Minimum weight for some binary geometric codes

Neil J. Calkin* J. D. Key
Department of Mathematical Sciences
Clemson University
Clemson SC 29634
U.S.A.

M. J. de Resmini
Dipartimento di Matematica
Universitá di Roma 'La Sapienza'
I-00185 Rome
Italy

September 4, 2008

Abstract

The geometric codes are the orthogonals of the codes defined by the designs associated with finite geometries. The latter are generalized Reed-Muller codes, but the geometric codes are, in general, not. We obtain values for the minimum weight of these codes in the binary case, using geometric constructions in the associated geometries, and the BCH bound from coding theory. Using Hamada's formula, we also show that the dimension of the orthogonal code of the projective geometry design is a polynomial function in the dimension of the geometry.

1 Introduction

For any finite dimensional vector space V over a finite field F_q, the projective geometry $\mathcal{P}(V)$ and the affine geometry $\mathcal{A}(V)$ provide combinatorial 2-designs by taking the structures consisting of points and subspaces or flats of a fixed dimension. The codes over F_p, the prime sub-field of F_q, are the well known Reed-Muller (for $q = 2$) or generalized Reed-Muller codes; this was established in a series of papers by Delsarte [5, 7, 8], Goethals [10] and MacWilliams [6] (see [2, Chapters 5 and 6],or [1], for more references). The dimensions of these codes can be computed from various algorithms or formulas, and the minimum weight and the nature of the minimum-weight vectors in this special case when these codes are the codes of designs from geometries, is also completely 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.

The situation regarding the orthogonals of these codes is not as clear. These are the so-called "geometric codes"(see [3, Chapter 2]) and they are not generalized Reed-Muller codes, in general, unless q is a prime. Furthermore, the minimum weight of these

*Support of NSA grant MDA904-97-1-0059 acknowledged.

codes is also not generally known, although some bounds are given: see, for example, [2, Chapter 5] for a summary of what is currently known.

In this paper we use the geometry of the projective space and some lower bounds obtained by Delsarte [5] using the BCH bound to determine the minimum weight when the order of the field is even. In particular we obtain

Theorem 1 *The minimum weight of the orthogonal of the binary code of the design of points and r-subspaces of $PG_m(F_q)$ and that of the design of points and r-flats of $AG_m(F_q)$, where q is even, $1 \leq r < m$, $m \geq 2$, is $(q+2)q^{m-r-1}$.*

We also obtain a simplification of Hamada's well-known formula (see Section 4):

Theorem 2 *Let $q = p^t$ and let $\mathcal{D}$ denote the design of points and r-dimensional subspaces of the projective geometry $PG_m(F_q)$, where $0 < r < m$. Then the p-rank of $\mathcal{D}$ is given by*

$$\frac{q^{m+1}-1}{q-1} - h(m),$$

where, for any fixed value of r, $h(m)$ is a polynomial in m of degree $(q-1)r$.

The proof of Theorem 1 is in Section 3, and that of Theorem 2 is in Section 4. We include also a short appendix showing the polynomials $h(m)$ for some values of r and q.

2 Background

Our notation and terminology for designs and codes will be standard and can be found in [2], for example.

Notation will include $PG_{m,r}(F_q)$ to denote the design of points and r-dimensional subspaces of the projective space $PG_m(F_q)$, i.e. a 2-(v,k,λ) design with

$$v = \frac{q^{m+1}-1}{q-1},\ k = \frac{q^{r+1}-1}{q-1},\ \lambda = \frac{(q^{m-1}-1)\dots(q^{m+1-r}-1)}{(q^{r-1}-1)\dots(q-1)}.$$

Similarly, $AG_{m,r}(F_q)$ will denote the 2-design of points and r-flats (cosets of dimension r) in the affine geometry $AG_m(F_q)$.

For any design $\mathcal{D}$, a set of points is called an $(n_1, n_2, \dots, n_s)$-set if blocks of the design meet the set in n_i points for some i such that $1 \leq i \leq s$, and if for each i there exists at least one block meeting the set in n_i points. The n_i's are the **intersection numbers** for the set, and an **n_i-secant** is a block meeting the set in n_i points. When the design has even order, and thus in particular in the case of $PG_{m,r}(F_q)$ when q is even, a set of points is called a **set of even type**, or an **even set**, if it is of type $(n_1, n_2, \dots, n_s)$ where all the n_i are even. Elementary counting shows that any set of

even type will have even size. If the design is $PG_{m,r}(F_q)$ where q is even, then a set that is an even set for r-subspaces (i.e. blocks) will be a set of even type for t-subspaces for $t \geq r$. A **hyperoval** in a plane of even order q is a set of $q+2$ points such that every line of the plane meets the set in 0 or 2 points.

The code C_F of the design $\mathcal{D}$ over the finite field F is the space spanned by the incidence vectors of the blocks over F. We take F to be a prime field F_p; in the case of the designs from finite geometries that we consider here, p will be the same as the characteristic of the field over which the geometry is defined. If the point set of $\mathcal{D}$ is denoted by $\mathcal{P}$ and the block set by $\mathcal{B}$, and if $\mathcal{Q}$ is any subset of $\mathcal{P}$, then we will denote the incidence vector of $\mathcal{Q}$ by $v^{\mathcal{Q}}$. Thus $C_F = \left\langle v^B \mid B \in \mathcal{B} \right\rangle$, and is a subspace of $F^{\mathcal{P}}$. The orthogonal, or dual, code is the orthogonal under the standard inner product. If a linear code over a field of order q is of length n, dimension k, and minimum weight d, then we write $[n,k,d]_q$ to show this information. In the case where $p=2$, so that the code is binary, any set of points that is met evenly by the blocks of $\mathcal{D}$ will have incidence vector in the binary code $C^\perp$ orthogonal to the binary code C of the design. Thus the search for sets of even type of smallest size will yield the minimum words of $C^\perp$, and the minimum weight. Even in the case of the finite geometry designs, this minimum weight is not always known. However, notice that in the case $q=2$ the codes of the designs, and their orthogonal codes, are the Reed-Muller codes, and all the questions we ask here have well-known answers. Other cases are also well known, for example if $m=2$ and q is even. The known bounds in the general case are summed up in [2, Theorem 5.7.9] and are given as follows:

