Bases of Minimum-Weight Vectors for Codes from Designs

S. Gao and J. D. Key*
Department of Mathematical Sciences
Clemson University
Clemson SC 29634

July 29, 1997

Abstract

An explicit basis of incidence vectors for the p-ary code of the design of points and hyperplanes of the affine geometry $AG_m(F_p)$ for any prime p and any integer $m \geq 2$ is obtained, which, as a corollary, gives a new elementary proof that this code is a generalized Reed-Muller code. In the proof a class of non-singular matrices related to Vandermonde matrices is introduced.

1 Introduction

If V is a vector space of finite dimension m over a finite field F_q then the projective geometry $\mathcal{P}(V)$ and the affine geometry $\mathcal{A}(V)$ provide designs by taking the structures consisting of points and subspaces or flats of a fixed dimension. The codes over F_p, where q is a power of p, are the well known Reed-Muller (for $q = 2$) or generalized Reed-Muller codes, as was proved first in a series of papers by Delsarte [11, 12], Goethals [13] and MacWilliams [10] (see [2, Chapters 5 and 6],or [3], for detailed references). The dimensions of these codes are known from the general definitions of the Reed-Muller or generalized Reed-Muller codes. The minimum weight and the nature of the minimum-weight vectors in the special cases when these codes are the codes of designs from geometries is also known: the minimum-weight vectors are the scalar multiples of the incidence vectors of the blocks of the design, i.e. of the flats or subspaces. Thus these codes are all known to be spanned by minimum-weight vectors. However, apart from a few somewhat isolated cases, an explicit basis of minimum-weight vectors is not known, and the general aim here will be to find suitable bases of such vectors, in convenient geometric or algebraic terms. We exhibit such a basis for the affine, and hence also the projective, designs of points and hyperplanes of geometries over prime fields and will prove the following result:

*Support of NSF grant GER-9450080 acknowledged.

Theorem 1 *Let $\mathcal{D}$ be the design $AG_{m,m-1}(F_p)$ of points and hyperplanes, i.e. $(m-1)$-flats, in the affine space $AG_m(F_p)$ of dimension m over the prime field F_p. For $0 \leq t \leq \mu = \min(m, p-1)$ define a set $\mathcal{K}_t$ of hyperplanes with equations as follows:*

$$\begin{aligned} \mathcal{K}_0 &= \{X_1 + 1 = 0\} \\ \mathcal{K}_t &= \{\sum_{j=1}^{t} a_j X_{i_j} + b = 0\} \end{aligned}$$

for all choices of $\{i_1, i_2, \ldots, i_t, a_1, a_2, \ldots, a_t, b\}$ such that $1 \leq i_1 < i_2 < \ldots < i_t \leq m$, $1 = a_1 < a_2 < \ldots < a_t \leq p-1$ and $b = 0$ or $1 < b < a_2$. (When $t = 1$ we interpret a_2 as equal to p in the last inequality.)

If $\mathcal{K} = \bigcup_{t=0}^{\mu} \mathcal{K}_t$, then the incidence vectors of the hyperplanes in $\mathcal{K}$ form a basis for the p-ary code $C_p(\mathcal{D})$ of dimension $\binom{p+m-1}{m}$.

As a corollary we obtain a basis for the symmetric design of points and hyperplanes in $PG_m(F_p)$. Here we use the space spanned by a column vector $\langle (a_0, a_1, \ldots, a_m)^t \rangle$ to denote the hyperplane with equation $\sum_{i=0}^{m} a_i X_i = 0$.

Corollary 2 *A basis for the p-ary code of $PG_{m,m-1}(F_p)$ for any m and p is given by the incidence vectors of the following set $\mathcal{H}$ of hyperplanes, using homogeneous coordinates and writing*

$$e_{i-1} = (\underbrace{0, 0, \ldots, 1}_{i}, 0, \ldots, 0)^t \quad \text{for } i = 1, \ldots, m+1 :$$

$\mathcal{H} = \bigcup_{i=0}^{\mu} \mathcal{H}_i$ where

$$\mathcal{H}_0 = \{\langle e_0 + e_1 \rangle, \langle e_0 \rangle\},$$

and $\mathcal{H}_t$, for $1 \leq t \leq \mu = \min(m, p-1)$, is the collection of hyperplanes

$$\langle b e_0 + \sum_{j=1}^{t} a_j e_{i_j} \rangle$$

for all choices of $\{i_1, i_2, \ldots, i_t, a_1, a_2, \ldots, a_t, b\}$ such that $1 \leq i_1 < i_2 < \ldots < i_t \leq m$, $1 = a_1 < a_2 < \ldots < a_t \leq p-1$ and $b = 0$ or $1 < b < a_2$. (When $t = 1$ we interpret a_2 as equal to p in the last inequality.) The code has dimension $\binom{p+m-1}{m} + 1$.

As a by-product of Theorem 1 we obtain an elementary proof that the code of the affine design of points and hyperplanes is a generalized Reed-Muller code for the prime case: see Corollary 8. There are also applications of our bases to *visible sets*, in the sense of Ward [20]: see the note after Corollary 8 in Section 4.

