

UNIVERSITY OF NORTH CAROLINA

Department of Statistics

Chapel Hill, N. C.

A CHARACTERIZATION OF FLAT SPACES IN A
FINITE GEOMETRY AND THE UNIQUENESS OF
THE HAMMING AND THE MacDONALD CODES

by

R. C. Bose and R. C. Burton

August 1964

This research was supported by U. S. Army Research Office - Durham
under Contract No. DA-31-124-AROD-254.

Institute of Statistics
Mimeo Series No. 407

Number of Pages: 11

Number of Figures: 1

Proposed Running Head: Uniqueness of Codes

ABSTRACT

Let $PG(k-1, q)$ be the projective geometry of dimension $k-1$ over the finite field $GF(q)$ where q is a prime power. The flat spaces of $PG(k-1, q)$ may be characterized by the following

Theorem. If F is a set of points in $PG(k-1, q)$ which has a non-empty intersection with every v -flat, then the number of points in F is greater than or equal to $(q^{k-v} - 1)/(q-1)$. Equality holds if, and only if, F is a $(k-v-1)$ -flat.

It may be shown from this theorem that the Hamming codes which maximize n for a given redundancy r , $q = 2$, and minimum distance $d = 4$, are unique. An extension of the theorem shows that the MacDonal codes with $d = q^{k-1} - q^\mu$ ($\mu = 0, 1, \dots, k-2$) are unique.

I. GEOMETRIC THEOREMS

Since most researchers are probably more familiar with vector spaces than with projective spaces, we recall the following well known 1-1 correspondence. To each subspace of rank s in a vector space of rank k , there corresponds a flat of dimension $s-1$ in the $(k-1)$ -dimensional projective geometry. A one-dimensional subspace, for example, corresponds to a projective point or 0-flat. Two flats F_1 and F_2 are said to intersect in a flat F_3 provided the subspaces corresponding to F_1 and F_2 have the subspace corresponding to F_3 as their intersection.

Every statement about the projective geometry $PG(k-1, q)$ can be translated into a statement about the vector space. Indeed, following Baer (1952), we may regard $PG(k-1, q)$ as the projective geometry of subspaces of the vector space. We will make frequent use of the following

Theorem 0. Let $r(A)$ denote the rank of a subspace A . Then if S and T are subspaces,

- (a) $S \subseteq T$ and $r(S) = r(T)$ imply $S = T$, and
- (b) $r(S) + r(T) = r(S \cap T) + r(S + T)$.

A proof of this theorem is found on page 18 of Baer (1952). By $S \subseteq T$ we mean that S is a subspace of T , $S \cap T$ is the intersection of S and T , and $S + T$ denotes the subspace spanned by S and T together. Theorem 1.6 remains true if the subspaces are considered as flats, and if for $r(A)$ we write $\dim(A)$, the dimension of the flat.

The connection between the above realization of a projective geometry and the realization in terms of proportional coordinates is easily seen. A subspace of rank 1 consists of all vectors which are proportional to some non-null vector. Any non-null vector in the subspace can serve as the basis for the subspace, or, as the vector of coordinates of the corresponding projective point.

Subspaces of higher rank may be given in terms of basis vectors which are independent and therefore not proportional. Hence the corresponding flat is defined in terms of distinct projective points. Projective points are said to be independent if the corresponding vectors are independent.

Alternately, a subspace may be defined as all vectors satisfying a set of homogeneous linear equations. Since the equations are homogeneous, they may be multiplied by non-zero constants without affecting the solutions. And if a vector satisfies the equations, then so do all vectors proportional to it.

Carmichael (1937) gives a readable introduction to finite projective geometries from this latter point of view, and the following formula which we will need.