Result 1 *1. Let C be the p-ary code of the design $PG_{m,r}(F_q)$ where $q=p^t$ and p is prime. Then the minimum weight $d^\perp$ of $C^\perp$ satisfies*

$$\frac{q^{m-r+1}-1}{q-1} + 1 \leq d^\perp \leq 2q^{m-r}.$$

2. Let C be the p-ary code of the design $AG_{m,r}(F_q)$ where $q=p^t$ and p is prime. Then the minimum weight $d^\perp$ of $C^\perp$ satisfies

$$(q+p)q^{m-r-1} \leq d^\perp \leq 2q^{m-r}.$$

See also Blake and Mullin [3, Section 2.2], Delsarte, Goethals and MacWilliams [6] or Delsarte [7, 5]. The bounds are deduced in [5] from the BCH bound using the fact that the projective codes are cyclic and the affine codes are extended cyclic.

3 Minimal sets of even type

The following construction is basic to our determination of the minimum weight.

Proposition 3 *Let $\mathcal{D} = PG_{m,1}(F_q)$ where $q = 2^t$ for $t \geq 1$, i.e. $\mathcal{D}$ is the 2-$(\frac{q^{m+1}-1}{q-1}, q+1, 1)$ design of points and lines in $\mathcal{P} = PG_m(F_q)$. Let $\mathcal{H}$ be a hyperplane in $\mathcal{P}$, and let $\mathcal{S}$ be a set of even type in $\mathcal{H}$, i.e. $\mathcal{S}$ is a set of points such that every line of $\mathcal{H}$ meets $\mathcal{S}$ evenly. Let V be a point of $\mathcal{P}$ that is not in $\mathcal{H}$. Then the set of points*

$$\mathcal{S}^* = \{X | X \text{ on a line } VY \text{ for } Y \text{ on } \mathcal{S}\} - \{V\}$$

is a set of even type for $\mathcal{D}$, of size $q|\mathcal{S}|$.

Proof: We need to show that every line L of $\mathcal{P}$ meets $\mathcal{S}^*$ evenly. If L is in $\mathcal{H}$ then this is clear, since $\mathcal{S}$ is of even type. If L is not in $\mathcal{H}$ then $L \cap \mathcal{H} = \{X\}$, i.e. a single point.

If $X \in \mathcal{S}$ and $L = VX$ then L meets $\mathcal{S}^*$ in q points and we are done. If $L \neq VX$ then let Π be the plane containing L and V. Since $V \notin \mathcal{H}$, Π is not in $\mathcal{H}$ and thus meets it in a line ℓ containing X. The line ℓ meets $\mathcal{S}$ evenly in a set $\mathcal{T}$, say, and for each $Q \in \mathcal{T}$, VQ is in Π and thus meets L. Thus L has precisely $|\mathcal{T}|$ points of $\mathcal{S}^*$, and no more, and thus L meets $\mathcal{S}^*$ evenly.

If $X \notin \mathcal{S}$ and V is not on L then again look at the plane Π containing L and V, and let Π meet $\mathcal{H}$ in the line ℓ. As in the last case, ℓ meets $\mathcal{S}$ evenly in a set $\mathcal{T}$ which is possible empty, and the lines VY for $Y \in \mathcal{T}$ will meet L in an even number of points. If V is on L then clearly L does not meet $\mathcal{S}^*$ at all. □

Note: For any $\mathcal{S}$, the set $\mathcal{S}^*$ has $n_s = q$ amongst its intersection numbers.

Corollary 4 *The designs $PG_{m,1}(F_q)$ and $AG_{m,1}(F_q)$ for q even, $m \geq 2$, have even sets of size $(q+2)q^{m-2}$ and of type $(0, 2, q)$.*

Proof: In the projective design $PG_{m,1}(F_q)$, starting with a hyperoval in the plane, the set of size $(q+2)q^{m-2}$ can be built up in steps as described in Proposition 3. That lines meet the set in $(0, 2, q)$ points is clear from the construction.

To show that $AG_{m,1}(F_q)$ also has such sets, we need only show that there is some hyperplane in $PG_m(F_q)$ that does not meet the even set of size $q^{m-2}(q+2)$ constructed as in Proposition 3 in $PG_m(F_q)$. We show this inductively: it is clear for $m = 2$, choosing simply a line external to the hyperoval. Suppose it is true for $m-1$ and let $\mathcal{S}^*$ be an even set from the construction of Proposition 3, and $\mathcal{S}$ the set in the hyperplane $\mathcal{H}$. By the induction hypothesis, let $\mathcal{H}'$ by a hyperplane of $\mathcal{H}$ that does not meet $\mathcal{S}$. Then the hyperplane of $PG_m(F_q)$ that is spanned by $\mathcal{H}'$ and the point V of the proposition will clearly not meet $\mathcal{S}^*$. The intersection numbers are thus $(0, 2, q)$. □

Corollary 5 *1. If C denotes the binary code of the design $\mathcal{D} = PG_{m,1}(F_q)$, where q is even, then for $m \geq 2$, the minimum weight $d^\perp$ of $C^\perp$ satisfies*

$$q^{m-1} + q^{m-2} + \cdots + q + 2 \leq d^\perp \leq q^{m-2}(q+2).$$

Furthermore, if $q \geq 4$ and $m \geq 3$, then

$$q^{m-1} + q^{m-2} + \cdots + q + 4 \leq d^\perp \leq q^{m-2}(q+2).$$

2. *If C denotes the binary code of the design $\mathcal{D} = AG_{m,1}(F_q)$, where q is even, then for $m \geq 2$, the minimum weight $d^\perp$ of $C^\perp$ satisfies*

$$d^\perp = q^{m-2}(q+2).$$

Proof: The upper bound follows from Corollary 4. For the lower bound, use Result 1 or argue simply as follows: let X be a point on a non-empty even set $\mathcal{S}$; then every line through X must meet $\mathcal{S}$ again, which gives the first lower bound.