Basis vectors for Reed-Muller and generalized Reed-Muller codes are given in the general case in terms of polynomial functions. The geometrical interpretation of these bases might not be immediately clear. In certain cases, when the geometry is over a

prime field, the group algebra can give a more convenient basis, *viz.* the Jennings basis [14], but again the geometrical interpretation of this basis is not, in general, helpful. In the general case of a finite-geometry design, it is not immediate how a basis for the code can be chosen from the incidence vectors of the design. In the prime case results of Moorhouse [19] and of Blokhuis and Moorhouse [6] give methods of choosing a basis of incidence vectors of lines for the desarguesian planes of prime order p. For the general designs of points and lines over F_p, only the Jennings basis always applies and this is not a basis of minimum weight vectors except in some special cases.

We will survey the known results below, after a section to explain the terminology. The proof of the theorem will follow in the final section, where we reduce the proof to showing that a class of matrices related to Vandermonde matrices are non-singular: see Proposition 6.

2 Terminology and background

The notation and terminology will mostly be consistent with that used in Assmus and Key [2].

An incidence structure $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ with point set $\mathcal{P}$ of size v and block set $\mathcal{B}$ is a t-(v, k, λ) **design** if every block is incident with precisely k points and any set of t distinct points are together incident with precisely λ blocks. For any field F, $F^{\mathcal{P}}$ is the vector space of functions from $\mathcal{P}$ to F with basis given by the characteristic functions of the singleton subsets of $\mathcal{P}$. If $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ is an incidence structure, the **code** $C_F(\mathcal{D})$ of $\mathcal{D}$ over F is the subspace of $F^{\mathcal{P}}$ spanned by the characteristic functions of the blocks of $\mathcal{D}$. If $F = F_p$ we write also $C_p(\mathcal{D})$ or $C(\mathcal{D})$ and its dimension is referred to as the **p-rank** of $\mathcal{D}$. The **weight** of a vector is the number of its non-zero entries. Clearly the code from a design will have minimum weight at most the block size k. The vector in $F^{\mathcal{P}}$, all of whose entries are 1, is called the **all-one vector** and denoted by $\boldsymbol{\jmath}$.

Let V be a vector space of dimension m over a finite field F. For $1 \leq t \leq m$, we denote by $AG_{m,t}(F)$ the design of points and t-flats (i.e. t-dimensional cosets) in the affine geometry $AG_m(F)$. Similarly, for $1 \leq t \leq m-1$, denote by $PG_{m-1,t}(F)$ the design of points and t-dimensional projective subspaces of the projective geometry $PG_{m-1}(F)$ defined by V. For these designs it is well known that the codes need to be over a prime field of the same characteristic as that of F to be of interest: see [2]. The codes of these designs are the Reed-Muller codes in the case $F = F_2$, or various generalized Reed-Muller codes, as was proved mostly by the work of Delsarte et al. [11, 12, 13, 10]. These results are described in [2, Chapter 5] or in [3], but we give a brief definition here in terms of the so-called *m-variable* approach involving monomials, as we shall need this concept in the proof of our theorem. Proofs of the statements can be found in [2, Chapter 5] or in [3].

Let $q = p^t$, where p is a prime. Set $E = F_q$ and let $V = E^m$ be a vector space of dimension m over E of m-tuples, with the usual standard basis. The codes will be

codes over E, and the ambient space will be the function space E^V where members $f \in E^V$ are functions of the m-variables denoting the coordinates of a variable vector in V, i.e. if $\mathbf{x} = (x_1, x_2, \ldots, x_m) \in V$, then $f \in E^V$ is given by

$$f = f(x_1, x_2, \ldots, x_m)$$

and the x_i take values in E. Since every element in E satisfies $a^q = a$, the polynomial functions in the m variables can be reduced modulo $x_i^q - x_i$ and we form the set $\mathcal{M}$ of q^m monomial functions

$$\mathcal{M} = \{x_1^{i_1} x_2^{i_2} \ldots x_m^{i_m} \,|\, 0 \leq i_k \leq q-1, k = 1, 2, \ldots, m\}.$$

For a monomial in $\mathcal{M}$ the degree ρ is the total degree, i.e. $\rho = \sum_{k=1}^{m} i_k$ and clearly $0 \leq \rho \leq m(q-1)$. $\mathcal{M}$ forms another basis for E^V. The polynomial $1 - (x_i - a)^{q-1}$ is the characteristic function of the $(m-1)$-flat in E^m given by the equation $X_i = a$.

Definition 1 *Let $E = F_q$, where $q = p^t$ and p is a prime, and set $V = E^m$. Then for any ρ such that $0 \leq \rho \leq m(q-1)$, the ρ^{th} order* **generalized Reed-Muller code** *$\mathcal{R}_E(\rho, m)$ over E is the subspace of E^V of all reduced m-variable polynomial functions of degree at most ρ. Thus*

$$\mathcal{R}_E(\rho, m) = \mathcal{R}_{F_q}(\rho, m) = \left\langle x_1^{i_1} x_2^{i_2} \ldots x_m^{i_m} \in \mathcal{M} \,|\, \sum_{k=1}^{m} i_k \leq \rho \right\rangle.$$

For any ρ such that $0 \leq \rho \leq m(q-1)$,

$$\dim(\mathcal{R}_{F_q}(\rho, m)) = \sum_{i=0}^{\rho} \sum_{k=0}^{m} (-1)^k \binom{m}{k} \binom{i - kq + m - 1}{i - kq}.$$

Also, for $0 \leq r \leq m$ and $\rho \geq r(q-1)$, $\mathcal{R}_{F_q}(\rho, m)$ contains the incidence vector of any $(m-r)$-flat of $AG_m(F_q)$, since the polynomial function that gives the incidence of an $(m-r)$-flat with equations

$$\sum_{j=1}^{m} a_{ij} X_j = w_i, \text{ for } i = 1, 2, \ldots, r$$

where all a_{ij} and w_i are in F_q is

$$p(x_1, \ldots, x_m) = \prod_{i=1}^{r} \left(1 - (\sum_{j=1}^{m} a_{ij} x_j - w_i)^{q-1} \right),$$

of degree $r(q-1)$.