The number of s -flats in a given t -flat ($s \leq t$) is

$$\frac{(q^{t+1} - 1)(q^t - 1) \cdots (q^{t+1-s} - 1)}{(q^{s+1} - 1)(q^s - 1) \cdots (q - 1)} . \quad (1)$$

In particular, the number of points in a v -flat is

$$(q^{v+1} - 1)/(q - 1) . \quad (1a)$$

In a $PG(k-1, q)$, the number of t -flats which contain a given s -flat ($s \leq t$) is

$$\frac{(q^{k-1-s} - 1)(q^{k-2-s} - 1) \cdots (q^{k-t} - 1)}{(q^{t-s} - 1)(q^{t-s-1} - 1) \cdots (q - 1)} , \quad (2)$$

as may be seen by dualizing (1). By specializing (2) we find that in a $PG(k-1, q)$, the number of lines through a point is

$$(q^{k-1} - 1)/(q - 1), \quad (2a)$$

the number of v -flats on a $(v-1)$ -flat is

$$(q^{k-v} - 1)/(q - 1), \quad (2b)$$

and the number of $(k-2)$ -flats on a given u -flat is

$$(q^{k-u-1} - 1)/(q - 1) . \quad (2c)$$

A $(k-2)$ -flat in $PG(k-1, q)$ is called a hyperplane. Let $|S|$ denote the number of elements in a set S . We prove first a preliminary theorem.

Theorem 1. If F is a set of points in $PG(k-1, q)$ which has a non-empty intersection with every line of $PG(k-1, q)$, then $|F| \geq (q^{k-1} - 1)/(q - 1)$. Equality holds if, and only if, F is a hyperplane.

We note first that if F is a hyperplane it intersects every line (by Theorem 0) and $|F| = (q^{k-1} - 1)/(q - 1)$.

Now let us suppose only that F intersects every line. Let S be the complementary set of F and let P be any point of S . By formula (2a) there are $(q^{k-1} - 1)/(q - 1)$ distinct lines l_i on P . By assumption each l_i has a point Q_i in common with F . If $Q_i = Q_j$, then $l_i = PQ_i = PQ_j = l_j$, which contradicts the fact that the lines l_i are all distinct. Hence the points Q_i are distinct and $|F| \geq (q^{k-1} - 1)/(q - 1)$.

Now suppose that F intersects every line and that $|F| = (q^{k-1} - 1)/(q - 1)$. Then the points Q_i described above are all the points of F . Since P was an arbitrary point of S , we conclude that any line which contains a point of S contains but one point of F . In other words, a line which is on two points of F is contained in F . (The equivalent property in terms of vector spaces is that if F contains two vectors it contains all linear combinations of them.) This shows that F is a flat space, and from the number of points it contains, F is clearly a $(k-2)$ -flat or hyperplane. This completes the proof of the theorem.

Corollary. If S is a set of q^{k-1} points in $PG(k-1, q)$ which does not contain all the points of any line, then S is the complementary set of a hyperplane. Any set which contains more points contains at least one line.

This is just a restatement of the theorem in terms of S , the complementary set of F . The number

$$q^{k-1} = \frac{q^k - 1}{q-1} - \frac{q^{k-1} - 1}{q-1}$$

is just the number of points in the complementary set.

Theorem 2. If F is a set of points in $PG(k-1, q)$ which has a non-empty intersection with every v -flat, then $|F| \geq (q^{k-v} - 1)/(q-1)$. Equality holds if, and only if, F is a $(k-v-1)$ -flat.

We note that if F is a $(k-v-1)$ -flat, it has a non-empty intersection with every v -flat (by Theorem 0) and $|F| = \frac{(q^{k-v} - 1)}{(q-1)}$.

The remainder of the proof is by induction on v . The theorem is obviously true if $v = 0$, and for $v = 1$ it reduces to Theorem 1. We assume that it is true for v^* if $v^* \leq v-1$.

Assume that F has a non-empty intersection with every v -flat and that $|F| \leq (q^{k-v} - 1)/(q-1)$. Then, by the inductive hypothesis, there exists a $(v-1)$ -flat L having no points in common with F since $|F| < (q^{k-v+1} - 1)/(q-1)$. By formula (2b) there are $(q^{k-v} - 1)/(q-1)$ distinct v -flats on L which we denote by $\Pi_1, \Pi_2, \dots, \Pi_m$, $m = (q^{k-v} - 1)/(q-1)$. By assumption each Π_i has a point P_i in common with F .