If the bound is met, then every line through X meets $\mathcal{S}$ exactly twice, for any $X \in \mathcal{S}$, and this is only possible for $m = 2$ or for $q = 2$, by a result of Qvist, and Barlotti, as quoted in Dembowski [9, Page 49], or see Hirschfeld [13]. This now gives the second set of inequalities, and completes the proof for the projective case.

For the affine case, the lower bound given in Result 1 is the same as the upper bound in Corollary 4. □

Before turning to the proof of Theorem 1, we show that the even sets constructed in Corollary 4 are unique when $m = 3$. In this case, when $m = 3$, the even set is a hyperoval cone with its vertex deleted.

Proposition 6 *For $q \geq 4$ even, any even set in $PG_{3,1}(F_q)$ of type $(0, 2, q)$ and of size $q(q+2)$ is a hyperoval cone with its vertex deleted.*

Proof: Let $\mathcal{S}$ be such a set. We first show that there is exactly one q-secant on each point of $\mathcal{S}$, so that the q-secants partition $\mathcal{S}$. Thus letting v_j denote the number of j-secants on a point of $\mathcal{S}$, we have

$$\begin{aligned} v_2 + v_q &= q^2 + q + 1 \\ v_2 + (q-1)v_q &= q^2 + 2q - 1, \end{aligned}$$

so that $v_q = 1$, as asserted.

A similar count shows that the only sets of points in the projective plane $PG_2(F_q)$ with intersection numbers from the set $(0, 2, q)$ and at most one q-secant on each point are the hyperoval (of size $(q+2)$ and type $(0, 2)$) and the $2q$-set, of type $(0, 2, q)$, consisting of the points on two lines from which the point of intersection has been removed. Thus planes meet $\mathcal{S}$ in a hyperoval, a $2q$-set of the type described, or not at all.

Let L be a q-secant of $\mathcal{S}$ and let w_j be the number of j-planes on L. Then

$$\begin{aligned} w_{q+2} + w_{2q} &= q + 1 \\ (q+2-q)w_{q+2} + (2q-q)w_{2q} &= q(q+2) - q, \end{aligned}$$

so that $(q-2)w_{2q} = q^2 - q - 2 = (q-2)(q+1)$, i.e. $w_{2q} = q+1$ and $w_{q+2} = 0$. Thus all planes on the q-set L are $2q$-planes, and, clearly, the lines other than L forming the

$2q$-sets on these planes all meet L in the same point, i.e. the unique point of L not in $\mathcal{S}$.

Next take a 2-secant L' of $\mathcal{S}$ and look at the planes on it. This yields

$$\begin{aligned} w_{q+2} + w_{2q} &= q+1 \\ qw_{q+2} + (2q-2)w_{2q} &= q(q+2)-2, \end{aligned}$$

so that $w_{2q} = 1$ and $w_{q+2} = q$. Thus the unique $2q$-plane on L' contains two lines that meet off $\mathcal{S}$, and, by the above, they meet at the deleted vertex of a hyperoval cone. □

We can now give the proof of Theorem 1, which uses Result 1 (2).

Proof of Theorem 1: Notice that if $\mathcal{S}$ is an even set for the design $PG_{m,r}(F_q)$, then $\mathcal{S}$ will be an even set for the design $PG_{m,s}(F_q)$ for any $s \geq r$. Furthermore, $\mathcal{S}$ will be an even set for any $PG_{m+t,r+t}(F_q)$ containing the $PG_m(F_q)$, for $t \geq 1$. If there is a hyperplane $\mathcal{H}$ of $PG_m(F_q)$ that does not meet $\mathcal{S}$, then $\mathcal{S}$ will be an even set for the design $AG_{m,r}(F_q)$ obtained by deleting the hyperplane $\mathcal{H}$ from the projective space.

We have shown that the even set in $PG_{m,1}(F_q)$ of size $(q+2)q^{m-2}$ constructed in Corollary 4 is not met by some hyperplanes, and thus it is an even set for some $AG_{m,1}(F_q)$. To obtain an even set of size $(q+2)q^{m-r-1}$ in $PG_{m,r}(F_q)$, we take a subspace W of dimension $m-r+1$ in our projective geometry of dimension m, and construct an even set for $PG_{m-r+1,1}(F_q)$ of size $(q+2)q^{m-r-1}$, according to Corollary 4. That this is an even set for $PG_{m,r}(F_q)$ follows by considering that any subspace U of dimension r must meet W in at least a line, by the dimension equation. Since a hyperplane can be constructed that does not meet this set, we also get an even set of this size for $AG_{m,r}(F_q)$.

Thus sets of the required size exist; we need to show that they are minimal. Now we can use the result of Delsarte [5, 6], quoted in Result 1, to deduce that this is the minimum size in the affine case. Thus we need only prove the same for the projective geometries. If an even set of smaller size existed for the projective case, it would have to be met by every hyperplane, since it could not be an even set for the affine geometry. We prove the result by induction on m. For $m = 2$ we have a projective plane and the theorem is well-known; suppose we have the result for all dimensions up to $m-1$ and all r such that $1 \leq r \leq m-2$. Let $\mathcal{S}$ be an even set for $PG_{m,r}(F_q)$, where $1 \leq r \leq m-1$. If $r = m-1$ then $|\mathcal{S}| \geq q+2$ by Result 1, or elementary counting. If $r < m-1$, suppose hyperplanes of $PG_m(F_q)$ meet $\mathcal{S}$ in $\{n_1, n_2, \ldots, n_k\}$ points where $0 < n_1 < n_2 < \ldots < n_k$ (since we are supposing that every hyperplane meets $\mathcal{S}$), and suppose that x_{n_i} hyperplanes meet $\mathcal{S}$ in n_i points. Counting gives