When $q = p$ is a prime the codes in the affine case have been shown to be powers of the nilpotent radical of a group algebra: see a treatment of this aspect in [3]. Let G be an additive elementary abelian p-group of order p^m and F a field of characteristic p, and let $F[G]$ denote the group algebra of G over F. Then we identify G with the underlying vector space F_p^m. If $\boldsymbol{M}$ denotes the nilpotent radical of $F[G]$, then we have, following Delsarte [12] and Charpin [8]:

Result 1 *For any prime p, the p-ary code of the design $AG_{m,r}(F_p)$ is $\mathcal{R}_{F_p}((m-r)(p-1), m)$ which is equal to $\boldsymbol{M}^{r(p-1)}$.*

Notice of course that the codes in the projective case are all cyclic, and that a generator polynomial can be given quite easily, and thus also a generator matrix can be found: see [2, Chapter 5]. Similarly, the definition of the generalized Reed-Muller codes allows a basis to be constructed. However, none of these bases have a convenient geometrical description, and do not, in general, consist of minimum-weight vectors.

The theorem of Jennings gives a basis for any of the generalized Reed-Muller codes when p is prime, as follows:

Result 2 (Jennings) *Let G be an additive elementary abelian p-group of order p^m and F a field of characteristic p. Denote a basis for the group algebra $F[G]$ by $\{X^g \mid g \in G\}$. For any basis $\{g_1, \ldots, g_m\}$ of G, the p^m elements*

$$\prod_{\nu=1}^{m} (X^{g_\nu} - 1)^{e_\nu}$$

where $0 \leq e_\nu < p$ form a linear basis for $F[G]$. Further,

$$\{\prod_{\nu=1}^{m} (X^{g_\nu} - 1)^{e_\nu} \mid \sum_{\nu=1}^{m} e_\nu \geq t, 0 \leq e_\nu < p\}$$

form a basis of $\boldsymbol{M}^t$, for $t = 1 \ldots m(p-1)$, where $\boldsymbol{M}$ is the radical of $F[G]$.

Such a basis for $F[G]$ was exhibited by Jennings [14] and is called a **Jennings basis** of the group algebra, although it first appeared in the work of Lombardo-Radice [18]. In particular, when $t = r(p-1)$, and $F = F_p$, then $\boldsymbol{M}^{r(p-1)} = C_p(AG_{m,r}(F_p))$, by Result 1. These are all Reed-Muller or generalized Reed-Muller codes, as described above. Those elements of the basis that have $e_\nu = (p-1)$ for precisely r values of ν are incidence vectors of subspaces of dimension r. See [3] or [1] for more details and properties of the Jennings basis. We mention also that Beth [5] uses the discrete Fourier transform to show that the incidence vectors of the lines of the affine geometry generate the code $\boldsymbol{M}^{p-1}$.

Finally we give the terminology (based on that given in [9]) for the ordering of the rows and columns of the matrix defined in Proposition 6. Let $n = (n_1, n_2, \ldots n_r)$

and $m = (m_1, m_2, \ldots, m_r)$ be r-tuples of non-negative integers. Using [9], **inverse lexicographic order** on these r-tuples defines $n > m$ if the *right-most* non-zero entry of $n - m$ is *positive*. In contrast, **inverse reverse lexicographic order** on these r-tuples defines $n > m$ if the *right-most* non-zero entry of $n - m$ is *negative*.

3 Known bases of minimum-weight vectors

Bases of incidence vectors of blocks for the p-ary codes of $AG_{m,t}(F_q)$ and $PG_{m,t}(F_q)$, where q is a power of p, are known in the following cases:

- $AG_{m,r}(F_2)$ and $PG_{m,r}(F_2)$ all r and all m: see Proposition 3;
- $PG_{3,2}(F_{2^s})$: see [4];
- $AG_{m,1}(F_3)$ and $PG_{m,1}(F_2)$ all m: see [16, 17];
- $AG_{2,1}(F_p)$ and $PG_{2,1}(F_p)$ all p: see [19, 6] and Result 3 below.

See also [15] for a survey.

The Jennings basis allows us to obtain a basis of minimum-weight vectors for the binary code of $AG_{m,r}(F_2)$ for any m and r, i.e. for the Reed-Muller code $\mathcal{R}(m-r, m)$. (See Note 2 at the end of Section 4 for a further correspondence between the group-algebra notation and the incidence vectors of hyperplanes.)

