{ when and only when } a_{iu} = a_{ju} = 1, \\ 0 \text{ otherwise,} \end{cases}$$

a special property of the multiplication in this algebra is that every element is *idempotent*; that is, for any n-place binary sequence T,

$$T^2 = T. \tag{6}$$

Two particularly useful properties follow from (6). For any two sequences T_1, T_2,

$$(T_1 + T_1T_2)(T_2 + T_1T_2) = T_1T_2 + T_1^2T_2 + T_1T_2^2 + T_1^2T_2^2 = 4T_1T_2 = 0, \tag{7}$$

$$(T_1 + T_2)(T_1T_2) = T_1^2T_2 + T_1T_2^2 = 2T_1T_2 = 0. \tag{8}$$

Consider the weight $w(T)$ of two binary sequences T_i and T_j, where $w(T)$ is as defined in Section 1 (the number of unities in T), and let us investigate $w(T_i + T_j)$ and $w(T_iT_j)$. An example of these T's could be

$$\begin{array}{rl} T_1: & (1 \ \ 1 \ \ 1 \ \ 1 \ \ 1 \ \ 0 \ \ 0 \ \ 0 \ \ 0 \ \ 0), \\ T_2: & (0 \ \ 0 \ \ 1 \ \ 1 \ \ 1 \ \ 1 \ \ 1 \ \ 1 \ \ 0 \ \ 0), \\ T_1 + T_2: & (1 \ \ 1 \ \ 0 \ \ 0 \ \ 0 \ \ 1 \ \ 1 \ \ 1 \ \ 0 \ \ 0), \\ T_1T_2: & (0 \ \ 0 \ \ 1 \ \ 1 \ \ 1 \ \ 0 \ \ 0 \ \ 0 \ \ 0 \ \ 0). \end{array}$$

T_iT_j has unities only in those positions occupied by unities in both T_i and T_j, so that $w(T_iT_j)$ is the number of unit coordinates common to T_i and T_j. These are precisely the unit coordinates yielding zeros in the sum $T_i + T_j$. Thus we have the following theorems.

THEOREM 1. $w(T_iT_j) \leqq \min [w(T_i), w(T_j)]$.

THEOREM 2. $w(T_i + T_j) = w(T_i) + w(T_j) - 2w(T_iT_j)$.

Useful corollaries to Theorem 2 are the following.

COROLLARY 2.1. *If* $w(T_iT_j) = w(T_iT_k) = w(T_i)$, *then* $w(T_jT_k) \geqq w(T_i)$.

PROOF. The theorem gives

$$w(T_j + T_k) = w(T_j) + w(T_k) - 2w(T_jT_k). \tag{9}$$

But also

$$\begin{aligned} w(T_j + T_k) &= w[(T_i + T_j) + (T_i + T_k)] \\ &\leqq w(T_i + T_j) + w(T_i + T_k) \\ &= w(T_i) + w(T_j) - 2w(T_iT_j) + w(T_i) + w(T_k) - 2w(T_iT_k) \\ &= w(T_j) + w(T_k) - 2w(T_i). \end{aligned}$$

Applying this result to (9), we obtain immediately $w(T_jT_k) \geqq w(T_i)$.

COROLLARY 2.2. *If $T_i = T_iT_j$ and $w(T_i) = w(T_j)$, then $T_i = T_j$.*

PROOF. From the given conditions we have

$$w(T_i + T_j) = w(T_i) + w(T_j) - 2w(T_iT_j)$$
$$= w(T_i) + w(T_i) - 2w(T_i) = 0.$$

That is, $T_i + T_j$ is the null sequence, whence $T_i = T_j$.

THEOREM 3. *The necessary and sufficient condition that $w(T_iT_j) = w(T_i)$ is that $T_iT_j = T_i$.*

PROOF. If $T_iT_j = T_i$, then obviously $w(T_iT_j) = w(T_i)$. Conversely, let $w(T_iT_j) = w(T_i)$. Before applying the condition, we have from the definition of multiplication that T_iT_j has zero for each coordinate which is zero in T_i. The remaining coordinates of T_iT_j are those which in T_i are unities. But if $w(T_iT_j) = w(T_i)$, then these coordinates must be unities in T_iT_j. Hence, the coordinates of T_iT_j are identical with those of T_i, that is, $T_iT_j = T_i$.

3. A geometry of binary sequences. Application is made of the notions of finite projective geometry introduced by Bose [1] and used by him and others in the development of incomplete block and factorial designs (for example, [1] and [2]).

The group alphabet in which we are interested is composed of the null letter $I = (0\,0\,0 \cdots 0)$ and $\mu = 2^k - 1$ nonnull letters, $U_1, U_2, \cdots, U_\mu$, which are generated by any k independent sequences, say

$$\begin{aligned} U_1 &= (a_{11}, a_{12}, a_{13}, \cdots, a_{1n}), \\ U_2 &= (a_{21}, a_{22}, a_{23}, \cdots, a_{2n}), \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ U_k &= (a_{k1}, a_{k2}, a_{k3}, \cdots, a_{kn}), \end{aligned} \tag{10}$$

where the a_{ij} are elements of the Galois field GF(2) and not all zero. The general nonnull letter U of the alphabet is thus

$$U = \lambda_1 U_1 + \lambda_2 U_2 + \cdots + \lambda_k U_k, \tag{11}$$

where $\lambda_1, \lambda_2, \cdots, \lambda_k$ are elements of GF(2), not all zero. For example, the nonnull letters of the alphabet (2) can be taken as:

$$\begin{aligned} U_1 &= (00111) = 1(U_1) + 0(U_2) + 0(U_3), \\ U_2 &= (11101) = 0(U_1) + 1(U_2) + 0(U_3), \\ U_3 &= (00011) = 0(U_1) + 0(U_2) + 1(U_3), \\ U_4 &= (11010) = 1(U_1) + 1(U_2) + 0(U_3), \\ U_5 &= (00100) = 1(U_1) + 0(U_2) + 1(U_3), \\ U_6 &= (11110) = 0(U_1) + 1(U_2) + 1(U_3), \\ U_7 &= (11001) = 1(U_1) + 1(U_2) + 1(U_3). \end{aligned} \tag{12}$$

Our geometry must take into account these $2^k - 1$ letters, and also all the remaining $2^n - 2^k$ possible nonnull binary sequences.

Consider a (topological) space Ω consisting of n distinct points $Y_1, Y_2, \cdots,$

Y_n, where the point Y_i of Ω is considered to correspond to the i-th position in an n-place binary sequence. In other words, Ω is a space of *positions*. Each binary sequence $T_j = (a_{j1}, a_{j2}, \cdots, a_{jn})$ corresponds to a unique subset of Ω, namely, the subset of those positions which are occupied by unity in T_j. For example, if $n = 6$, the binary sequence (011001) corresponds to the subset (Y_2, Y_3, Y_6) of Ω. Thus, Y_i is a member of the subset Ω_j corresponding to T_j if and only if a_{ji} is unity. Conversely, given any subset Ω_j of Ω, we can at once write down the corresponding binary sequence T_j by taking unities in those positions which correspond to the elements of Ω_j, and zeros in the other places. For example, if $n = 7$ and $\Omega_j = (Y_1, Y_2, Y_4, Y_6)$, we have at once $T_j = (1101010)$. Thus the 2^n binary sequences have (1,1) correspondence with the 2^n distinct subsets of Ω. In particular, the whole space Ω corresponds to the sequence $E = (1\ 1\ 1 \cdots 1)$, the unit element of the ring algebra introduced in the preceding section, and the null set corresponds to the sequence $I = (0\ 0\ 0 \cdots 0)$, the zero element of the ring.

As any other sequence, the letter U_j of the alphabet (11) corresponds to the Ω-subset of those positions in which U_j has unities. We shall denote this subset by $\Omega_1(U_j)$. We shall denote by $\Omega_0(U_j)$ the complementary set of positions (which are occupied by zero in U_j). These two sets are disjoint, and their union gives the whole space Ω. Referring to (12) for example, we have $\Omega_1(U_7) = (Y_1, Y_2, Y_5)$ and $\Omega_0(U_7) = (Y_3, Y_4)$.

For any k-place sequence $y_1, y_2, \cdots, y_k$ of elements of GF(2), we define the subset $\Omega(y_1, y_2, \cdots, y_k)$ by

$$(13) \qquad \Omega(y_1, y_2, \cdots, y_k) = \Omega_{y_1}(U_1) \cap \Omega_{y_2}(U_2) \cap \cdots \cap \Omega_{y_k}(U_k).$$

For example, referring again to (12), we have

$$\begin{aligned} \Omega(1, 0, 1) &= \Omega_1(U_1) \cap \Omega_0(U_2) \cap \Omega_1(U_3) \\ &= (Y_3, Y_4, Y_5) \cap (Y_4) \cap (Y_4, Y_5) \\ &= (Y_4). \end{aligned}$$

As shown by the definition (13), an element of Ω is a member of $\Omega(y_1, y_2, \cdots, y_k)$ if and only if it is a position which is occupied by y_1 in U_1, y_2 in U_2, $\cdots$, y_k in U_k. Each such position will then be occupied by $\lambda_1 y_1 + \lambda_2 y_2 + \cdots + \lambda_k y_k$ in $U = \lambda_1 U_1 + \lambda_2 U_2 + \cdots + \lambda_k U_k$. Thus, if in our preceding example, where $\Omega(1, 0, 1) = Y_4$, we consider $(\lambda_1, \lambda_2, \lambda_3) = (1, 1, 0)$, we have

$$\lambda_1 y_1 + \lambda_2 y_2 + \lambda_3 y_3 = 1(1) + 1(0) + 0(1) = 1,$$

which is seen to be the digit occupying the fourth position in

$$1(U_1) + 1(U_2) + 0(U_3) = (11010).$$

Hence, if

$$(14) \qquad \lambda_1 y_1 + \lambda_2 y_2 + \cdots + \lambda_k y_k \neq 0 \qquad \text{(i.e., } =1\text{)},$$

then each element of $\Omega(y_1, y_2, \cdots, y_k)$ is a member of the set $\Omega_1(U)$ corresponding to $U = \lambda_1 U_1 + \lambda_2 U_2 + \cdots + \lambda_k U_k$; otherwise, each element of $\Omega(y_1, y_2, \cdots, y_k)$ is a member of the complementary set $\Omega_0(U)$.