$$\begin{aligned} x_{n_1} + x_{n_2} + \cdots &= \frac{q^{m+1}-1}{q-1}, \\ n_1 x_{n_1} + n_2 x_{n_2} + \cdots &= s\frac{q^m-1}{q-1}, \end{aligned}$$

where $|\mathcal{S}| = s$. Multiply the first by n_1 and subtracting from the second yields

$$s\frac{q^m-1}{q-1} \geq n_1\frac{q^{m+1}-1}{q-1}.$$

Since the intersection of $\mathcal{S}$ with any hyperplane is met evenly by any r-subspace of the hyperplane, by induction we have that $n_1 \geq (q+2)q^{(m-1)-r-1} = (q+2)q^{m-2-r}$. Thus

$$s \geq (q+2)q^{m-2-r}\frac{q^{m+1}-1}{q^m-1} \geq (q+2)q^{m-1-r},$$

which completes the proof. □

Note: 1. The theorem gives an algorithm to construct an even set of minimal size in the design $PG_{m,r}(F_q)$ for q even: start with a hyperoval in a plane; this is an even set for the design of hyperplanes. Now choose a point outside of the plane as described in Corollary 4 and obtain an even set of size $(q+2)q$ for the design of $(m-2)$-dimensional spaces. Continue this process for $m-r$ steps to obtain an even set of size $(q+2)q^{m-r-1}$ for the design $PG_{m,r}(F_q)$.
2. The regular hyperovals in the projective planes, giving vectors of weight $q+2$, actually generate the orthogonal code in the case of $m = 2$: the Singer cycle acting on a regular hyperoval will give a spanning set, as was proved by Pott [15]. In fact we believe a similar argument will prove that a regular hyperoval under a Singer cycle on $PG_{m,m-1}(F_q)$ will give a spanning set for the orthogonal binary code in this general case.

Corollary 7 *The even set of Corollary 4 of size* $(q+2)q^{m-2}$ *in* $PG_{m,m-1}(F_q)$*, q even,* $m \geq 2$*, is a set of type* $(0,2)$ *for* $m = 2$*, and of type* $(0,(q+2)q^{m-3},2q^{m-2})$ *for* $m \geq 3$*.*

Proof: We prove this by induction on m. For $m = 2$ it is clear, but we need to start the induction at $m = 3$. Let $\mathcal{H}$ be the distinguished hyperplane in $PG_3(F_q)$ that contains the hyperoval $\mathcal{S}$ of our set $\mathcal{S}^*$, and let V be the vertex point of the construction. Let H be any hyperplane (plane). If $H = \mathcal{H}$ then the result is clear. If $H \neq \mathcal{H}$, let $L = H \cap \mathcal{H}$. Then L meet $\mathcal{S}$ in 0 or 2 points. If $V \in H$ then H meets $\mathcal{S}^*$ in $2q$ or 0 points; if $V \notin H$, then H meets $\mathcal{S}^*$ in $q+2$ points, since H meets every line through V exactly once. This proves the result for $m = 3$.

Suppose now that it is true for $m-1$. With the same notation as above, H is a hyperplane in $PG_m(F_q)$. If $H = \mathcal{H}$ then H meets $\mathcal{S}^*$ in $\mathcal{S}$, i.e. in $(q+2)q^{m-3}$ points. Otherwise H meets $\mathcal{S}$ in t points, where $t \in \{0,(q+2)q^{m-4},2q^{m-3}\}$, by the induction hypothesis. If $V \in H$ then H meets $\mathcal{S}^*$ in qt points; if $V \notin H$ then H meets each line through V exactly once, in distinct points, and thus it meets $\mathcal{S}^*$ in $(q+2)q^{m-3}$ points. This gives the result. □

Note: 1. For $q \geq 4$ a power of 2, by forming a matrix whose columns are the $(q+2)q^{m-2}$ vectors of length $m+1$ corresponding to the points of the even set, and using this as the generator matrix of a q-ary code, Corollary 7 provides us with a construction of linear q-ary codes of length $(q+2)q^{m-2}$, dimension $m+1$, minimum distance q^{m-1}, and just three non-zero weights, i.e. $\{q^{m-1}, (q-1)(q+2)q^{m-3}, (q+2)q^{m-2}\}$. Thus we have, for $m \geq 3$,

$$[(q+2)q^{m-2}, m+1, q^{m-1}]_q$$

three-weight codes. We can give the weight enumerator for such a code, since we can solve the three equations we get from counting: denoting by x_{n_i} the number of hyperplanes that meet the even set $\mathcal{S}$ in n_i points, for $i = 0, 1, 2$, where $n_0 = 0$, $n_1 = (q+2)q^{m-3}$ and $n_2 = 2q^{m-2}$, the standard equations

$$\begin{aligned} x_{n_0} + x_{n_1} + x_{n_2} &= \frac{q^{m+1}-1}{q-1}, \\ n_1 x_{n_1} + n_2 x_{n_2} &= s\frac{q^m - 1}{q-1}, \\ n_1(n_1-1)x_{n_1} + n_2(n_2-1)x_{n_2} &= s(s-1)\frac{q^{m-1}-1}{q-1} \end{aligned}$$

yield

$$x_{n_0} = \frac{1}{2}q(q-1), \quad x_{n_1} = q^3\frac{q^{m-2}-1}{q-1} \quad x_{n_2} = \frac{1}{2}(q+1)(q+2).$$

Thus the weight distribution is given by the table:

Weight	0	q^{m-1}	$(q-1)(q+2)q^{m-3}$	$(q+2)q^{m-2}$
Number of words	1	$\frac{1}{2}(q^2-1)(q+2)$	$q^3(q^{m-2}-1)$	$\frac{1}{2}q(q-1)^2$

2. Corollary 7 can be generalised: using the notation of Proposition 3, suppose that $\mathcal{S}$ has type $(n_1, n_2, \ldots, n_t)$ with respect to hyperplanes of $\mathcal{H}$. Then $\mathcal{S}^*$ has intersection numbers $\{s, qn_1, qn_2, \ldots, qn_t\}$ with respect to hyperplanes, where $|\mathcal{S}| = s$. In particular, starting with an even set of size s in the plane $PG_2(F_q)$, and intersection numbers $(n_1, \ldots, n_t)$ with respect to lines, using the construction of Proposition 3 recursively, we obtain $\mathcal{S}^*$ with intersection numbers for hyperplanes $\{q^{m-3}s, q^{m-2}n_1, \ldots, q^{m-2}n_t\}$. Thus we have an $(m+1)$-dimensional code with $t+1$ non-zero weights, length $q^{m-2}s$ and minimum weight $q^{m-2}(s-n_t)$. Notice, of course, that here $s \geq q+2$ and $n_t \leq q$, so that $s - n_t \geq 2$.