Proposition 3 *For any r and any m such that $1 \leq r < m$ the binary code of $AG_{m,r}(F_2)$ has a basis of incidence vectors of r-flats corresponding to all the following elements of the group algebra:*

$$\prod_{j=1}^{r}(X^{g_{i_j}} - 1) \prod_{j=r+1}^{r+t} X^{g_{i_j}} \tag{1}$$

for $0 \leq t \leq m - r$, where $1 \leq i_1 < i_2 < \ldots < i_{r+t} \leq m$, and where $\{g_1, \ldots, g_m\}$ is a basis for the additive elementary abelian 2-group that acts as the translation group of F_2^m. The dimension of the code is $\sum_{s=0}^{r} \binom{m}{s}$.

The group-algebra element (1) *corresponds to the incidence vector of the r-flat given by the $m - r$ equations*

$$X_i = 0 \text{ for } i \notin \{i_1, \ldots, i_{r+t}\} \quad \text{and } X_i = 1 \text{ for } i \in \{i_{r+1}, \ldots, i_{r+t}\}$$

with the same conditions on the i_j and t as above.

Proof: The proof is really almost immediate from the Jennings basis in the binary case. □

The basis obtained by Moorhouse [19] for the desarguesian affine plane of prime order is as follows:

Result 3 *Let π denote the desarguesian affine plane of prime order p. A basis for the code $C_p(\pi)$ can be found by taking the incidence vectors of the following lines: all the p lines from any one parallel class; any $p-1$ lines from any other parallel class; and so on, until a single line is chosen from one of the final two parallel classes, and no lines are chosen from the remaining class. This gives*

$$p + (p-1) + (p-2) + \cdots + 1 = \frac{1}{2}p(p+1) = \binom{p+1}{2}$$

lines, whose incidence vectors form a basis for $C_p(\pi)$.

In the case $m = 2$ our bases are all of this type.

A different basis of minimum-weight vectors for $PG_{2,1}(F_p)$ (and hence for the affine case as well) is described by Blokhuis and Moorhouse [6] and involves any conic in the plane. In [17] and [16] bases for the codes of Steiner triple systems arising from finite geometries, i.e. $PG_{m,1}(F_2)$ and $AG_{m,1}(F_3)$, are described.

4 Proof of the theorem

We now proceed to the proof of the theorem, using the monomial basis. In terms of the monomial basis for $\mathcal{R}_{F_p}(p-1,m)$, the incidence vector of the hyperplane

$$\sum_{j=1}^{t} a_j X_{i_j} + b = 0$$

is given by the function in m variables

$$h(x_1, x_2, \ldots, x_m) = 1 - (\sum_{j=1}^{t} a_j x_{i_j} + b)^{p-1}.$$

Thus the monomials in the terms of $\mathcal{K}_t$ have at most t of the variables x_i appearing.

First notice that for $\mathcal{K}_t$ we can choose the sets $\tau = \{i_1, \ldots, i_t\}$ in $\binom{m}{t}$ ways, and for each τ we can choose the distinct coefficients $\{b, a_2, \ldots, a_t\}$ from the elements $\{0, 2, \ldots, p-1\}$ in $\binom{p-1}{t}$ ways, so we have $|\mathcal{K}_t| = \binom{m}{t}\binom{p-1}{t}$, and thus $|\mathcal{K}| = \sum_{t=0}^{\mu} \binom{m}{t}\binom{p-1}{t} = \binom{p+m-1}{m}$, which is the required dimension of the code.

In order to prove our theorem we will express our sets $\mathcal{K}_t$ in monomial notation; then we will form a $\binom{p+m-1}{m} \times \binom{p+m-1}{m}$ transformation matrix A with rows indexed by the elements of $\mathcal{K}_t$ for $t \in \{0, 1, 2, \ldots, \mu\}$ and with columns indexed by the monomials on $x_1, x_2, \ldots, x_m$, in $\mathcal{R}_{F_p}(p-1,m)$ starting with 1, then those in one variable $x_i^{e_i}$, then those in two $x_i^{e_i} x_j^{e_j}$, and so on. Further, within those monomials in t variables, we start with those of the form $x_{i_1}^{e_1} \ldots x_{i_t}^{e_t}$ where $\sum_{i=1}^{t} e_i = p-1$. We wish of course to show that

A is non-singular over F_p, and thus that all these monomials are in the code spanned by $\mathcal{K}$.

Next we need to partition our matrix A and order the hyperplanes in each section $\mathcal{K}_t$ in a particular way. The vectors from $\mathcal{K}$ should be arranged according to ascending values of t. For $t = 0$ we replace the incidence vector of $X_1 + 1 = 0$ with the all-one vector $\boldsymbol{\jmath}$; this is allowed since the sum of all the incidence vectors of the hyperplanes $X_1 + b = 0$ for $b \in F_p$ is $\boldsymbol{\jmath}$, which corresponds to the constant function 1. This makes the first row of A have a single entry 1 in the left-most position and 0 in all the other positions. For each value of $t \geq 1$ we collect all those with the same set $\tau = \{i_1, i_2, \ldots, i_t\}$ and form $\binom{m}{t}$ square $\binom{p-1}{t} \times \binom{p-1}{t}$ matrices, $A_{t,\tau}$. Furthermore, we take for the first $\binom{p-2}{t-1}$ rows of $A_{t,\tau}$ the hyperplanes with $b = 0$. In this way we will have the matrix A partitioned with square submatrices of size $\binom{p-1}{t} \times \binom{p-1}{t}$ on the diagonal, for $t = 0$ to μ, with only zero entries above this diagonal. If we can show that the determinant of each of these submatrices is nonzero, then the determinant of A will be nonzero. There are $\mu + 1$ distinct submatrices, since all those for the same value of t will be the same. Thus let us write A_t instead of $A_{t,\tau}$ for the square submatrix for t, for $t = 0, \ldots, \mu$, and further notice that for $t \geq 1$ A_t is partitioned into submatrices with square submatrices on the diagonal corresponding to the choice of $b = 0$ in the first rows of A_t. The monomials involved with the values $b = 0$ must all have total degree $p - 1$ and thus again we will get a block of zeros above the second submatrix, i.e. we get, for $1 \leq t \leq \mu$,