We can assume that there is no position which is occupied by zero in every one of $U_1, U_2, \cdots, U_k$, for otherwise this position would be occupied by zero in every letter of the alphabet and would therefore convey no information. Hence the set $\Omega(0, 0, \cdots, 0)$ is always null, and we shall neglect it. Thus there are $2^k - 1$ different sets $\Omega(y_1, y_2, \cdots, y_k)$, $(y_1, y_2, \cdots, y_k) \neq (0, 0, \cdots, 0)$. Any two distinct sequences $y_1, y_2, \cdots, y_k$ will differ as regards at least one element, and hence the two sets $\Omega(y_1, y_2, \cdots, y_k)$ will differ with respect to at least one factor in (13), say the u-th. Then we shall have $\Omega_1(U_u)$ in one case, and $\Omega_0(U_u)$ in the other. These two sets are disjoint, and hence so are the two sets $\Omega(y_1, y_2, \cdots, y_k)$, since each is a subset of each of its factors. Furthermore, since each position is clearly defined in every U_j, every element of Ω is a member of *some* $\Omega(y_1, y_2, \cdots, y_k)$; one need only write down for $y_1, y_2, \cdots, y_k$ the digits occupying the corresponding position in $U_1, U_2, \cdots, U_k$ [in (12) for example, Y_3 is an element of $\Omega(1, 1, 0)$]. Hence, as $(y_1, y_2, \cdots, y_k)$ runs over the $2^k - 1$ possible sets of values, the sets $\Omega(y_1, y_2, \cdots, y_k)$ exhaust Ω. Thus *the sets* $\Omega(y_1, y_2, \cdots, y_k)$ *are disjoint, and their union gives the whole space.*

From what has been stated concerning (14) above, it is clear that the set $\Omega_1(U)$ corresponding to U is the union of all the (disjoint) sets $\Omega(y_1, y_2, \cdots, y_k)$ for which $(y_1, y_2, \cdots, y_k)$ satisfies (14). If $n(y_1, y_2, \cdots, y_k)$ denotes the number of points in $\Omega(y_1, y_2, \cdots, y_k)$, then, since the sets $\Omega(y_1, y_2, \cdots, y_k)$ are disjoint and exhaust Ω, $\sum n(y_1, y_2, \cdots, y_k) = n$, the summation being over all the $2^k - 1$ values $(y_1, y_2, \cdots, y_k)$. Also, for the weight $w(U)$ of U, as defined in Section 1, we have

$$w(U) = \tilde{\sum} n(y_1, y_2, \cdots, y_k), \tag{15}$$

where $\tilde{\sum}$ indicates summation over all those values $(y_1, y_2, \cdots, y_k)$ satisfying $\lambda_1 y_1 + \lambda_2 y_2 + \cdots + \lambda_k y_k = 1$.

Consider now the finite projective space $PG(k - 1, 2)$, and to the point $P = (y_1, y_2, \cdots, y_k)$ of this space associate the set $\Omega(y_1, y_2, \cdots, y_k)$. Let the points of $PG(k - 1, 2)$ be $P_1, P_2, \cdots, P_\mu$, $\mu = 2^k - 1$, where $P_i = (y_{1i}, y_{2i}, \cdots, y_{ki})$. If we define the n-measure of the point P_i as $n(P_i) = n(y_{1i}, y_{2i}, \cdots, y_{ki}) = n_i$, then there are n_i points of Ω which constitute the set associated with P_i. These points we may now rename as $P_{i1}, P_{i2}, \cdots, P_{in_i}$, and identify with the point P_i taken n_i times. Thus Ω may be considered to consist of the points $P_1, P_2, \cdots, P_\mu$, the point P_i being taken with a multiplicity n_i. If in particular $n_i = 0$, then P_i does not belong to Ω. It is useful to institute a logical distinction between geometric points and Ω-points. Each P_i constitutes a single geometric point, but counts as $n_i = n(P_i)$ Ω-points. The total number of geometric points is $\mu = 2^k - 1$; the total number of Ω-points is n.

The points $(y_1\ ,\ y_2\ ,\ \cdots\ ,\ y_k)$ which satisfy (14) are the points *not* lying on the $(k - 2)$-flat

$$(16)\qquad \lambda_1 y_1 + \lambda_2 y_2 + \cdots + \lambda_k y_k = 0.$$

This $(k - 2)$-flat we shall call the *U-associated flat,* where

$$U = \lambda_1 U_1 + \lambda_2 U_2 + \cdots + \lambda_k U_k\ .$$

The set $\Omega_1(U)$ corresponding to U is then the union of the sets $\Omega(y_1\ ,\ y_2\ ,\ \cdots\ ,\ y_k)$ associated with those points $(y_1\ ,\ y_2\ ,\ \cdots\ ,\ y_k)$ of $PG(k - 1,\ 2)$ which do not lie on the U-associated flat. We shall call such points *U-associated points.* Hence, from (15)

$$(17)\qquad w(U) = \text{the number of } U\text{-associated points in } \Omega.$$

This result is a special application of a property studied in another connection by Bose and Burton in [3].

As is clear in all the preceding discussion, the ordering of the points in Ω is completely immaterial. However, for notational convenience, and to fix ideas, we shall ordinarily take $Y_1\ ,\ Y_2\ ,\ \cdots\ ,\ Y_n = P_{11}\ ,\ P_{12}\ ,\ \cdots\ ,\ P_{1n_1},\ P_{21}\ ,\ P_{22}\ ,\ \cdots\ ,\ P_{2n_2}\ ,\ \cdots\ ,\ P_{\mu 1}\ ,\ P_{\mu 2}\ ,\ \cdots\ ,\ P_{\mu n_\mu}$. The subset $(P_{i1}\ ,\ P_{i2}\ ,\ \cdots\ ,\ P_{in_i})$ may be represented by $P_i^{n_i}$; it must be understood to be empty when $n_i = 0$. The correspondence between the points of Ω and the generating letters $U_1\ ,\ U_2\ ,\ \cdots\ ,\ U_k$ of the alphabet can be exhibited in the following array.

	Letter	Ω-point													
		P_{11}	P_{12}	$\cdots$	P_{1n_1}	P_{21}	P_{22}	$\cdots$	P_{2n_2}	$\cdots$	$P_{\mu 1}$	$P_{\mu 2}$	$\cdots$	$P_{\mu n_\mu}$
	U_1	y_{11}	y_{11}	$\cdots$	y_{11}	y_{12}	y_{12}	$\cdots$	y_{12}	$\cdots$	$y_{1\mu}$	$y_{1\mu}$	$\cdots$	$y_{1\mu}$
(18)	U_2	y_{21}	y_{21}	$\cdots$	y_{21}	y_{22}	y_{22}	$\cdots$	y_{22}	$\cdots$	$y_{2\mu}$	$y_{2\mu}$	$\cdots$	$y_{2\mu}$
	U_3	y_{31}	y_{31}	$\cdots$	y_{31}	y_{32}	y_{32}	$\cdots$	y_{32}	$\cdots$	$y_{3\mu}$	$y_{3\mu}$	$\cdots$	$y_{3\mu}$
	.	.	.	...	.	.	.	...	.	...	.	.	...	.
	.	.	.	...	.	.	.	...	.	...	.	.	...	.
	.	.	.	...	.	.	.	...	.	...	.	.	...	.
	U_k	y_{k1}	y_{k1}	$\cdots$	y_{k1}	y_{k2}	y_{k2}	$\cdots$	y^{32}	$\cdots$	$y_{k\mu}$	$y_{k\mu}$	$\cdots$	$y_{k\mu}$

This is precisely the array (10) with respect to the U's. Each U is given by a horizontal sequence of n digits. But now we can see the columns of the array as the sets of homogeneous coordinates of points in $PG(k - 1,\ 2)$. Thus, $U_1\ ,\ U_2\ ,\ \cdots\ ,\ U_k$, and hence all the letters of the alphabet, are completely defined by the ordered set of Ω-points. Hence the study of group alphabets can be pursued through the study of sets Ω composed of points of $PG(k - 1,\ 2)$.

We should call attention at this point to the correspondence between our geometric representation and the group representation of Slepian. Slepian [14] employs the isomorphism of B_n, the group of n-place binary sequences under the operation of addition modulo 2, with the abstract group C_n generated by n commuting elements of order 2, together with the isomorphism of the (n, k)-alphabet (subgroup of B_n of order 2^k) with C_k. Rows 2 through $(k + 1)$ of Slepian's *modular representation table* for the group C_k give, columnwise, precisely the homogeneous coordinates of the points P_i of $PG(k - 1, 2)$. When Slepian forms an (n, k)-alphabet by choosing n columns (including possible repetitions) of the modular representation table, the rows 2 through $(k + 1)$ of the resulting array is, to within possible permutation of columns, precisely our representation of Ω. Our measure n_β for the point P_β is Slepian's quantity d_β, both indicating the number of times the β-set of coordinates is taken from $PG(k - 1, 2)$, or from the modular representation table, for forming the (n, k)-alphabet.