3. The proof of Theorem 1 used the BCH bounds for the codes as obtained by Delsarte [5]. In the case $q = 4$ and $r = 1$ a self-contained combinatorial argument will suffice, since the upper and lower bounds are close enough to obtain the minimum weight. By observing the value of the dimension of the dual code of $C_2(PG_{m,1}(F_4))$ for values of

m for $2 \leq m \leq 10$, we obtain the following formula for the dimension (which we will prove below):

$$\dim(C_2(PG_{m,1}(F_4))^{\perp} = \frac{1}{3}(m+1)(m^2+2m+3),$$

so that the codes for $q = 4$ are

$$\left[\frac{4^{m+1}-1}{3}, \frac{1}{3}(m+1)(m^2+2m+3), 4^{m-2}6\right]_2$$

linear binary codes.

4. We can prove that the minimal sets of size 96 for $PG_{4,1}(F_4)$ described in Proposition 3 are the only ones of this size met evenly by lines: see [14].

4 Dimension formulas

The dimension of any of these codes from finite geometries can be computed from the general formula of Hamada [11, 12] (see [2, Theorem 5.8.1]), or by counting the cardinality of a set of integers that satisfy certain conditions on their q-weight, as given in [2, Theorem 5.7.9]. See also Brouwer and Wilbrink [4, Theorem 4.8]. We will use Hamada's formula:

Result 2 (Hamada [11, 12]) *Let $q = p^t$ and let $\mathcal{D}$ denote the design of points and r-dimensional subspaces of the projective geometry $PG_m(F_q)$, where $0 < r < m$. Then the p-rank of $\mathcal{D}$ is given by*

$$\sum_{s_0} \cdots \sum_{s_{t-1}} \prod_{j=0}^{t-1} \sum_{i=0}^{L(s_{j+1},s_j)} (-1)^i \binom{m+1}{i} \binom{m+s_{j+1}p-s_j-ip}{m},$$

where $s_t = s_0$ and summations are taken over all integers s_j (for $j = 0, 1, \ldots, t-1$) such that

$$r+1 \leq s_j \leq m+1, \text{ and } 0 \leq s_{j+1}p - s_j \leq (m+1)(p-1),$$

and

$$L(s_{j+1}, s_j) = \lfloor \frac{s_{j+1}p - s_j}{p} \rfloor,$$

i.e. the greatest integer not exceeding $(s_{j+1}p - s_j)/p$, i.e. the floor function.

For particular parameter sets there are more concise formulas for the p-rank: see [2, Chapter 5] or [1] for a summary of these. It turns out that Hamada's formula can be simplified in the general case, and used to construct a polynomial function in m for the dimension of the orthogonal codes.

Since the case $q = 4$ and $r = 1$ is particularly simple, we will first give a proof of this before turning to the general formula, for which the results are more technical.

4.1 Formulas for $q = 4$

Throughout this section we will work under the convention that a sum $\sum_s$ is the sum over all integer values of s for which the summands are non-zero: we will only place conditions on the limits of the summands if there are some non-zero terms which we wish to discard. Notation will be as in Hamada's theorem, Result 2.

Theorem 8 *The dimension of the orthogonal of the binary code of the design $PG_{m,1}(F_4)$ for $m \geq 2$ is $\frac{1}{3}(m+1)(m^2+2m+3)$.*

Proof: The sum under consideration is

$$\sum_{s_0}\sum_{s_1}\prod_{j=0}^{1}\sum_{i}(-1)^i\binom{m+1}{i}\binom{m+2s_{j+1}-s_j-2i}{m}$$

together with restrictions which are equivalent to

- $2 \leq s_j \leq m+1$;
- the entries in the binomial coefficients are all non-negative;
- $2s_{j+1} - s_j - 2i$ is non-negative.

Then we can rewrite the sum as

$$\sum_{s_0}\sum_{s_1}\prod_{j=0}^{1}\sum_{i}(-1)^i\binom{m+1}{i}\binom{m+2s_{j+1}-s_j-2i}{2s_{j+1}-s_j-2i}$$

$$\begin{aligned} &= \sum_{s_0}\sum_{s_1}\prod_{j=0}^{1}\sum_{i}(-1)^i\binom{m+1}{i}(-1)^{2s_{j+1}-s_j-2i}\binom{-(m+1)}{2s_{j+1}-s_j-2i} \\ &= \sum_{s_0\geq 2}\sum_{s_1\geq 2}\prod_{j=0}^{1}\binom{m+1}{2s_{j+1}-s_j} \end{aligned}$$

by an application of Vandermonde's identity (with negative upper binomial coefficient). Here all the other restrictions are implied by the standard conventions about binomial coefficients.

Now, this sum is

$$\sum_{s_0}\sum_{s_1}\binom{m+1}{2s_1-s_0}\binom{m+1}{2s_0-s_1}$$

$$-\binom{m+1}{0}\binom{m+1}{0}-\binom{m+1}{1}\binom{m+1}{1}-\binom{m+1}{3}\binom{m+1}{0}-\binom{m+1}{0}\binom{m+1}{3}$$

(i.e. we consider the full sum with no restrictions on the s_j's and just subtract off the terms which have a non-zero contribution: those for which $0 \le s_j \le 2$ and $s_{j+1} \le 2s_j$, and so on.)