$$A_t = \begin{bmatrix} B_t & 0 \\ \star & C_t \end{bmatrix}$$

where B_t and C_t are square of size b_t and c_t, respectively, and $b_t + c_t = \binom{p-1}{t}$. Define C_0 to be A_0.

Lemma 4 *For $1 \leq t \leq \mu$, the matrix B_t is equivalent to C_{t-1} under a monomial transformation.*

Proof: Since the matrices A_t for fixed t are independent of the choice of the set $\tau = \{i_1, \ldots, i_t\}$ we can take the sets $\{1, \ldots, t-1\}$ and $\{1, \ldots, t\}$ for C_{t-1} and B_t, respectively. The matrix B_t has terms from the expansion of the polynomials $1 - (\sum_{j=1}^{t} a_j x_j)^{p-1}$ where $1 = a_1 < a_2 < \ldots < a_t \leq p - 1$, and we only take the terms involving all the t variables; since there is no constant term, all the terms will have full degree $p - 1$.

Further, the matrix C_{t-1} has terms from the expansion of the polynomials $1 - (\sum_{j=1}^{t-1} a_j x_j + b)^{p-1}$ where $1 = a_1 < b < a_2 < \ldots < a_{t-1} \leq p - 1$ where we take only the terms involving all the $t - 1$ variables and of less than full degree. This means that we take the same selection of terms as for B_t, with b taking the role of the t^{th} variable.

If the rows of B_t are arranged such that we start with $a_2 = 2$ and the rows of C_{t-1} are arranged starting with $b = 2$, it is easy to see that the rows and columns can be arranged so that we have exactly the same matrices. □

Lemma 5 *For $1 \leq t \leq \mu$, the matrix C_t is equivalent to a matrix M_t of size $\binom{p-2}{t}$ with columns indexed by the distinct t-tuples $(\tau_1, \tau_2, \ldots, \tau_t)$ where $0 \leq \tau_i$ and $0 \leq \sum_{i=1}^{t} \tau_i \leq p-2-t$ and with rows indexed by the distinct t-tuples $(a_1, a_2, \ldots, a_t)$ where $2 \leq a_1 < a_2 < \ldots < a_t \leq p-1$ and with entry at column $(\tau_1, \tau_2, \ldots, \tau_t)$ and row $(a_1, a_2, \ldots, a_t)$ given by*

$$M_t(a_1, a_2, \ldots, a_t; \tau_1, \tau_2, \ldots, \tau_t) = a_1^{\tau_1} a_2^{\tau_2} \ldots a_t^{\tau_t}.$$

Proof: Recall that C_t is of size $c_t = \binom{p-1}{t} - \binom{p-2}{t-1} = \binom{p-2}{t}$ and has terms from the expansion of $1 - (\sum_{j=1}^{t} a_j x_j + b)^{p-1}$. Taking out constant non-zero factors from the rows and columns gives us the matrix M_t. □

To complete the proof of the theorem we thus need to show that the matrix M_t is non-singular for every t. We achieve this by formulating a more general proposition which is of interest in its own right. Notice that here we assume that $0^i = 1$ for $i = 0$.

Proposition 6 *For any integers $m \geq 0$ and $r \geq 1$, and any $m+r$ elements $c_1, c_2, \ldots, c_{m+r}$ from a field F, define a matrix $M(m,r)$ as follows: the rows are indexed by r-tuples of integers $(a_1, a_2, \ldots, a_r)$ with $1 \leq a_1 < a_2 < \ldots < a_r \leq m+r$, and the columns are indexed by r-tuples of integers $(b_1, b_2, \ldots, b_r)$ where $b_i \geq 0$ for $1 \leq i \leq r$ and $\sum_{i=1}^{r} b_i \leq m$, and the entry at row $(a_1, a_2, \ldots, a_r)$ and column $(b_1, b_2, \ldots, b_r)$ is*

$$M(a_1, a_2, \ldots, a_r; b_1, b_2, \ldots, b_r) = \prod_{i=1}^{r} c_{a_i}^{b_i}.$$

Then

$$\det(M(m,r)) = \prod_{1 \leq i < j \leq m+r} (c_i - c_j)^{\binom{m+r-1-j+i}{r-1}},$$

where the ordering of the columns is inverse lexicographic and the ordering of the rows is inverse reverse lexicographic.