Obviously, if P_{iu} is outside $\lambda_1 y_1 + \lambda_2 y_2 + \cdots + \lambda_k y_k = 0$ for *any* u, it is outside the flat for *all* u. That is, *all* repetitions of P_i in Ω are U-associated points. On any $(k - 2)$-flat in $PG(k - 1, 2)$ there are $2^{k-1} - 1$ points, so that there are $(2^k - 1) - (2^{k-1} - 1) = 2^{k-1}$ points of $PG(k - 1, 2)$ lying *outside* the flat. Hence the letter $U = \lambda_1 U_1 + \lambda_2 U_2 + \cdots + \lambda_k U_k$ is uniquely defined by the Ω-points contributed by the 2^{k-1} geometric points lying outside

$$\lambda_1 y_1 + \lambda_2 y_2 + \cdots + \lambda_k y_k = 0$$

in $PG(k - 1, 2)$. As suggested in the remark preceding (18), we shall use exponent notation to indicate multiplicity, setting

$$U = P_{i_1}^{n_{i_1}} P_{i_2}^{n_{i_2}} \cdots P_{i_\eta}^{n_{i_\eta}}, \qquad \eta = 2^{k-1}. \tag{19}$$

The order of the P_i's in (19) is clearly of no importance, nor are the exponents essential, since the symbol P_i by itself specifies that U has unities in those positions occupied by $P_{i1}, P_{i2}, \cdots, P_{in_i}$ in the ordered sequence of Ω-points $Y_1, Y_2, \cdots, Y_n$. Thus there is a (1,1) correspondence between a letter

$$U = \lambda_1 U_1 + \lambda_2 U_2 + \cdots + \lambda_k U_k$$

and the set of geometric points

$$(P_{i_1} P_{i_2} \cdots P_{i_\eta}) \tag{20}$$

which lie outside the $(k - 2)$*-flat* $\lambda_1 y_1 + \lambda_2 y_2 + \cdots + \lambda_k y_k = 0$.

Let $\bar{S}$ represent the complement of the set S with respect to the entire space, here $PG(k - 1, 2)$. From (20) we have the useful correspondences:

$$\text{(21)}\quad \begin{cases} U\colon \{P_{i_1}, P_{i_2}, \cdots, P_{i_\eta}, \text{ lying } \textit{outside } \lambda_1 y_1 + \lambda_2 y_2 + \cdots + \lambda_k y_k = 0\}, \\ \bar{U}\colon \{P_i \text{ lying } \textit{on } \lambda_1 y_1 + \lambda_2 y_2 + \cdots + \lambda_k y_k = 0\} \\ \qquad \textit{or simply } \lambda_1 y_1 + \lambda_2 y_2 + \cdots + \lambda_k y_k = 0. \end{cases}$$

The letter U can thus be viewed in any one of the following ways.

(i) *U is a sequence of n binary digits.* As such, U is an element of the ring algebra introduced in Section 2.

(ii) *U is the set $\Omega_1(U)$ of U-associated points in Ω.* As such, U is given by (19).

(iii) *U is the set of geometric points of $PG(k - 1, 2)$ lying outside the U-asso-*

ciated flat. In this view, the multiplicity n_i is understood as attached to the point P_i, and U is expressed by (20).

For example of this geometry, we shall consider again the alphabet in (2). Here $k = 3, n = 5, PG(k - 1, 2)$ is the projective plane $PG(2, 2)$, and $(k - 2)$-flats are lines. The situation is presented in Figure 1.

$$\begin{array}{llll}
\bar{U}_1 : y_1 = 0, & & \bar{U}_4 : y_1 + y_2 = 0, \\
\bar{U}_2 : y_2 = 0, & & \bar{U}_5 : y_1 + y_3 = 0, \\
\bar{U}_3 : y_3 = 0, & & \bar{U}_6 : y_2 + y_3 = 0, \\
 & & \bar{U}_7 : y_1 + y_2 + y_3 = 0.
\end{array}$$

One alphabet design assigns measures $n(P_i) = n_i$ to the points P_i as shown in the following table. The subsets of associated Ω-points are then as indicated.

Geometric points:	P_1	P_2	P_3	P_4	P_5	P_6	P_7
$n(P_i)$:	0	2	0	1	1	0	1
Associated subsets of Ω:	null	Y_1, Y_2	null	Y_3	Y_4	null	Y_5

Taking points of Ω in column form, as in (18), we have

$$\begin{array}{rccccc}
\text{Positions:} & Y_1 & Y_2 & Y_3 & Y_4 & Y_5 \\
\text{Geometric points:} & P_{21} & P_{22} & P_{41} & P_{51} & P_{71} \\
\Omega: & \multicolumn{5}{l}{\left\{\begin{array}{ccccc} 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{array}\right.}
\end{array}$$

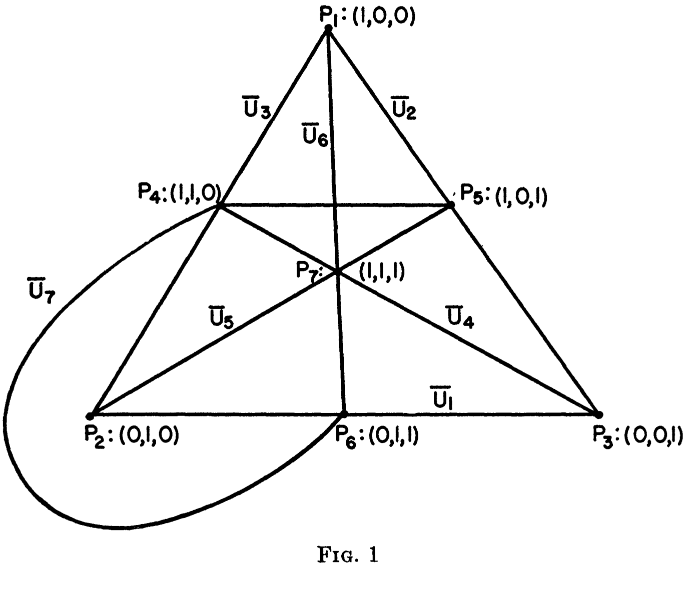

FIG. 1

Then

$$U_1 = (00111), \qquad U_2 = (11101), \qquad U_3 = (00011),$$

and the alphabet follows as in (12). The various identifications of the letters are as follows.

	Letter $U = \lambda_1 U_1 + \lambda_2 U_2 + \lambda_3 U_3$	Binary sequence	Set of geometric points	Set of associated Ω-points
	$U_1 = 1(U_1) + 0(U_2) + 0(U_3)$	(00111)	$(P_1P_4P_5P_7)$	$P_1^0P_4^1P_5^1P_7^1$
	$U_2 = 0(U_1) + 1(U_2) + 0(U_3)$	(11101)	$(P_2P_4P_6P_7)$	$P_2^2P_4^1P_6^0P_7^1$
	$U_3 = 0(U_1) + 0(U_2) + 1(U_3)$	(00011)	$(P_3P_5P_6P_7)$	$P_3^0P_5^1P_6^0P_7^1$
(22)	$U_4 = 1(U_1) + 1(U_2) + 0(U_3)$	(11010)	$(P_1P_2P_5P_6)$	$P_1^0P_2^2P_5^1P_6^0$
	$U_5 = 1(U_1) + 0(U_2) + 1(U_3)$	(00010)	$(P_1P_3P_4P_6)$	$P_1^0P_3^0P_4^1P_6^0$
	$U_6 = 0(U_1) + 1(U_2) + 1(U_3)$	(11110)	$(P_2P_3P_4P_5)$	$P_2^2P_3^0P_4^1P_5^1$
	$U_7 = 1(U_1) + 1(U_2) + 1(U_3)$	(11001)	$(P_1P_2P_3P_7)$	$P_1^0P_2^2P_3^0P_7^1$

To reiterate the meaning of the exponent notation relating to Ω-points, we note the example

$$U_4 = P_1^0P_2^2P_5^1P_6^0 = P_{21}P_{22}P_{51} .$$

Consider now the binary sequences which are not letters, that is, the sequences which are members of cosets. As we saw when the Ω-set was introduced, *every* binary sequence is in correspondence with a subset of Ω. Hence each nonletter can be identified with a subset of Ω-points; as in the case of letters, we shall call the points of such a subset the *associated* points of the sequence. But the Ω-set corresponding to a nonletter does not *necessarily* include all n_i repetitions of P_i as in the case of a letter U. Thus, for example, in the array (2), $L = (10000) = P_{21}$, or again, $L + U_6 = (10000) + (11110) = (01110) = P_{22}P_{41}P_{51}$. Hence, in general the binary sequences which are not letters can not be identified with sets of *geometric* points as can the letters. Of course there will be special cases in which the Ω-subset defining a nonletter will contain all n_i repetitions of P_i for all i in the subset, and indeed these special cases as they affect coset leaders L are of particular importance in design investigations.

Some observations should be made on the relation between operations performed in the algebra of binary sequences and operations performed on corresponding sets. By the definition of multiplication (5), T_iT_j has unities in just those positions which are occupied by unities in *both* T_i and T_j. Hence T_iT_j is defined by the subset of Ω-points associated with both T_i and T_j. Thus, *when regarded as sets of Ω-points,*

$$(23) \qquad T_iT_j = T_i \cap T_j .$$

By the definition of addition (4), $T_i + T_j$ has unities in those positions occupied by unities in *one of T_i and T_j but not in both.* Hence $T_i + T_j$ is defined by those associated points of T_i and T_j which are not common. Thus, regarded as sets of Ω-points,

$$T_i + T_j = T_i \cup T_j - \{T_i \cap T_j\}. \tag{24}$$

When each member of the pair T_i, T_j is a sequence whose set of associated Ω-points includes $P_{i1}, P_{i2}, \cdots, P_{in_i}$ whenever it includes any P_{iu} [such sequences are the letters U and the special cases of nonletters mentioned above], then (23) and (24) apply with the sequences regarded as sets of *geometric* points (P_i).