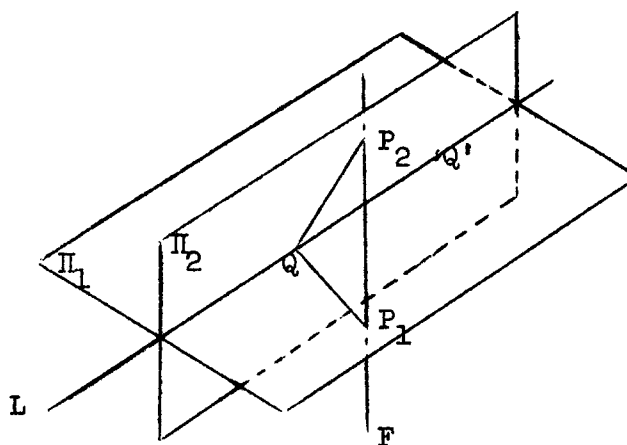


Figure 1

The points P_i are all distinct, for if $P_i = P_j$ then $\Pi_i = \Pi_j$ by Theorem 0, since Π_i and Π_j would have the $(v-1)$ -flat L and the point $P_i = P_j$, not on L , in common. Hence F contains at least $(q^{k-v}-1)/(q-1)$ points, as asserted by the theorem.

Now suppose F intersects every v -flat and that $|F| = (q^{k-v}-1)/(q-1)$. Then F is just the set of points P_i described above. Let Q be a point on L , and consider the lines QP_i . Since QP_i belongs to Π_i and QP_j does not, the lines QP_i are all distinct. Hence if G is the set of all points on the lines QP_i , then G contains $[q(q^{k-v}-1)/(q-1)]+1 = (q^{k-v+1}-1)/(q-1)$ points.

First assume that G is not a $(k-v)$ -flat. Then, by the inductive hypothesis, there is a $(v-1)$ -flat L' which has no points in common with G .

Now Q is not on L' since Q is on G . Let Σ be the v -flat QL' . Now Σ must have a point P_i common with F . The line QP_i and the $(v-1)$ -flat L' must have a common point, since both are subspaces of Σ . This is a contradiction since QP_i is in G , which is disjoint with L' .

Hence G is a $(k-v)$ -flat. Let Q' be a point on L distinct from Q . Let G' be the set of all points on the lines $Q'P_i$. Then G' is a $(k-v)$ -flat just as G is. The $(k-v)$ -flats G and G' are not identical, since if Q belonged to G' it would lie on a line $Q'P_i = Q'Q$ and P_i would be on L . Hence the intersection of G and G' is a flat space of dimension not greater than $k-v-1$. Since the $(q^{k-v}-1)/(q-1)$ points P_i all belong both to G and G' , we see that $G \cap G'$ is a $(k-v-1)$ -flat which consists of just the points P_i . That is, $G \cap G' = F$. This completes the proof of the theorem.

Corollary I. If S is a set of $(q^k - q^{k-v})/(q-1)$ points in $PG(k-1, q)$ which does not contain all the points of any v -flat, then S is the complementary set of a $(k-v-1)$ -flat. Any set which contains more points contains at least one v -flat.

This is just a restatement of the theorem in terms of S , the complementary set of F .

Corollary II. If F is a set of points in $PG(k-1, q)$ such that if Π is any v -flat when the intersection $F \cap \Pi$ contains a u -flat, then $|F| \geq (q^{k-v+u}-1)/(q-1)$. Equality holds if, and only if, F is a $(k-v+u-1)$ -flat.

To prove the corollary, let Π be any v -flat and let L be a u -flat which is contained in $F \cap \Pi$. By the conditions of the corollary, such an L exists. Since every $(v-u)$ -flat in Π has at least a point in common with L , F has a non-empty intersection with every $(v-u)$ -flat in Π .

Since every $(v-u)$ -flat is contained in some v -flat, F has a non-empty intersection with every $(v-u)$ -flat. Hence the corollary follows from the theorem on replacing v by $v-u$.

The above corollary suggests the following theorem.

Theorem 3. If F is a set of points in $PG(k-1, q)$ such that if Π is any v -flat then the intersection $F \cap \Pi$ contains at least $(q^{u+1}-1)/(q-1)$ points, then

$|F| \geq (q^{k-v+u}-1)/(q-1)$. Equality holds if, and only if, F is a $(k-v+u-1)$ -flat.