We can evaluate the full sum by setting $u = 2s_1 - s_0$ so that $s_0 = 2s_1 - u$ and the sum becomes

$$\sum_{s_0}\sum_{s_1}\binom{m+1}{2s_1-s_0}\binom{m+1}{2s_0-s_1} = \sum_{u}\sum_{s_1}\binom{m+1}{u}\binom{m+1}{3s_1-2u}.$$

Observe now that the inner sum (which is by convention over all integer values of s_1) is a trisected sum:

$$\sum_{u}\binom{m+1}{u}\sum_{s_1}\binom{m+1}{3s_1-2u}.$$

The standard method for handling trisections is to use the cube root of unity in any extension field, which we shall denote by ω. Recall that if we take a generating function $f(x) = \sum a_k x^k$ then

$$\sum_k a_{2k}x^{2k} = \frac{1}{2}(f(x) + f(-x)).$$

Similarly,

$$\begin{aligned}
\sum_k a_{3k}x^{3k} &= \frac{1}{3}(f(x) + f(\omega x) + f(\omega^2 x)),\\
\sum_k a_{3k+1}x^{3k+1} &= \frac{1}{3}(f(x) + \omega^{-1}f(\omega x) + \omega^{-2}f(\omega^2 x)),\\
\sum_k a_{3k+2}x^{3k+2} &= \frac{1}{3}(f(x) + \omega^{-2}f(\omega x) + \omega^{-4}f(\omega^2 x)),
\end{aligned}$$

i.e.

$$\sum_k a_{3k+u}x^{3k+u} = \frac{1}{3}(f(x) + \omega^{-u}f(\omega x) + \omega^{-2u}f(\omega^2 x)).$$

Thus with $f(x) = (1+x)^{m+1}$,

$$\begin{aligned}
\sum_{s_1}\binom{m+1}{3s_1-2u} &= \frac{1}{3}(2^{m+1} + \omega^{-u}(1+\omega)^{m+1} + \omega^{-2u}(1+\omega^2)^{m+1})\\
&= \frac{1}{3}(2^{m+1} + \omega^{-u}(-\omega^2)^{m+1} + \omega^{-2u}(-\omega)^{m+1})\\
&= \frac{1}{3}(2^{m+1} + (-1)^{m+1}(\omega^{m+u+1} + \omega^{2(m+u+1)})).
\end{aligned}$$

Therefore the full sum is

$$\sum_{s_0}\sum_{s_1}\binom{m+1}{2s_1-s_0}\binom{m+1}{2s_0-s_1} = \sum_{u}\binom{m+1}{u}\frac{1}{3}(2^{m+1}+(-1)^{m+1}(\omega^{m+u+1}+\omega^{2(m+u+1)}))$$

$$\begin{aligned} &= \frac{4^{m+1}}{3} + (-1)^{m+1}\frac{1}{3}((1+\omega)^{m+1}\omega^{m+1} + (1+\omega^2)^{m+1}\omega^{2(m+1)}) \\ &= \frac{4^{m+1}}{3} + (-1)^{m+1}\frac{1}{3}((-\omega^3)^{m+1} + (-\omega^3)^{m+1}) \\ &= \frac{4^{m+1}+2}{3}. \end{aligned}$$

Hence the dimension in this case is

$$\frac{4^{m+1}+2}{3} - 1 - (m+1)^2 - 2\binom{m+1}{3} = \frac{4^{m+1}-1}{3} - \frac{1}{3}(m+1)(m^2+2m+3).$$

□

Corollary 9 *The dimension of the orthogonal of the binary code of the design $AG_{m,1}(F_4)$ for $m \geq 2$ is m^2+m+1.*

Proof: Use the fact that, for any m, r, and $q = p^t$, p prime,

$$\dim(C_p(AG_{m,r}(F_q))) = \dim(C_p(PG_{m,r}(F_q))) - \dim(C_p(PG_{m-1,r}(F_q)))$$

(see [2, Lemma 5.7.1] for a proof of this statement), and the formula we have just obtained. □

We observe now that the same techniques work for any value of the parameter r, where r is the dimension of the subspaces under consideration: the only change is that we have to subtract off all the terms $\binom{m+1}{2s_1-s_0}\binom{m+1}{2s_0-s_1}$ for which at least one of the $s'_j s$ is at most r. For example, the term subtracted for $r=2$ is

$$\binom{m+1}{0}^2 + \binom{m+1}{1}^2 + 2\binom{m+1}{3}\binom{m+1}{0} + \binom{m+1}{2}^2 + 2\binom{m+1}{4}\binom{m+1}{1} + 2\binom{m+1}{6}\binom{m+1}{0},$$

corresponding to (s_0, s_1) being in the set of pairs

$$\{(0,0),(1,1),(1,2),(2,1),(2,2),(2,3),(3,2),(2,4),(4,2)\}.$$

This gives the formula for the dimension of the binary code of the design $PG_{m,2}(F_4)$:

$$\frac{4^{m+1}-1}{3} - \frac{1}{360}(m+1)(m+2)(m^4+18m^3+29m^2+72m+180).$$

4.2 The general Hamada formula

We now consider the situation for general values of the main parameters m, r, p, t. Clearly these come into play at different points of the analysis: the parameter p being 2 was essential in the evaluation of the sum over i at the begining, and the parameter t being 2 enabled us to rewrite the sum $\sum_{s_0}\sum_{s_1}\binom{m+1}{2s_1-s_0}\binom{m+1}{2s_0-s_1}$. If $t \geq 2$, then we will have a larger product to evaluate. Furthermore, we will have more terms to subtract off from the full sum to compute the sum restricted to $s_j \geq r+1$.