4. Geometric conditions in a group alphabet. As shown in the preceding section, the construction of a binary signaling (n, k)-alphabet is equivalent to the selection of a set Ω of n points from $PG(k - 1, 2)$, the geometric point P_i appearing n_i times in Ω. The selection of Ω is in turn equivalent to the distribution of a total measure n over the points of $PG(k - 1, 2)$, whereby the nonnegative integral measure $n(P_i) = n_i$ is attached to the point P_i,

$$\sum_{i=1}^{\mu} n_i = n, \qquad \mu = 2^k - 1. \tag{25}$$

We define the *n-measure N_j of the j-th $(k - 2)$-flat* U_j of $PG(k - 1, 2)$ as

$$N_j = \sum_{\bar{U}_j} n_i, \qquad j = 1, 2, \cdots, \mu, \tag{26}$$

where $\sum_{\bar{U}_j}$ indicates summation over the points P_i which lie on $\bar{U}_j$. Since every point of $PG(k - 1, 2)$ is on $2^{k-1} - 1$ $(k - 2)$-flats, summing (26) on j gives

$$\sum_j N_j = (2^{k-1} - 1)n. \tag{27}$$

Consider now any point P_i. Any point of the space other than P_i determines with P_i a line, and there are as many $(k - 2)$-flats "on" a line as there are points on a $(k - 3)$-flat [by duality], namely, $2^{k-2} - 1$. Hence each point of the space other than P_i lies on $2^{k-2} - 1$ of the $(k - 2)$-flats passing through P_i. Thus, if we sum (26) over the $(k - 2)$-flats containing P_i, we obtain

$$\begin{aligned}\sum_{P_i} N_j &= (2^{k-1} - 1)n_i + (2^{k-2} - 1)(n - n_i) \\ &= (2^{k-2} - 1)n + 2^{k-2}n_i, \qquad i = 1, 2, \cdots, \mu,\end{aligned} \tag{28}$$

where $\sum_{P_i}$ indicates summation over those j indexing the $(k - 2)$-flats which pass through P_i.

We shall call the space of the points P_i and $(k - 2)$-flats $\bar{U}_j$ the *primary space*. Corresponding to this primary space is the *dual space*, in which the point Υ_j corresponds to the $(k - 2)$-flat $\bar{U}_j$ of the primary space, and the $(k - 2)$-flat π_i corresponds to the point P_i of the primary space. Each space is a projective space $PG(k - 1, 2)$. In the dual space we define a *w-measure* which assigns to the point Υ_j the integer w_j, where

$$(29) \qquad w_j = n - N_j, \qquad j = 1, 2, \cdots, \mu.$$

By (19), the weight $w(U_j)$ of the letter U_j is $n_{i_1} + n_{i_2} + \cdots + n_{i_\eta}$ $(\eta = 2^{k-1})$, the sum of the n-measures of all points P_i lying outside $\bar{U}_j$. Hence,

$$(30) \qquad w(U_j) = n - N_j = w_j, \qquad j = 1, 2, \cdots, \mu.$$

That is, the w-measure of a point Υ in the dual space is the weight $w(U)$ of the letter whose associated flat $\bar{U}$ in the primary space is the dual of Υ. If we sum (30) on j, applying (27), we obtain

$$(31) \qquad \sum_{j=1}^{\mu} w(U_j) = \sum_{j=1}^{\mu} w_j = (2^k - 1)n - (2^{k-1} - 1)n = 2^{k-1}n.$$

This is Slepian's Proposition 6 [14].

Since the distribution of the measure n assigns nonnegative integers to the $\mu = 2^k - 1$ points of the primary space, it is convenient to express n as $\mu t + \gamma$, and set $n_i = t + \delta_i (\delta_i \geqq -t)$. Taking into account that $n \geqq k$, we have

$$(32) \qquad n = (2^k - 1)t + \gamma,$$

where t is a positive integer or zero, and

$$\gamma = \sum_{i=1}^{\mu} \delta_i = \begin{cases} -1, 0, 1, \cdots, k, k+1, \cdots, 2^k - 3 & \text{if } t > 0, \\ \qquad\qquad k, k+1, \cdots, 2^k - 3 & \text{if } t = 0. \end{cases}$$

This representation has the advantage that, for given k, it reduces the problem of constructing (n, k)-alphabets for all n to the problem of constructing $2^k - 1$ γ-*classes* of (n, k)-alphabets.

Since to each letter U there correspond 2^{k-1} points of the primary space [cf. (19), (20)], the weight $w(U_j)$ of U_j is of the form

$$(33) \qquad w(U_j) = 2^{k-1}t + b_j,$$

where b_j is the sum of the δ_i's over the points corresponding to U_j.

Now, an essential feature of the code associated with an (n, k)-alphabet is the following. When the letter U is transmitted, the detector will correctly report U if and only if the errors in transmission occur in precisely those positions occupied by unity in a coset leader L. Hence, if all possible n-place sequences containing s unities serve as coset leaders, then the code will *correct all* s-tuple errors. If the number of weight-s sequences occurring as coset leaders is less than $\binom{n}{s}$, say α, then the code corrects α s-tuple errors. The advantage of maximizing the number of lowest-weight sequences serving as coset leaders, discussed in Section 1 with reference to maximizing the probability of correct detection, now appears again, this time with reference to maximizing the number W such that *all* W-tuple (and lower order multiple) errors are corrected by the code.

As shown in Section 3, every n-place sequence, whether letter U, coset leader L, or interior coset member $L + U$, is identified by certain Ω-points associated with the sequence. Since addition is modulo 2, the binary sequence $L + U$ contains a zero in each position identified with an Ω-point which is an associated point of *both* L and U. If $w(L) = g$, there are g Ω-points associated with L. The class of Ω-subsets representing all possible sequences of weight g embraces all possible combinations of g points out of the n Ω-points, including any set of g Ω-points associated with a letter U. Now, *all* weight-g sequences can be coset leaders if and only if $w(L + U) > w(L)$ for all U's and all weight-g L's. Hence, in order that all weight-g sequences can serve as coset leaders, it is necessary and sufficient that $g < \frac{1}{2}w(U_j)$ for all j. Define

(34) W = the largest integer such that all sequences of weight $\leqq W$ can serve as coset leaders.

Then W is the largest integer such that there exists an (n, k)-alphabet in which $w(U_j) > 2W$ for all j, whence the well-known condition $w(U_j) \geqq 2W + 1$ for all j. Considering the form (33) of $w(U_j)$, we set

$$W = 2^{k-2}t + e, \tag{35}$$

where e *is the largest integer such that there exists an* (n, k)*-alphabet in which*

$$w(U_j) \geqq 2W + 1 = 2^{k-1}t + 2e + 1 \quad \text{for all } j. \tag{36}$$

For given k, γ, and e, we confine our attention to the construction of only those (n, k)-alphabets which satisfy (36), that is, (n, k)-alphabets which provide W-error-correcting codes. Such codes have been termed *largest-nearest-neighbor-distance* group codes. There has been no demonstration that this class includes that code which has the smallest probability of incorrect decoding for all values of $p < 1/2$, but the class does include such a code for sufficiently small values of p, and the class has the desirable feature of maximizing the multiplicity of error which will be completely corrected. For such an alphabet, the w-measure in the dual space must, in view of (30), satisfy

$$w_j \geqq 2W + 1 \quad \text{for all } j. \tag{37}$$

Set

$$w_j = 2W + 1 + d_j, \tag{38}$$

where d_j *is a positive integer or zero.* We now define as *D-measure* a measure which assigns nonnegative integers d_j to the points Υ_j of the dual space. (It will be unambiguous to refer to an individual d_j as the D-measure of the point Υ_j, and to the sum of the d_j's for all points on a c-flat σ_c as the D-measure of σ_c.) Since (37) is sufficient as well as necessary for an (n, k)-alphabet to give a W-

error-correcting code, provided the w-measure is otherwise consistent with an (n, k)-alphabet, it follows that any D-measure which is consistent with an (n, k)-alphabet will provide a sufficient condition for the alphabet to give a W-error-correcting code. The conditions on the D-measure are readily identified.

First, if we sum (38) on j, applying (31), (32), and (35), we have

$$2^{k-1}n = (2^k - 1)(2W + 1) + \sum_j d_j,$$

$$2^{k-1}[(2^k - 1)t + \gamma] = (2^k - 1)(2^{k-1}t + 2e + 1) + \sum_j d_j,$$

$$\sum_j d_j = 2^{k-1}\gamma - (2^k - 1)(2e + 1). \tag{39}$$

Next, if we sum (29) over those j which index the points Υ_j lying on that $(k - 2)$-flat π_i which is the dual of the point P_i of the primary space, we obtain

$$\sum_{\pi_i} w_j = (2^{k-1} - 1)n - \sum_{P_i} N_j,$$

where $\sum_\xi$ indicates summation over those j indexing the elements which are "on" ξ. Then by (38), (28), (35), and (32) we have

$$(2^{k-1} - 1)(2W + 1) + \sum_{\pi_i} d_j = (2^{k-1} - 1)n - (2^{k-2} - 1)n - 2^{k-2}n_i,$$

$$(2^{k-1} - 1)(2^{k-1}t + 2e + 1) + \sum_{\pi_i} d_j = 2^{k-2}[(2^k - 1)t + \gamma] - 2^{k-2}n_i,$$

$$n_i = t + \gamma - 2(2e + 1) - (1/2^{k-2})\,[\sum_{\pi_i} d_j - (2e + 1)]. \tag{40}$$

Since n_i, t, γ, and e are integral for all i, (40) shows that

$$\sum_{\pi_i} d_j \equiv 2e + 1 \pmod{2^{k-2}} \quad \text{for all } i. \tag{41}$$

For defining uniquely an n-measure over the points P_i of the primary space, the equalities (39) and (40) are clearly sufficient as well as necessary, provided that all the n_i given by (40) are integral and nonnegative. We have thus established the following theorem.