We note first that if F is a $(k-v+u-1)$ -flat then $|F| = (q^{k-v+u}-1)/(q-1)$, and if Π is any v -flat then $F \cap \Pi$ contains at least a u -flat so that

$|F \cap \Pi| \geq (q^{u+1}-1)/(q-1)$.

The remainder of the proof is by induction on u . For $u = 0$ the theorem reduces to Theorem 2. We assume that it is true for u^* if $u^* \leq u-1$, and give a proof for u .

Let us assume that either

$$(a) \quad |F| < (q^{k-v+u}-1)/(q-1),$$

or

$$(b) \quad |F| = (q^{k-v+u}-1)/(q-1) \text{ and } F \text{ is not a } (k-v+u-1)\text{-flat.}$$

Then, by the inductive hypothesis for $u^* = u-1$, there exists at least one $(v-1)$ -flat L which has fewer than $(q^{u^*+1}-1)/(q-1) = (q^u-1)/(q-1)$ points in common with F .

By formula (2b) there are $(q^{k-v}-1)/(q-1)$ distinct v -flats on L . No two of these v -flats have one point in common other than the points of L . Since by the assumption of the theorem every v -flat has at least $(q^{u+1}-1)/(q-1)$ points in common with F , we have

$$\begin{aligned} |F| &> \frac{q^{k-v}-1}{q-1} \frac{q^{u+1}-1}{q-1} - \left[\frac{q^{k-v}-1}{q-1} - 1 \right] \frac{q^u-1}{q-1} \\ &= \frac{q^{k-v}-1}{q-1} q^u + \frac{q^u-1}{q-1} = \frac{q^{k-v+u}-1}{q-1}. \end{aligned}$$

The inequality is strict since L has fewer than $(q^u-1)/(q-1)$ points in common with F . Hence either of the assumptions (a) or (b) leads to a contradiction, and the proof of the theorem is complete.

Corollary. If S is a set of $(q^k - q^{k-v+u})/(q-1)$ points in $PG(k-1, q)$ which does not have more than $(q^{v+1} - q^{u+1})/(q-1)$ points in common with any v -flat ($v > u$), then S is the complementary set of a $(k-v+u-1)$ -flat. If $|S| > (q^k - q^{k-v+u})/(q-1)$, then there exists a v -flat such that $|S \cap \Pi| > (q^{v+1} - q^{u+1})/(q-1)$.

This is just a restatement of the theorem in terms of S , the complementary set of F .

II. APPLICATIONS TO CODES

Let V be an (n, k) code, that is, a subspace of rank k of the vector space of all n -tuples over $GF(q)$. V may be specified in terms of a $k \times n$ generator matrix G whose rows are a basis for V , or in terms of an $r \times n$ parity check matrix H where $r = n-k$. A vector \underline{x} belongs to V if and only if

$$H \underline{x} = \underline{0}. \quad (3)$$

From (3) we see that if no $d-1$ columns of H are linearly dependent, then every non-null vector in V has at least d non-zero coordinates. That is, the code V is of minimum weight (or distance) at least d .

Consider the case $d \geq 3$. Then no two columns of H can be proportional, so we may consider the n columns as projective coordinates of n distinct points in $PG(r-1, q)$.

Suppose $q = 2$ so that there are 3 points on a line of $PG(r-1, 2)$. Then for $d = 4$, the set S of points whose coordinate vectors are columns of H must not contain a line. We want to maximize the number n of columns, and, by the Corollary of Theorem 1, the only way to do this is to let S be the complementary set of a hyperplane in $PG(r-1, 2)$ so that $n = 2^{r-1}$. These are the distance 4 Hamming codes described in Hamming (1950) or Peterson (1961).

Now let us consider an (n, k) code V defined in terms of a generator matrix G . A vector \underline{x} belongs to V if and only if

$$\underline{x} = \underline{c} G, \quad (4)$$

where \underline{c} is some row k -vector. If there are $n-d$ columns \underline{g}_i of G such that the scalar product

$$\underline{c} \cdot \underline{g}_i = 0, \quad (5)$$

whereas $\underline{c} \cdot \underline{g}_i \neq 0$ for the other d columns of G , then \underline{x} is of weight d . (Scalar products and other matrix operations are to be taken over $GF(q)$.)