Proof: (See the end of Section 2 for our terminology for the ordering of the rows and columns.) There is a one-one correspondence between the r-tuples $(a_1, a_2, \ldots, a_r)$ and $(b_1, b_2, \ldots, b_r)$ given by

$$a_1 = 1 + b_1,\ a_2 = 2 + b_1 + b_2,\ \ldots,\ a_r = r + b_1 + b_2 + \cdots + b_r,$$

or

$$b_1 = a_1 - 1,\ b_2 = a_2 - a_1 - 1,\ \ldots,\ b_r = a_r - a_{r-1} - 1.$$

Thus $M(m,r)$ is a square matrix of size $\binom{m+r}{r} \times \binom{m+r}{r}$.

The proof is by induction on r. When $r = 1$, $M(m,1)$ is an $(m+1) \times (m+1)$ Vandermonde matrix, and the proposition holds. Assume that the proposition holds for $r-1$ and any m. We prove it now for r.

First divide $M(m,r)$ into $(m+1)^2$ submatrices $M_{i,j}$ according to the values of a_r and b_r: the submatrices in the first rows have $a_r = r+m$, in the next set of rows $a_r = r+m-1$, and so on until the last row has $a_r = r$. The rows in each block of submatrices with constant value of a_r are further ordered by decreasing values of a_{r-1}, and so on. Similarly, the submatrices in the first columns have $b_r = 0$, in the next $b_r = 1$, and so on, until the last column has $b_r = m$. Also write $n = m + r$ for convenience. Then

$$M(m,r) = \left[\begin{array}{cccccc||c} b_r=0 & b_r=1 & \dots & b_r=j & \dots & b_r=m & a_r \\ \hline M_{0,0} & M_{0,1} & \dots & M_{0,j} & \dots & M_{0,m} & n \\ M_{1,0} & M_{1,1} & \dots & M_{1,j} & \dots & M_{1,m} & n-1 \\ \vdots & \vdots & & \vdots & & \vdots & \vdots \\ M_{i,0} & M_{i,1} & \dots & M_{i,j} & \dots & M_{i,m} & n-i \\ \vdots & \vdots & & \vdots & & \vdots & \vdots \\ M_{m,0} & M_{m,1} & \dots & M_{m,j} & \dots & M_{m,m} & r \end{array}\right],$$

Thus $M_{i,j}$ has $a_r = r+m-i = n-i$ and $b_r = j$. The number of columns in $M_{i,j}$ is equal to the number of $(r-1)$-tuples $(b_1, b_2, \dots, b_{r-1})$ such that $b_t \geq 0$ and $\sum_{t=1}^{r-1} b_t \leq m-j$, which is $\binom{m-j+r-1}{r-1}$ for $0 \leq j \leq m$. The number of rows of $M_{i,j}$ is equal to the number of $(r-1)$-tuples $(a_1, a_2, \dots, a_{r-1})$ such that $1 \leq a_1 < a_2 < \dots < a_{r-1} \leq r+m-i-1$, which is $\binom{r+m-i-1}{r-1}$ for $0 \leq i \leq m$. Setting $d_j = \binom{m-j+r-1}{r-1}$ for $0 \leq j \leq m$, we have that $M_{i,j}$ is a $d_i \times d_j$ matrix for $0 \leq i,j \leq m$. Clearly, $d_0 > d_1 > \dots > d_m = 1$. For each column of $M_{i,j}$ indexed by $(b_1, b_2, \dots, b_{r-1}, j)$, $M_{i,0}$ has a corresponding column indexed by $(b_1, b_2, \dots, b_{r-1}, 0)$, where $\sum_{t=1}^{r-1} b_t \leq m-j$. Since

$$M(a_1, a_2, \dots, a_r; b_1, b_2, \dots, j) = c^j_{a_r} M(a_1, a_2, \dots, a_r; b_1, b_2, \dots, 0),$$

we see that $M_{i,j}$ is a submatrix of $M_{i,0}$ with a factor c^j_{m+r-i}, where the submatrix consists of the columns of $M_{i,0}$ indexed by $(b_1, b_2, \dots, b_{r-1}, 0)$ with $\sum_{t=1}^{r-1} b_t \leq m-j$. Now we temporarily reorder the columns of each block of submatrices of $M(m,r)$ by decreasing values of $\sum_{t=1}^{r-1} b_t$ and by inverse lexicographical order (see Section 2) for $(b_1, b_2, \dots, b_{r-1}, 0)$ with fixed sum. Then the columns of $M_{i,j}$ have exactly the same order as the last d_j columns of $M_{i,0}$ for $0 \leq i \leq m$ and $0 \leq j \leq m$. Thus

$$M_{i,j} = c^j_{n-i} M_{i,0} J_{0,j},$$

where, for any $k < j$,

$$J_{k,j} = \left[\begin{array}{c} 0 \\ I_{d_j} \end{array}\right]$$

is a $d_k \times d_j$ matrix with the first $(d_k - d_j)$ rows equal to zero, and the last d_j rows