Proof of Theorem 2: Write

$$N_r = \sum_{\underline{s} \geq r} \prod_{j=1}^{t} \sum_i (-1)^i \binom{m+1}{i} \binom{-(m+1)}{ps_{j+1} - s_j - pi},$$

where $\underline{s}$ denotes the t-tuple $(s_1, s_2, \ldots, s_t)$ in Hamada's formula. If we define

$$f(x) = \frac{(1-x^p)^{m+1}}{(1-x)^{m+1}},$$

then we obtain

$$\sum_i (-1)^i \binom{m+1}{i} \binom{-(m+1)}{u-pi} = [x^u]\, f(x),$$

where the right-hand side denotes the coefficient of x^u in $f(x)$. Note that $f(x)$, although presented as a rational function, is a polynomial in x of degree $(p-1)(m+1)$, and $f(1) = p^{m+1}$. Thus

$$N_r = \sum_{\underline{s} \geq r} \prod_{j=1}^{t} \left[x_j^{ps_{j+1}-s_j}\right] f(x_j).$$

We now change variables to allow us to compute N_0. Define $u_j = ps_{j+1} - s_j$ for $j = 1, \ldots, t-1$, so that

$$\begin{aligned} ps_1 - s_t &= p^2 s_2 - pu_1 - s_t \\ &\vdots \\ &= p^t s_t - p^{t-1}u_{t-1} - p^{t-2}u_{t-2} - \ldots - p^2 u_2 - pu_1 - s_t \\ &= (p^t - 1)s_t - p^{t-1}u_{t-1} - p^{t-2}u_{t-2} - \ldots - p^2 u_2 - pu_1. \end{aligned}$$

Thus

$$\begin{aligned} N_0 &= \sum_{\underline{u} \geq 0} \sum_{s_t \geq 0} \left(\prod_{j=1}^{t-1} \left[x_j^{u_j}\right] f(x_j) \right) \left[x_t^{(p^t-1)s_t - p^{t-1}u_{t-1} - \ldots - pu_1}\right] f(x_t) \\ &= \sum_{\underline{u} \geq 0} \left(\prod_{j=1}^{t-1} \left[x_j^{u_j}\right] f(x_j) \right) \sum_{s_t \geq 0} \left[x_t^{(p^t-1)s_t - p^{t-1}u_{t-1} - \ldots - pu_1}\right] f(x_t). \end{aligned}$$

Now let $g(x) = \sum_{i=0}^{\infty} a_i x^i$. Then, with $b = q-1$ and ω a primitive $(q-1)^{th}$ root of unity, for any integer a

$$\sum_{i \equiv a (mod\, b)} a_i x^i = \frac{1}{b} \sum_{l=0}^{b-1} \omega^{-la} g(\omega^l x),$$

so that

$$\sum_{s_t \geq 0} \left[x_t^{(p^t-1)s_t - p^{t-1}u_{t-1} - \ldots - pu_1} \right] f(x_t) = \frac{1}{p^t - 1} \sum_{l=0}^{p^t-2} \omega^{l(pu_1 + p^2 u_2 + \ldots + p^{t-1}u_{t-1})} f(\omega^l)$$

and thus

$$\begin{aligned} N_0 &= \frac{1}{p^t-1} \sum_{l=0}^{p^t-2} \sum_{\underline{u} \geq 0} \left(\prod_{j=1}^{t-1} \left[x_j^{u_j} \right] \omega^{lp^j u_j} f(x_j) \right) f(\omega^l) \\ &= \frac{1}{p^t-1} \sum_{l=0}^{p^t-2} f(\omega^l) \prod_{j=1}^{t-1} \sum_{\underline{u} \geq 0} \left[x_j^{u_j} \right] \omega^{lp^j u_j} f(x_j) \\ &= \frac{1}{p^t-1} \sum_{l=0}^{p^t-2} f(\omega^l) \prod_{j=1}^{t-1} f(\omega^{lp^j}) \\ &= \frac{1}{p^t-1} \sum_{l=0}^{p^t-2} \prod_{j=1}^{t} f(\omega^{lp^j}), \end{aligned}$$

since $\omega^{p^t} = \omega$.

If $l = 0$ then $f(\omega^{lp^j}) = f(1) = p^{m+1}$. Further, if $1 \leq l \leq p^t - 2$, then $\prod_{j=1}^{t} f(\omega^{lp^j}) = 1$, as is easily seen by writing out terms: the numerators and denominators cancel cyclically. Hence

$$N_0 = \frac{p^{t(m+1)} + p^t - 2}{p^t - 1} = \frac{p^{t(m+1)} - 1}{p^t - 1} + 1.$$

Finally, to determine N_{r+1}, which is the dimension of the code arising from the r-dimensional subspaces, we need to subtract off all terms in the original sum which have some $s_j \leq r$. There are only finitely many of these (a priori upper bounds are easy to obtain on their number). For any fixed p, r, t, these terms are easily computed: they contribute a polynomial amount to the sum, and thus

$$N_{r+1} = N_0 - g(m) = \frac{p^{t(m+1)} - 1}{p^t - 1} + 1 - g(m) \tag{1}$$

where $g(m) = h(m) + 1$ is a polynomial of degree $(q-1)r$. The proof of Theorem 2, as stated in the introduction, is now complete. □

Note: To compute the polynomial $g(m)$ in any particular case we need to evaluate

$$\sum_{\underline{s}} \prod_{j=1}^{t} \sum_{i} (-1)^i \binom{m+1}{i} \binom{m + ps_{j+1} - s_j - pi}{m}$$

over $\underline{s}$ where at least one of the s_i's satisfies $s_i \leq r$. Notice that $s_i = 0$ only occurs if all the s_j's are 0, and the term contributed is the term "1" in Equation (1).

5 Minimum weight in the non-binary case

Values for the minimum weight of the orthogonal codes of the p-ary codes of the geometry for $p > 2$ are known, in general, only for $q = p$. In this case the minimum weight for the designs of points and r-dimensional subspaces or flats in an m-dimensional projective or affine geometry is $2p^{m-r}$, since the codes here are generalized Reed-Muller codes and the lower and upper bounds in the affine case of Result 1 actually coincide. The minimum vectors are not constant in this case, and unlikely to be in the general case. Words of weight $2q^{m-r}$ are easily constructed, and this does provide an upper bound for the minimum weight: see [2, Chapter 5].