If the i -th column \underline{g}_i of G is replaced by $a\underline{g}_i$ where a is a non-zero element of $GF(q)$, then the weights of the code vectors are unaffected since $\underline{c} \cdot a\underline{g}_i = 0$ if and only if $\underline{c} \cdot \underline{g}_i = 0$. Hence the columns of G may be regarded as coordinates of points in $PG(k-1, q)$. (In fact, replacing \underline{g}_i by $a\underline{g}_i$ has no effect on the distribution of coset weights and hence on the probability of correct decoding, cf. Burton (1964a) pp. 24-25).

Now let us note that if b is a non-zero element of $GF(q)$, then the code vector

$$b \underline{x} = b \underline{c} G$$

has the same weight as \underline{x} . Hence there are $q-1$ code vectors corresponding to \underline{c} under the different choices for b . If we regard the equation

$$\underline{c} \cdot \underline{y} = 0$$

as the equation of a hyperplane Π in $PG(k-1, q)$, and the columns \underline{g}_i of G as coordinates of points P_i of $PG(k-1, q)$, then a necessary and sufficient condition that the $q-1$ code vectors corresponding to \underline{c} be of weight at least d is that Π should not contain more than $n-d$ of the points P_i .

Suppose we seek to find a code with parameters k , $n = (q^k - q^{u+2}) / (q-1)$, and $d = q^{k-1} - q^{u+1}$, where u is some integer in the range $u = -1, 0, 1, 2, \dots, k-3$. Then in the Corollary of Theorem 3, let S be the set of points P_i , $|S| = n$, and the v -flat be Π with $v = k-2$. Then $n-d = (q^{v+1} - q^{u+1}) / (q-1)$ so that

$$d = \frac{q^k - q^{u+2}}{q-1} - \frac{q^{k-1} - q^{u+1}}{q-1} = q^{k-1} - q^{u+1},$$

and the code is possible if and only if S is the complement of a flat of dimension

$$k-v+u-1 = u+1.$$

It is easily seen that d cannot be increased for the given n and k . In fact, the Corollary tells us that even if n is increased to $n+1$, then d cannot be increased.

We have glossed over one point. That is, the Corollary was only proved in case the points P_i are all distinct which means that no two columns of the generator matrix are proportional. What we have shown then, is that if the columns are not proportional, they must be the complementary set of a $(u+1)$ -flat.

MacDonald (1959) and McCluskey (1959) give a description of these codes for the case $q = 2$ which is equivalent to omitting a particular $(u+1)$ -flat. See also Peterson (1961).

The geometric theorems find other uses in coding theory in the papers by Burton (1964a), (1964b). In the second of these, we must face squarely the problem of proportional columns or even equal columns, and further discussion is deferred to that paper.

ACKNOWLEDGEMENT

Dr. Dale Mesner suggested Corollary II of Theorem 2, which in turn suggested Theorem 3.

REFERENCES

- Baer, Reinhold, (1952), "Linear Algebra and Projective Geometry," Academic Press, New York.
- Burt
- Burton, R.C., (1964a), "An Application of Convex Sets to the Construction of Error-Correcting Codes and Factorial Designs," Institute of Statistics Mimeo Series No. 393, University of North Carolina, Chapel Hill.
- Burton, R.C., (1964b), "Iterated bounds for error-correcting codes," submitted for publication.
- Carmichael, R.D., (1937), "Introduction to the Theory of Groups of Finite Order," Ginn & Co., reissued by Dover, New York.
- Hamming, R.W., (1950), "Error-detecting and error-correcting codes, "Bell System Tech. J., 29, 147-160.
- MacDonald, J.E., (1958), "Constructive Coding Methods for the Binary Symmetric Independent Data Transmission Channel," M.S. Thesis, Department of Electrical Engineering, Syracuse University, Syracuse, N.Y.
- McCluskey, E.J., Jr., (1959), "Error-correcting codes - a linear programming approach," Bell System Tech. J., 38, 1485-1512.
- Peterson, W.W., (1961), "Error-Correcting Codes," The M.I.T. Press, Cambridge, Mass.