forming the identity matrix I_{d_j}. Writing $J_{0,j} = J_j$ we have

$$M(m,r) = \begin{bmatrix} M_{0,0} & c_n M_{0,0}J_1 & c_n^2 M_{0,0}J_2 & \dots & c_n^j M_{0,0}J_j & \dots & c_n^m M_{0,0}J_m \\ M_{1,0} & c_{n-1} M_{1,0}J_1 & c_{n-1}^2 M_{1,0}J_2 & \dots & c_{n-1}^j M_{1,0}J_j & \dots & c_{n-1}^m M_{1,0}J_m \\ \vdots & \vdots & \vdots & & \vdots & & \vdots \\ M_{i,0} & c_{n-i} M_{i,0}J_1 & c_{n-i}^2 M_{i,0}J_2 & \dots & c_{n-i}^j M_{i,0}J_j & \dots & c_{n-i}^m M_{i,0}J_m \\ \vdots & \vdots & \vdots & & \vdots & & \vdots \\ M_{m,0} & c_r M_{m,0}J_1 & c_r^2 M_{m,0}J_2 & \dots & c_r^j M_{m,0}J_j & \dots & c_r^m M_{m,0}J_m \end{bmatrix}.$$

Now perform column operations on the blocks of $M(m,r)$. Since $J_{j-1}J_{j-1,j} = J_j$ for $1 \le j \le m$, we can eliminate the submatrices in the first row by column operations on the blocks. For j from m to 1, multiply column $j-1$ by $-c_n J_{j-1,j}$ on the right and add to column j. Writing $e_i = (c_{n-i} - c_n)$ for $i = 1$ to m, the matrix becomes

$$\begin{bmatrix} M_{0,0} & 0 & \dots & 0 & \dots & 0 \\ M_{1,0} & e_1 M_{1,0}J_1 & \dots & c_{n-1}^{j-1} e_1 M_{1,0}J_j & \dots & c_{n-1}^{m-1} e_1 M_{1,0}J_m \\ \vdots & \vdots & & \vdots & & \vdots \\ M_{i,0} & e_i M_{i,0}J_1 & \dots & c_{n-i}^{j-1} e_i M_{i,0}J_j & \dots & c_{n-i}^{m-1} e_i M_{i,0}J_m \\ \vdots & \vdots & & \vdots & & \vdots \\ M_{m,0} & e_m M_{m,0}J_1 & \dots & c_r^{j-1} e_m M_{m,0}J_j & \dots & c_r^{m-1} e_m M_{m,0}J_m \end{bmatrix}.$$

Note that $M_{0,0} = M(m, r-1)$ is a square matrix defined on $c_1, \dots, c_{m+r-1}$. Taking the determinant we have

$$\det(M(m,r)) = \prod_{i=1}^{m} e_i^{d_i} \det(M_{0,0}) \det(A)$$

where

$$A = \begin{bmatrix} M_{1,0}J_1 & \dots & c_{n-1}^{j-1} M_{1,0}J_j & \dots & c_{n-1}^{m-1} M_{1,0}J_m \\ \vdots & & \vdots & & \vdots \\ M_{i,0}J_1 & \dots & c_{n-i}^{j-1} M_{i,0}J_j & \dots & c_{n-i}^{m-1} M_{i,0}J_m \\ \vdots & & \vdots & & \vdots \\ M_{m,0}J_1 & \dots & c_r^{j-1} M_{m,0}J_j & \dots & c_r^{m-1} M_{m,0}J_m \end{bmatrix}.$$

Continue with the Gauss-like elimination to obtain a diagonal block matrix. We obtain

$$\det(M(m,r)) = \det(M_{0,0}) \prod_{r \le i < j \le n} (c_i - c_j)^{d_{n-i}} \prod_{i=1}^{m} \det(M_{i,0}J_i).$$

We now restore our original ordering of columns, and note that for $1 \le i \le m$ we have $M_{i,0}J_i = M(m-i, r-1)$ defined on $c_1, \dots, c_{m-i+r-1}$.

We thus get a recursive formula:

$$\det(M(m,r)) = \prod_{k=1}^{m} \det(M(k, r-1)) \prod_{r \le i < j \le m+r} (c_i - c_j)^{d_{m+r-i}}, \tag{2}$$

where $d_j = \binom{m-j+r-1}{r-1}$ so that $d_{m+r-i} = \binom{i-1}{r-1}$, and we interpret $\det(M(k,0))$ as 1, and note that $\det(M(0,r)) = 1$ for all $r \geq 1$. Induction and the use of the identity

$$\binom{m}{n} = \sum_{i=n-1}^{m-1} \binom{i}{n-1},$$

allow us to obtain, from the identity (2), the formula given for the determinant. □

Since $\binom{m-j+r-1+i}{r-1} = 0$ if $j - i > m$, we obtain

Corollary 7 *The matrix $M(m,r)$ is non-singular if and only if any $m+1$ consecutive elements from the sequence $c_1, c_2, \ldots, c_{m+r}$ are distinct.*

The matrix we need for the theorem is simply a special case of the matrix $M(m,r)$ in Proposition 6, with $F = F_p$, $r = t$, $m = p-2-t$, $b_i = \tau_i$, and $c_{a_i} = \alpha^{a_i}$ where α is a primitive element for the field. Thus the theorem is also now proved. □

We also have a new elementary proof of the prime case of a well-known result (see [2, Corollary 5.7.1] or [1] for references to other proofs):

Corollary 8 *For any $m \geq 2$ and any prime p, the p-ary code of the affine-geometry design $AG_{m,m-1}(F_p)$ of points and hyperplanes of the affine geometry $AG_m(F_p)$ over the prime field F_p is the p-ary generalized Reed-Muller code $\mathcal{R}_{F_p}(p-1,m)$.*