THEOREM 4. *Given any k, γ, and e, where γ and e are functions of n in accordante with* (32) *and* (35), *respectively, the necessary and sufficient conditions that a D-measure uniquely define a γ-class of n-measures over the points P_i of $PG(k - 1, 2)$, and thence define, uniquely to within ordering of Ω-points, a γ-class of (n, k)-alphabets which give W-error-correcting codes (where W is the largest integer for which an (n, k)-alphabet exists) are*

$$\sum_{j=1}^{\mu} d_j = 2^{k-1}\gamma - (2^k - 1)(2e + 1), \qquad \mu = 2^k - 1, \tag{1}$$

$$\sum_{\pi_i} d_j \equiv 2e + 1 \pmod{2^{k-2}} \quad \text{for all } i, \tag{2}$$

(3) $\qquad n_i \geqq 0 \quad \text{for all } i,$

where n_i *is given by* (40).

If Theorem 4 is restated in terms of n, W, and the w-measure, it is the equivalent of Slepian's statement at the end of Section 2.9 of [14]. Similarly, such restatement of Theorem 6, below, taken in conjunction with Corollary 5.1, is the equivalent of Slepian's Proposition 7. In addition to giving unity to the geometric approach and providing tools for later geometric work, the present propositions, for any fixed k, organize matters relating to an infinite number of n-values into just $2^k - 1$ γ-classes.

The congruence condition in Theorem 4 is a special case of a more general property given by the following theorem.

THEOREM 5. *Any D-measure satisfying Theorem* 4 *has the property*

$$\sum_{\sigma_c} d_j \equiv 2e + 1 \pmod{2^c} \tag{42}$$

for all *c-flats* σ_c *in the dual space* $PG(k-1, 2)$, $c = 1, 2, \cdots, k-1$.

PROOF. For $c = k - 1$, the congruence follows at once from condition (1) in Theorem 4. Now consider any c-flat σ_c in the dual space, $c = 1, 2, \cdots, k - 2$. Summing (38) over the points which lie on σ_c, we have

$$\begin{aligned}\sum_{\sigma_c} w_j &= (2^{c+1} - 1)(2W + 1) + \sum_{\sigma_c} d_j \\ &= (2^{c+1} - 1)(2^{k-1}t + 2e + 1) + \sum_{\sigma_c} d_j\end{aligned}$$

by virtue of (35). Thus, since $c \leqq k - 2$,

$$\sum_{\sigma_c} d_j \equiv (2e + 1) + \sum_{\sigma_c} w_j \pmod{2^c}. \tag{43}$$

Now, if we designate by S_{k-2-c} the flat, of dimension $k - 2 - c$, which in the primary space is the dual of σ_c, we have from (29)

$$\sum_{\sigma_c} w_j = (2^{c+1} - 1)n - \sum_{S_{k-2-c}} N_j. \tag{44}$$

The number of $(k - 2)$-flats which are "on" (pass through) S_{k-2-c} is by duality the same as the number of points on a c-flat, namely $2^{c+1} - 1$. Each of these $(k - 2)$-flats contains all the points of S_{k-2-c}. Further, any point outside S_{k-2-c} determines with S_{k-2-c} a $(k - 1 - c)$flat, through which pass $2^c - 1$ $(k - 2)$-flats; that is, every point of $PG(k - 1, 2)$ which is not on S_{k-2-c} is on $2^c - 1$ of the $(k - 2)$-flats which pass through S_{k-2-c}. Hence

$$\begin{aligned}\sum_{S_{k-2-c}} N_j &= (2^{c+1} - 1) \sum_{S_{k-2-c}} n_i + (2^c - 1)(n - \sum_{S_{k-2-c}} n_i) \\ &= (2^c - 1)n + 2^c \sum_{S_{k-2-c}} n_i,\end{aligned}$$

giving in (44)

$$\sum_{\sigma_c} w_j = 2^c[n - \sum_{S_{k-2-c}} n_i],$$

whence, since n and all n_i's are integral,

$$\sum_{\sigma_c} w_j \equiv 0 \pmod{2^c}.$$

This result applied to (43) gives the congruence stated in the theorem.

The congruence condition in Theorem 4 is the special case $c = k - 2$. Another special case of particular importance is given in the following corollary, taking $c = 1$.

COROLLARY 5.1. *For any D-measure satisfying Theorem* 4, *the D-measure of every line in the dual space is odd.*

The means of satisfying Corollary 5.1 are given by the following theorem.

THEOREM 6. *A necessary and sufficient condition that a D-measure assigning nonnegative integers d_j to the points Υ_j of $PG(k - 1, 2)$, $k \geqq 2$, shall be such that the D-measure of every line is odd is that either every point of the space has odd D-measure, or every point of one $(k - 2)$-flat π^* has odd D-measure while all points outside π^* have even D-measure.*

PROOF. I. *Sufficiency.* Suppose there is associated with the j-th point of

$$PG(k - 1, 2)$$

the measure d_j, $j = 1, 2, \cdots, \mu$, such that d_j is a positive integer or zero. If all the d_j are odd, then clearly the sum of the measures of the three points on any line is odd. If the d_j's associated with the points of a specified $(k - 2)$-flat π^* are odd, while all the remaining d_j's are even, then the situation is as follows. All the lines lying wholly within π^* are clearly of odd total point measure. Any line not lying wholly within π^* contains one point of π^* and two points outside π^*; since both the latter points are of even measure, the total point measure of the line is odd.

II. *Necessity.* Suppose that the measures d_j have been assigned to the μ points of $PG(k - 1, 2)$ so that each point measure d_j is a positive integer or zero, and the sum of the measures of the three points on any line is odd. Consider first the case $k = 2$. We are then dealing with the projective line $PG(1, 2)$, in which $(k - 2)$-flats are points. There is just one line in the space, and that line by hypothesis has odd D-measure. Obviously, either d_1, d_2, and d_3 are all odd, or one of these d_j's is odd and the remaining two are even. Hence, the conclusion stated in the theorem holds when $k = 2$.

Let us now *assume* that the stated conclusion follows from the hypothesis when $k = u$, where u is any integer equal to or greater than 2. That is, given that every line in $PG(u - 1, 2)$ has odd D-measure, either all the points of $(u - 1)$-space have odd D-measure or the points of a specified $(u - 2)$-flat have odd D-measure while all the remaining points of the space have even D-measure. For ease of reference, we shall call a point *odd* or *even* according as its D-measure is odd or even.

Consider now a projective u-space $PG(u, 2)$ satisfying the hypothesis. Then by our assumption concerning the nature of the measure in $(u - 1)$-space, every $(u - 1)$-flat in $PG(u, 2)$ is of one of two kinds:

first kind: all points are odd,

second kind: all the points of one $(u - 2)$-flat are odd, and all the remaining points of the $(u - 1)$-flat are even.

Hence in any $(u - 1)$-flat of the u-space there is at least one $(u - 2)$-flat containing only odd points. Take such a $(u - 2)$-flat, say Σ, and consider the three $(u - 1)$-flats passing through it, say ψ_1, ψ_2, ψ_3, keeping in mind that these three $(u - 1)$-flats exhaust the u-space of points. Take a line m which does not intersect Σ. That such choice is possible is seen from the following lemma.

Lemma 6.1. *In $PG(u, 2)$ there are 2^{2u-2} lines which do not intersect an arbitrary $(u - 2)$-flat Σ.*

Proof of Lemma. There are $2^{u-1} - 1$ points in Σ. Through any one of these points there pass $2^u - 1$ lines of $PG(u, 2)$. The number of these which lie entirely in Σ is the number of lines passing through a point in $(u - 2)$-space, namely $2^{u-2} - 1$. Also, the total number of lines in $PG(\alpha, 2)$ is [1],

$$(2^{\alpha+1} - 1)(2^\alpha - 1)/(2^2 - 1)(2^1 - 1) = \tfrac{1}{3}(2^{\alpha+1} - 1)(2^\alpha - 1).$$

Hence, the number of lines intersecting Σ, including those which lie wholly within Σ, is $(2^{u-1} - 1)[(2^u - 1) - (2^{u-2} - 1)] + \tfrac{1}{3}(2^{u-1} - 1)(2^{u-2} - 1) = \tfrac{1}{3}(2^{u-1} - 1)(2^{u+1} + 2^{u-1} - 1)$. Thus, since the total number of lines in $PG(u, 2)$ is $\tfrac{1}{3}(2^{u+1} - 1)(2^u - 1)$, the number of lines which do not intersect Σ is

$$\tfrac{1}{3}(2^{u+1} - 1)(2^u - 1) - \tfrac{1}{3}(2^{u-1} - 1)(2^{u+1} + 2^{u-1} - 1) = 2^{2u-2}.$$

This establishes the lemma.

The line m will intersect each of ψ_1, ψ_2, ψ_3 in a point. Say these points are P_1, P_2, P_3, respectively.

(i) If m is of the first kind, P_1, P_2, and P_3 are all odd, so that, since all the points of Σ are odd, each of ψ_1, ψ_2, ψ_3 must be of the first kind, whence all the points of $PG(u, 2)$ are odd.

(ii) If m is of the second kind—say P_1 is odd and P_2, P_3 even—then ψ_1 is of the first kind and ψ_2, ψ_3 are of the second kind, whence all the points of $PG(u, 2)$ lying on ψ_1 are odd and all the remaining points of $PG(u, 2)$ are even.

Thus, either all the d_j's are odd, or the d_j's associated with the points of one $(u - 1)$-flat are odd and the remaining d_j's are even.