Proof: The code of the design is evidently inside the code $\mathcal{R}_{F_p}(p-1,m)$ since the incidence vector of every block is. However, the non-singularity of the matrix A of transformation to the monomial basis shows that the dimensions are the same, and the codes are thus equal. □

Note:

1. It seems to be the case that our bases provide *visible sets* (in the sense of Ward [20]) in the ambient space $F_p^{p^m}$, for any fixed prime p, by concatenating all our bases for the affine spaces of dimension k where $2 \leq k \leq m$, and inserting zeros in the adjoined positions. This is equivalent to adding $m-k$ equations $X_i = 0$ for $i = k+1$ to m for each hyperplane in the k-dimensional space, for $2 \leq k \leq m$. Then for any subset S of vectors from this sequence, the minimum weight of the code spanned by S should be the minimum weight of the vectors in S. This indeed appears to be true but we do not have a complete proof.

2. In the group algebra, the incidence vector of the hyperplane ($(m-1)$-flat) H with equation

$$\sum_{j=1}^{t} a_j X_{i_j} + b = 0$$

is the element

$$\prod_{i \notin \tau}^{m} (X^{g_i} - 1)^{p-1} \prod_{j=2}^{t} (X^{-a_j g_{i_1} + g_{i_j}} - 1)^{p-1} X^{-b g_{i_1}} = \sum_{h \in H} X^h$$

of the group algebra, where $\tau = \{i_1, i_2, \ldots, i_t\}$, and using the same notation as in Sections 2 and 3. This is an element of $\boldsymbol{M}^{(m-1)(p-1)}$, so that we get Result 1 for this case again, by a dimension argument.

Acknowledgements:

The second author would like to thank the Department of Computer Science and Engineering and the Center for Communication and Information Science (CCIS) at the University of Nebraska for their hospitality.

Both authors thank the referees for their careful reading of the manuscript and for their suggestions.

References

[1] E. F. Assmus, Jr. and J. D. Key. Polynomial codes and finite geometries. To appear in Handbook of Coding Theory, edited by V. Pless, W. C. Huffman and R. Brualdi.

[2] E. F. Assmus, Jr. and J. D. Key. *Designs and their Codes*. Cambridge University Press, 1992. Cambridge Tracts in Mathematics, Vol. 103 (Second printing with corrections, 1993).

[3] Edward F. Assmus, Jr. and Jennifer D. Key. Codes and finite geometries. Technical report, INRIA, 1993. Report No. 2027.

[4] Bhaskar Bagchi and N. S. Narasimha Sastry. Even order inversive planes, generalized quadrangles and codes. *Geom. Dedicata*, 22:137–147, 1987.

[5] Thomas Beth. The $GF(p)$-dimension of the codes generated by the classical point-line geometries over $GF(p)$. *Des. Codes Cryptogr.*, 3:199–207, 1993.

[6] Aart Blokhuis and G. Eric Moorhouse. Some p-ranks related to orthogonal spaces. *J. Algebraic Combin.*, 4:295–316, 1995.

[7] Wieb Bosma and John Cannon. *Handbook of Magma Functions*. Department of Mathematics, University of Sydney, November 1994.

[8] Pascale Charpin. Une generalisation de la construction de Berman des codes de Reed et Muller p-aires. *Communications in Algebra*, 16:2231–2246, 1988.

[9] David Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms.* Springer-Verlag, 1996. Undergraduate Texts in Mathematics.

[10] P. Delsarte, J. M. Goethals, and F. J. MacWilliams. On generalized Reed-Muller codes and their relatives. *Inform. and Control*, 16:403–442, 1970.

[11] Philippe Delsarte. A geometric approach to a class of cyclic codes. *J. Combin. Theory*, 6:340–358, 1969.

[12] Philippe Delsarte. On cyclic codes that are invariant under the general linear group. *IEEE Trans. Inform. Theory*, 16:760–769, 1970.

[13] Jean-Marie Goethals and Philippe Delsarte. On a class of majority-logic decodable cyclic codes. *IEEE Trans. Inform. Theory*, 14:182–188, 1968.

[14] S. A. Jennings. The structure of the group ring of a p-group over a modular field. *Trans. Amer. Math. Soc.*, 50:175–185, 1941.

[15] J. D. Key. Bases for codes of designs from finite geometries. *Congr. Numer.*, 102:33–44, 1994.

[16] J. D. Key. Ternary codes of Steiner triple systems. *J. Combinatorial Designs*, 2:25–30, 1994.

[17] J. D. Key and F. E. Sullivan. Codes of Steiner triple and quadruple systems. *Des. Codes Cryptogr.*, 3:117–125, 1993.

[18] Lucio Lombardo-Radice. Intorno alle algebre legate ai gruppi di ordine finito. *Rend. Sem. Mat. Fac. Sci. R. Univ. Roma (4)*, 2:312–322, 1938.

[19] G. Eric Moorhouse. Bruck nets, codes, and characters of loops. *Des. Codes Cryptogr.*, 1:7–29, 1991.

[20] Harold N. Ward. Visible codes. *Arch. Math.*, 54:307–312, 1990.