Hence, the stated conclusion follows from the hypothesis when $k = u + 1$ provided the same is true for $k = u$. Since we determined at the outset that the implication holds when $k = 2$, the same result for any integral $k \geqq 2$ follows at once by induction.

5. Determination of W. When k is fixed, W—the largest integer such that all sequences of weight $\leqq W$ can serve as coset leaders—is a function of n. We may write $W = W_k(n)$, where the subscript k indicates the size (2^k) of the group alphabet. There is also the inverse function $n = W_k^{-1}(W)$.

THEOREM 7. *For a given k, $W = W_k(n)$ is a monotonically nondecreasing function of n, specifically*

$$W_k(n) \leqq W_k(n+1) \leqq W_k(n) + 1, \tag{45}$$

and $n = W_k^{-1}(W)$ is a monotonically increasing function of W.

PROOF. Given $W = W_k(n)$, there exists an n-measure over the points of $PG(k-1, 2)$ such that $w(U_j) \geqq 2W + 1$ for all letters U_j, that is, such that the points lying outside any $(k-2)$-flat have total n-measure equal to or greater than $2W + 1$. When n is changed to $n + 1$, we may amend the original n-measure by simply adding 1 to the n-measure of any one particular point, say P. Then clearly the total measure of the points lying outside any $(k-2)$-flat is not reduced. Indeed, such measure remains the same for every set of points lying outside a flat which contains P, and increases by 1 for every set of points lying outside a flat which does not contain P. Thus, the weight of every letter U_j of the alphabet is at least as large as it was under the original measure, so that $W_k(n+1) \geqq W_k(n)$. The two-sided bound (45) states that the jump in value of $W_k(n)$ cannot be greater than one for a unit increase in n. We may establish this by considering the contrary. For that purpose, assume

$$W_k(n) = W \tag{46}$$

and

$$W_k(n+1) = W + c, \qquad c \geqq 2. \tag{47}$$

Then by (47) we can distribute a total measure $n + 1$ over the points of

$$PG(k-1, 2)$$

in such a way that the n-measure of the set of points outside any $(k-2)$-flat is at least $2(W + c) + 1 = 2W + 2c + 1$, where $2c + 1 \geqq 5$. If now we choose any one point P having nonzero n-measure, and reduce its measure by unity, we shall have a total measure n distributed over the points of $PG(k-1, 2)$ in such manner that the total measure of the set of points outside any $(k-2)$-flat which contains P is at least $2W + 2c + 1$ and the total measure of the set of points outside any $(k-2)$-flat which does not contain P is at least $2W + 2c$. Hence, for *all* letters U_j of the alphabet, $w(U_j) \geqq 2W + 2c \geqq 2W + 4 > 2(W + 1) + 1$, so that $W_k(n) \geqq W + 1$, contradicting (46).

When $n = k$, the array of alphabet and cosets consists of the alphabet alone, so that there is just the single coset leader $I = (000 \cdots 0)$, whence $W = 0$. As n increases in steps of one, W either stays constant or increases by unity. This step-function nature of $W = W_k(n)$ shows that n is a monotonically increasing function of W.

Corresponding to a given W there are in general more than one value of n. The smallest n corresponding to a given W is a definite function of W, namely, the smallest value of $W_k^{-1}(W)$. We shall call this value $n_k(W)$. Then $n_k(W)$ is a single-valued monotonically increasing function of W. Theorem 7 shows that, for fixed k, the problem of finding W for given n is completely equivalent to the problem of finding $n_k(W)$ for given W, that is, the minimum value of n for which $W_k(n) = W$. Further, by considering n and W in the forms (32) and (35), respectively, one can treat the matter in terms of γ-classes.

Taking W in the form (35), $W = 2^{k-2}t + e$, let us consider the case $e = -1$ for the general value (32) of n: $n = (2^k - 1)t + \gamma$, where now $t > 0$ (since W must be nonnegative) and $-1 \leqq \gamma \leqq 2^k - 3$. For $e = -1$, $W = 2^{k-2}t - 1$, and an (n, k)-alphabet will allow all sequences of weight $\leqq W$ to serve as coset leaders if and only if

$$(48) \qquad w(U_j) \geqq 2W + 1 = 2^{k-1}t - 1 \quad \text{for all } j.$$

Let us now define an n-measure over the points of the primary space as follows.

(i) If $\gamma = -1$,

$$(49) \qquad n_i = \begin{cases} t & \text{for all } i \text{ except one, say } i_0, \\ t - 1 & \text{for } i = i_0. \end{cases}$$

(ii) If $0 \leqq \gamma \leqq 2^k - 3$,

$$(50) \qquad n_i = \begin{cases} t + 1 & \text{for } \gamma \text{ distinct points } P_{i_1}, P_{i_2}, \cdots, P_{i_\gamma}, \\ t & \text{for each of the remaining points of the space.} \end{cases}$$

Since by (20) a letter U is identified with 2^{k-1} points of the primary space, the n-measure (i) gives $W(U_j) \geqq (t - 1) + (2^{k-1} - 1)t = 2^{k-1}t - 1$ for all j, and the n-measure (ii) gives $w(U_j) \geqq 2^{k-1}t$ for all j, thus satisfying (48) in each instance. Hence, for any value of n, k, the value (-1) can be attained for e. That is,

$$(51) \qquad e \geqq -1 \text{ for all } n, k.$$

Now whenever (36) holds, then necessarily

$$\sum_{j=1}^{\mu} w(U_j) \geqq (2^k - 1)(2^{k-1}t + 2e + 1),$$

whence, by (31) and (32), and taking (51) into account, we have

$$(52) \qquad -1 \leqq e \leqq \left[\frac{2^{k-1}\gamma - 2^k + 1}{2(2^k - 1)}\right],$$

where $[x]$ has its usual meaning "greatest integer not exceeding x." In terms of n, the upper bound in (52) is already well known (cf., for example, Weinitschke [15] and MacDonald [12]); the refinement given by (59) below appears to be new.

Since $\gamma \leqq 2^k - 3$, the quantity within brackets in (52) is bounded above by $2^{k-2} - 1 - 1/(2^{k+1} - 2)$, whence the most general boundary statement for e is

$$(53) \qquad -1 \leqq e \leqq 2^{k-2} - 2.$$

Applying (53) to (35), we have $W + 1 = 2^{k-2}t + (e + 1), 0 \leqq (e + 1) \leqq 2^{k-2} - 1$, so that

$$t = \left[\frac{W + 1}{2^{k-2}}\right]$$

is a well-defined single-valued function of W. Similarly, the bounds on γ in (32) show that

$$t = \left[\frac{n + 1}{2^k - 1}\right]$$

is a well-defined single-valued function of n. Moreover, if $W_k(n) = W$,

$$\left[\frac{n + 1}{2^k - 1}\right] = t = \left[\frac{W + 1}{2^{k-2}}\right]. \tag{54}$$

Thus, for fixed k, the problem of finding W for given n has the equivalent forms:

(i) given n, to find $W = W_k(n)$;

(ii) given γ, to find $e = W_k((2^k - 1)t + \gamma) - 2^{k-2}t = e_k(\gamma)$, say;

(iii) given W, to find $n = n_k(W) =$ smallest value of n for which $W_k(n) = W$;

(iv) given e, to find $\gamma = \gamma_k(e) =$ smallest value of γ for which $e_k(\gamma) = e$.

One general result for all k follows immediately from the demonstration relating to the n-measure (49):

$$\gamma_k(-1) = -1 \quad \textit{for all } k. \tag{55}$$

Further investigations concerning $e_k(\gamma)$ or $\gamma_k(e)$ need thus deal only with non-negative values of γ and e.

An immediate result of (55) is the complete specification of the class $\gamma = -1$ of (n, k)-alphabets which give W-error-correcting codes, where $W = 2^{k-2}t - 1$. For $\gamma = -1$, $e = -1$, Theorem 4 requires

$$\sum_j d_j = -2^{k-1} - (2^k - 1)(-1) = 2^{k-1} - 1,$$

while Corollary 5.1 and Theorem 6 require that *either* all the d_j's be odd *or* the d_j's associated with the points of one $(k - 2)$-flat π_{i_0} be odd and all other d_j's be even, so that there is *only one possible* D-measure: the D-measure which assigns $d_j = 1$ to each of the $2^{k-1} - 1$ points of π_{i_0} and $d_j = 0$ to each point outside π_{i_0}. A unique n-measure follows from this D-measure by application of (40), which here is

$$n_i = t + 1 - (1/2^{k-2})[\sum_{\pi_i} d_j + 1].$$

Since any $(k - 2)$-flat other than π_{i_0} meets π_{i_0} in a $(k - 3)$-flat, containing $2^{k-2} - 1$ points,

$$\sum_{\pi_i} d_j = 2^{k-2} - 1, \qquad i \neq i_0,$$

$$\sum_{\pi_{i_0}} d_j = 2^{k-1} - 1,$$

whence

$$(56) \qquad n_i = \begin{cases} t & \text{for } i \neq i_0, \\ t - 1 & \text{for } i = i_0, \end{cases} \qquad (\gamma = -1, \text{any } k).$$

This is precisely (49), which is thus seen to be the *unique* design for W-error-correcting (n, k)-alphabets of the class $\gamma = -1$. This is the Type t,1-alphabet of MacDonald [12].

For nonnegative e and γ, the functions $\gamma_k(e)$ and $e_k(\gamma)$ depend heavily on k. The case $k = 2$ is readily resolved. Here $PG(k - 1, 2)$ is the projective line $PG(1, 2)$, $(k - 2)$-flats are points, $n = 3t + \gamma$, $W = t + e$, and

$$-1 \leqq \gamma \leqq 2^k - 3$$

gives $\gamma = -1, 0, 1$. The bounds given by (52) are

$$-1 \leqq e \leqq \left[\frac{2\gamma - 3}{6}\right],$$

so that $e = -1$ for all γ. The n-measure admitting this value of e for $\gamma = -1$ is given by (56): $(t, t, t - 1)$; obvious n-measures admitting $e = -1$ (that is, $W = t - 1$) for $\gamma = 0, 1$ are (t, t, t) and $(t, t, t + 1)$, respectively. (The weight $w(U_j)$ of the letter U_j is the total n-measure of all points lying outside the U_j-associated flat (here, point), so that in both the latter cases

$$w(U_j) \geqq 2W + 1 = 2t - 1$$

for all j.) The relation of W and n in the case $k = 2$ may thus be summarized:

$$(57) \qquad k = 2: \begin{cases} n = 3t + \gamma, & t > 0, \gamma = -1, 0, 1; \\ W = t + e, & e = -1 \text{ for all } \gamma. \end{cases}$$

The upper bound on e given by (52) is a necessary, but unfortunately not a sufficient, condition for the existence of an (n, k)-alphabet admitting e for given k and γ. One might expect that if the bound were refined by taking into account all the conditions on an (n, k)-alphabet, the bound could be attained. A first refinement of the bound results from application of Corollary 5.1 and Theorem 6 to (39). We have by (39)

$$(58) \qquad e = \frac{2^{k-1}\gamma - 2^k + 1 - \sum d_j}{2(2^k - 1)},$$

and by Corollary 5.1 and Theorem 6 there must be at least one $(k - 2)$-flat in the dual space in which all points have odd D-measure, so that

$$\sum d_j \geqq (2^{k-1} - 1)(1),$$

whence

$$(59) \qquad -1 \leqq e \leqq \left[\frac{2^{k-2}(\gamma - 3) + 1}{2^k - 1}\right].$$

Consider the case $k = 3$. Here $PG(k - 1, 2)$ is the projective plane $PG(2, 2)$, $(k - 2)$-flats are lines, $n = 7t + \gamma$, $W = 2t + e$. Let us fix attention on determining $\gamma_3(e)$. From (53) we have $-1 \leqq e \leqq 0$, so that the only possible values of e are (-1) and 0. We know from (55) that $\gamma_3(-1) = -1$, so that we need find only $\gamma_3(0)$. For $k = 3$, $e = 0$, (59) gives

$$0 \leqq \left[\frac{2\gamma - 5}{7}\right],$$

yielding $\gamma = 3$ as the smallest value of γ potentially attainable, that is,

$$\gamma_3(0) \geqq 3.$$

We demonstrate that the bound is actually attainable by exhibiting an n-measure which defines an alphabet allowing all sequences of weight

$$W = 2t + e = 2t$$

to serve as coset leaders, given $n = 7t + 3$. Define the n-measure so that

$$n_i = t + 1$$

for three noncollinear points of $PG(2, 2)$, and $n_i = t$ for the remaining four points of $PG(2, 2)$. Then the greatest total n-measure of any $(k - 2)$-flat (line) is $3t + 2$, so that the total n-measure of the points lying outside any line is at least $(7t + 3) - (3t + 2) = 4t + 1$. That is, $w(U_j) \geqq 4t + 1$ for all j, whence obviously all sequences of weight $2t = W$ can serve as coset leaders. The relation of W and n in the case $k = 3$ may thus be summarized:

$$(60) \qquad k = 3: \begin{cases} n = 7t + \gamma, & \gamma = \begin{cases} -1, 0, 1, 2, 3, 4, 5 & \text{for } t > 0, \\ 3, 4, 5 & \text{for } t = 0; \end{cases} \\ \\ W = 2t + e, & e = \begin{cases} -1 & \text{for } \gamma = -1, 0, 1, 2, \\ 0 & \text{for } \gamma = 3, 4, 5. \end{cases} \end{cases}$$

We observe that the upper bound in (59) came about by placing in (58) the smallest possible value of $\sum d_j$ taking account of the congruence condition (42) for $c = 1$. This is the only pertinent value of c when $k = 3$. When $k > 3$, additional congruence conditions must be brought to bear. Consider the case $k = 4$. Here $PG(k - 1, 2)$ is the projective three-space $PG(3, 2)$, $(k - 2)$-flats are planes, $n = 15t + \gamma$, $W = 4t + e$. We set out to determine $\gamma_4(e)$ for nonnegative e; by (53) these values of e are 0, 1, 2. From (58) we have

$$(61) \qquad 8\gamma = 15(2e + 1) + \sum_j d_j ,$$

and if we designate by $\min \sum d_j$ the smallest value of $\sum_j d_j$ consistent with the congruence conditions on a D-measure, then a lower bound on γ for given e is provided by

$$(62) \qquad 8\gamma \geqq 15(2e + 1) + \min \sum d_j .$$

The congruence conditions (42) are

$$\sum_{\sigma_1} d_j \equiv 2e + 1 \pmod 2 \text{ for all lines } \sigma_1, \tag{63.1}$$

$$\sum_{\pi} d_j \equiv 2e + 1 \pmod 4 \text{ for all planes } \pi, \tag{63.2}$$

$$\sum_{j} d_j \equiv 2e + 1 \pmod 8). \tag{63.3}$$

The condition (63.1) is satisfied by means of Theorem 6: either all the d_j are odd, or the d_j for points of one plane π^* are odd and all other d_j are even. The smallest *provisional* $\sum d_j$, say $\sum^* d_j$, is obviously given by the second alternative, assigning $d_j = 1$ to each point of π^* and $d_j = 0$ to each of the remaining points of the dual space. Let us call this measure the *basic measure* D^*. For it we have $\sum^* d_j = 7$.

We shall consider the e-values in reverse order since the case $e = 0$ presents the most complications. When $e = 2$, the congruence conditions (63.2) and (63.3) are:

$$\sum_{\pi} d_j \equiv 1 \pmod 4 \text{ for all planes } \pi, \tag{63.2a}$$

$$\sum_{j} d_j \equiv 5 \pmod 8). \tag{63.3a}$$

We see that $\sum^* d_j = 7$ does not satisfy (63.3a) and that a minimum addition of 6 must be made. When this addendum is distributed to point or points Υ_j, the addition to any point must be a multiple of 2 in order that the congruence (63.1) be not disturbed. Let us distribute the addition by adding 2 to the D-measure of each point on a line l not lying wholly in π^* (meeting π^* in Υ^*, say). Then there are four categories of planes with respect to D-measure: π^*; the 3 planes π^u containing l; the 3 remaining planes π^v meeting π^* in a line containing Υ^*; the eight planes π^w meeting π^* in a line not containing Υ^*. The D-measures of these planes are as follows.

$$\sum_{\pi^*} d_j = 6(1) + 1(3) = 9 \equiv 1 \pmod 4,$$

$$\sum_{\pi^u} d_j = 2(1) + 1(3) + 2(2) + 2(0) = 9 \equiv 1 \pmod 4,$$

$$\sum_{\pi^v} d_j = 2(1) + 1(3) + 4(0) = 5 \equiv 1 \pmod 4,$$

$$\sum_{\pi^w} d_j = 3(1) + 1(2) + 3(0) = 5 \equiv 1 \pmod 4.$$

Thus (63.2a) is satisfied, $\min \sum d_j = 7 + 6 = 13$, and (62) gives

$$8\gamma \geqq 15(5) + 13 = 88, \qquad \gamma \geqq 11.$$

Moreover, the bound is attained by means of the D-measure specified in the above argument, for reference to (40) shows that the resulting n-measure satisfies

$$n_i \geqq t + 11 - 2(5) - \tfrac{1}{4}[\max_i \sum_{\pi_i} d_j - 5]$$

$$= t + 1 - \tfrac{1}{4}[9 - 5] = t \geqq 0 \qquad \text{for all } i.$$

Thus, $\gamma_4(2) = 11$.

When $e = 1$, we must satisfy

$$\text{(63.2b)} \qquad \sum_{\pi} d_j \equiv 3 \pmod 4 \text{ for all planes } \pi,$$

$$\text{(63.3b)} \qquad \sum_{j} d_j \equiv 3 \pmod 8.$$

The basic measure D^* does not satisfy (63.3b); the minimum amount which must be added to $\sum^* d_j$ is 4. We observe that D^* does satisfy (63.2b), since π^* has D-measure 7 and all other planes have D-measure 3. Hence, if the required addendum 4 is assigned to a single point, the congruences (63.2b) will not be disturbed. Keeping in mind that an alphabet requires $n_i \geqq 0$ for all i, and that by (40) n_i is a decreasing function of $\sum_{\pi_i} d_j$, our aim is to keep $\max_i \sum_{\pi_i} d_j$ as small as possible. Hence we assign the additional measure 4 to a point Υ_0 lying *outside* π^*. Then π^* has D-measure 7, any other plane not containing Υ_0 has D-measure $3(1) + 4(0) = 3$, and any plane containing Υ_0 has D-measure $1(4) + 3(1) + 3(0) = 7$. Thus, $\min \sum d_j = 7 + 4 = 11$, and

(62) gives $\gamma \geqq 7$. Moreover, the bound is attainable, since the D-measure constructed above gives

$$n_i \geqq t + 7 - 2(3) - \tfrac{1}{4}[\max_i \sum_{\pi_i} d_j - 3]$$

$$= t + 1 - \tfrac{1}{4}[7 - 3] = t \geqq 0 \quad \text{for all } i.$$

Thus, $\gamma_4(1) = 7$.

For $e = 0$, we must satisfy

$$\text{(63.2c)} \qquad \sum_{\pi} d_j \equiv 1 \pmod 4 \text{ for all planes } \pi,$$

$$\text{(63.3c)} \qquad \sum_{j} d_j \equiv 1 \pmod 8.$$

Again there must be an addition to $\sum^* d_j$ in order to satisfy (63.3). This time the minimum addendum is 2; however, if that additional measure is given to a point outside π^*, then the D-measure of π^* is $7 \not\equiv 1 \pmod 4$, and if the additional measure is given to a point Υ^* of π^*, then any plane meeting π^* in a line not containing Υ^* will have D-measure $3(1) + 4(0) = 3 \not\equiv 1 \pmod 4$. Hence addendum 2 must be ruled out, and the minimum addition to $\sum^* d_j$ must be considered to be 10. Keeping in mind that, for providing $n_i \geqq 0$ for all i, it is desirable that $\max_i \sum_{\pi_i} d_j$ be as small as possible, we try to spread the measure 10 as thinly as possible over the planes of the space. Let us then increase by 2 the D-measures of 5 points such that not more than 3 are on any plane and exactly one (say Υ^*) is on π^*. For ease of reference we shall call these 5 points *heavy* points. There are now three categories of planes.

(i) *The plane* π^*. The D-measure of this plane is $6(1) + 1(3) = 9 \equiv 1 \pmod 4$.

(ii) *Planes* π^u *meeting* π^* *in a line containing* Υ^*. There are 6 such planes, in pairs, each pair forming with π^* a pencil. Any pencil exhausts the points of the space. Hence, since not more than 3 heavy points are on a single plane, the 4 heavy points outside π^* must be distributed two each on the planes π^u of any pencil of the type under discussion. Hence the D-measure of any plane π^u is $1(3) + 2(1) + 2(2) + 2(0) = 9 \equiv 1 \pmod 4$.

(iii) *Planes* π^v *meeting* π^* *in a line not containing* Υ^*. There are 8 such planes, in pairs, each pair forming with π^* a pencil. Since the 4 heavy points outside π^* are not on a single plane, there are $\binom{4}{3} = 4$ distinct planes containing 3 heavy points each, and these must clearly be in 4 different pencils (since otherwise there would have to be 7 heavy points in the space). The third plane of each such pencil then contains one heavy point. Hence the D-measure of a plane π^v is either $3(1) + 3(2) + 1(0) = 9$ or $3(1) + 1(2) + 3(0) = 5$; both values are congruent to one modulo 4. Thus (63.2c) is satisfied,

$$\min \sum d_j = 7 + 10 = 17,$$

and (62) gives $\gamma \geqq 4$. The bound is attainable since the D-measure specified above gives

$$\begin{aligned} n_i &\geqq t + 4 - 2(1) - \tfrac{1}{4}[\max_i \sum_{\pi_i} d_j - 1] \\ &= t + 2 - \tfrac{1}{4}[9 - 1] = t \geqq 0 \quad \text{for all } i. \end{aligned}$$

Thus, $\gamma_4(0) = 4$. Since by (55) $\gamma_4(-1) = -1$, we may now summarize the relation of W and n in the case $k = 4$:

$$(64) \quad k = 4: \begin{cases} n = 15t + \gamma, & \gamma = \begin{cases} -1, 0, 1, 2, 3, 4, 5, \cdots, 13 \text{ for } t > 0, \\ \qquad\qquad 4, 5, \cdots, 13 \text{ for } t = 0; \end{cases} \\ W = 4t + e, & e = \begin{cases} -1 \text{ for } \gamma = -1, 0, 1, 2, 3, \\ 0 \text{ for } \gamma = 4, 5, 6, \\ 1 \text{ for } \gamma = 7, 8, 9, 10, \\ 2 \text{ for } \gamma = 11, 12, 13. \end{cases} \end{cases}$$

Given k, γ, and e, a γ-class of W-error-correcting codes is obtained by setting up a γ-class of (n, k)-alphabets defined by a D-measure which satisfies Theorem 4. The alphabet (22) is a member of such a class, specifically of a γ-class $5(k = 3)$ since $n = 5 = (2^3 - 1)(0) + 5$. For such a class, (60) gives $e = 0$, and then Theorem 4 requires

$$\text{(i)} \qquad \sum_j d_j = 4(5) - (7)(1) = 13,$$

(ii) $$\sum_{\pi} d_j \equiv 1 \pmod 2 \text{ for all lines } \pi,$$

(iii) $$n_i = t + 3 - \tfrac{1}{2}[\sum_{\pi_i} d_j - 1] \geqq 0 \text{ for all } i,$$

the last inequality demanding for any D-measure admitting *all* values of t

$$\sum_{\pi_i} d_j \leqq 7 \quad \text{for all } i.$$

The congruence condition is satisfied through application of Theorem 6. The class of alphabets to which (22) belongs is given by the D-measure exhibited in Figure 2; the point measures d_j are shown within parentheses. Application of (iii) readily verifies that $n_i = t, t + 2, t, t + 1, t + 1, t, t + 1$ for $i = 1, 2, \cdots, 7$, respectively. The n-measure for alphabet (22) is the special case $t = 0$.

As is clearly apparent in the foregoing example, there will in general be many D-measures satisfying Theorem 4 for given k, γ, and e. It is then reasonable from such a class of D-measures to select as "optimum" that measure (or those measures) whose resulting code(s) will correct the maximum number of

$$(W + 1)\text{-tuple}$$

errors. An optimum alphabet is thus one which allows the maximum number of weight-$(W + 1)$ sequences to serve as coset leaders. The alphabet (22) is such an optimum alphabet. The selection is based upon calculation of a quantity Δ for each competing D-measure, where Δ is termed the *discrepancy* and is defined as the number of weight-$(W + 1)$ sequences which do *not* serve as coset

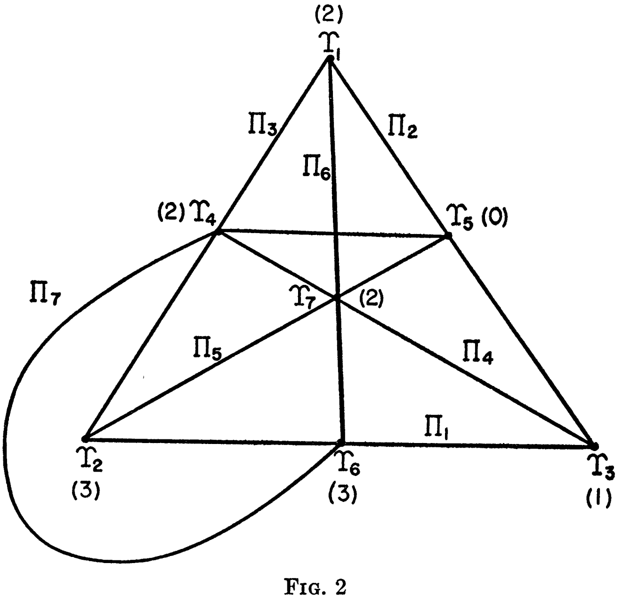

FIG. 2

leader. The derivation of a formula which allows convenient calculation of Δ will be presented in a subsequent paper. Also available are complete tables of optimum designs for $k = 2, 3, 4$ (all n), arrived at by application of the foregoing notions.

For increasing k, the establishment of $n_k(W)$ and the orderly construction of D-measures become increasingly more complicated. Thus far no general procedures are known. Some results in these matters, based on the geometric structure and theorems herein reported, will be presented in later communications.

REFERENCES

[1] R. C. Bose, "On the construction of balanced incomplete block designs," *Ann. Eugenics*, Vol. 9 (1939), pp. 353–399.

[2] R. C. Bose, "Mathematical theory of the symmetrical factorial design," *Sankhya*, Vol. 8 (1947), pp. 107–166.

[3] R. C. Bose and R. C. Burton, "On a problem in Abelian groups and the construction of fractionally replicated designs" (Abstract), *Ann. Math. Stat.*, Vol. 28 (1957), p. 533.

[4] L. Calabi and H. G. Haefeli, *On Hobbs' Code*, Technical Memorandum No. 14, Parke Mathematical Laboratories, Carlisle, Massachusetts, June 1957.

[5] Peter Elias, "Error-free coding," *Trans. I. R. E. Professional Group on Information Theory*, PGIT-4 (1954), pp. 29–37.

[6] Peter Elias, "Coding for noisy channels," *IRE Convention Record*, Vol. 3 (1955), Part 4, pp. 37–46.

[7] A. B. Fontaine and W. W. Peterson, *On Coding for the Binary Symmetric Channel*, Research Report RC-43, IBM Research Center, International Business Machines Corp., Poughkeepsie, N. Y., February 1958.

[8] E. N. Gilbert, "A comparison of signaling alphabets," *Bell System Technical J.*, Vol. 31 (1952), pp. 504–522.

[9] M. J. E. Golay, "Binary coding," *Trans. I. R. E. Professional Group on Information Theory*, PGIT-4 (1954), pp. 23–28.

[10] R. W. Hamming, "Error detecting and error correcting codes," *Bell System Technical J.*, Vol. 29 (1950), pp. 147–160.

[11] S. P. Lloyd, "Binary block coding," *Bell System Technical J.*, Vol. 36 (1957), pp. 517–535.

[12] J. E. MacDonald, Jr., *Constructive Coding Methods for the Binary Symmetric Independent Data Transmission Channel*, MEE Thesis, Syracuse University, January 1958.

[13] I. S. Reed, "A class of multiple-error-correcting codes and the decoding scheme," *Trans. I. R. E. Professional Group on Information Theory*, PGIT-4 (1954), pp. 38–49.

[14] David Slepian, "A class of binary signaling alphabets," *Bell System Technical J.*, Vol. 35 (1956), pp. 203–234.

[15] H. Weinitschke, *On Some Upper Bounds of Importance in Slepian's Theory of Coding*, Technical Memorandum No. 15, Parke Mathematical Laboratories, Carlisle, Massachusetts, June 1957.