In some cases, however, we can construct words of smaller weight in the orthogonal code: consider a projective (or affine) plane Π of square order q^2, where Π need not be desarguesian but we suppose it contains a Baer subplane, π. If $\mathcal{Q}$ is the set of points of π, and L is a line of Π that is a line of π, i.e. meets $\mathcal{Q}$ in $q+1$ points, then, writing v^X for the incidence vector of a set X of points (see Section 2), we find that the vector $v^{\mathcal{Q}} - v^L$ is in the orthogonal code of the design, and is of weight $2q^2 - q$. This set can clearly be found in an affine plane as well by taking for the line at infinity a tangent to the Baer subplane that meets L in π.

In fact, a construction as in Proposition 3, but placing signs on added points, will yield a word in the orthogonal code for $PG_{m,1}(F_q)$ from a word in the orthogonal for $PG_{m-1,1}(F_q)$: we use the sign + for points on lines through V that meet the set for the hyperplane in a point with a positive sign, and $-$ for points on lines through V that meet in points with a negative sign. This will provide a vector in the orthogonal code for $PG_{m,1}(F_q)$ of weight qs, where s is the weight of the word in the orthogonal code for the hyperplane. For example, using the above construction with a Baer subplane, we get a word of weight $(2q^2 - q)(q^2)^{m-2}$ in the orthogonal to the p-ary code for $PG_{m,1}(F_{q^2})$.

6 Appendix

We include here some computations of the polynomials $h(m)$ from Theorem 2. These, and further polynomials, can be found at the web site

http://www.math.clemson.edu/faculty/Key/poly.ps or Key/poly1 for a text file with further polynomials.

In each case the polynomial given is the value of the p-rank of the orthogonal (dual) code of the design of point and r-dimensional subspaces over F_q, where q is a power of the prime p, in the projective space of dimension m. The degree is $(q-1)r$ and the coefficient of $m^{(q-1)r}$ is $\frac{2}{((q-1)r)!}$.

$$q = 4,\ r = 2$$

$\frac{2}{6!}(m+2)(m+1)(m^4+18m^3+29m^2+72m+180)$

$$q = 4,\ r = 3$$

$\frac{2}{9!}(m+1)(m^8+44m^7+826m^6+1064m^5+9289m^4+25676m^3+85644m^2+149616m+181440)$

$$q = 4,\ r = 4$$

$\frac{2}{12!}(m+2)(m+1)(m^{10}+75m^9+2490m^8+37590m^7-164247m^6+1245795m^5+167660m^4+8592060m^3+26605296m^2+43346880m+119750400)$

$$q = 4,\ r = 5$$

$\frac{2}{15!}(m+1)(m^{14}+119m^{13}+6461m^{12}+181909m^{11}+2735733m^{10}-27390363m^9+226658003m^8-287580293m^7+2393897506m^6+5448887444m^5+35100765336m^4+92455219584m^3+296459386560m^2+548983008000m+653837184000)$

$$q = 4,\ r = 6$$

$\frac{2}{18!}(m+2)(m+1)(m^{16}+168m^{15}+13060m^{14}+554736m^{13}+13436374m^{12}+165307968m^{11}-5539922740m^{10}+73291099728m^9-438573851551m^8+2073529633560m^7-4530978319000m^6+15864574614336m^5+12967596594576m^4+90381188306304m^3+383263652954880m^2+567413363865600m+1600593426432000)$

$$q = 4,\ r = 7$$

$\frac{2}{21!}(m+1)(m^{20}+230m^{19}+24795m^{18}+1529310m^{17}+57436506m^{16}+1267975260m^{15}+14063772070m^{14}-985235601460m^{13}+18063909964581m^{12}-157011781481490m^{11}+925909983165375m^{10}-3095429863328010m^9+9832975608844816m^8-5173838215516720m^7+8539285088486136 0m^6+199017299982872160m^5+1383418617290868096m^4+3716165306079198720m^3+11374243844734310400m^2+21557619010013184000m+25545471085854720000)$

$$q = 4,\ r = 8$$

$\frac{2}{24!}(m+2)(m+1)(m^{22}+297m^{21}+41657m^{20}+3426555m^{19}+177442716m^{18}+5730690042m^{17}+105277470562m^{16}+690891106950m^{15}-198150319603159m^{14}+5776269732740397m^{13}-83669958539637483m^{12}+79155204261090457 5m^{11}-514210113479394853 4m^{10}+251791744409363473 92m^{9}-882279893511919228 48m^{8}+265253484517196015280m^{7}-435354887506633753824m^{6}+126954156158451516787 2m^{5}+202603808781625231411 2m^{4}+750913783446024152064 0m^{3}+382656345994171404288 00m^{2}+545752937302906798080 00m+155112100433309859840000)$

$$q = 8,\ r = 1$$

$\frac{2}{7!}(m+1)(m^6+27m^5+295m^4+825m^3+1744m^2+2148m+1680)$

$$q = 8,\ r = 2$$

$\frac{2}{14!}(m+2)(m+1)(m^{12}+102m^{11}+4697m^{10}+129030m^9+2353263m^8+29994426m^7+213181331m^6+528949410m^5+1498825636m^4+4977145272m^3+8664003072m^2+13144844160m+14529715200)$

$$q = 8,\ r = 3$$

$\frac{2}{21!}(m+1)(m^{20}+230m^{19}+24795m^{18}+1664970m^{17}+78056826m^{16}+2714110860m^{15}+72575557990m^{14}+1519524165140m^{13}+24975789135141m^{12}+296234479265790m^{11}+2094571157806335m^{10}+3092495888499810m^9+3793791631060273 6m^8+1248176839084959 20m^7+5524880142221656 80m^6+1609891392776482080m^5+4701785318691175296m^4+1031887774033470720 0m^3+1903468921294187520 0m^2+2322010204893388800 0m+17030314057236480000)$

$$q = 8,\ r = 4$$

$\frac{2}{28!}(m+2)(m+1)(m^{26}+403m^{25}+77350m^{24}+9410050m^{23}+814656895m^{22}+53417849485m^{21}+2756902291000m^{20}+114771333047800m^{19}+3910733252961535m^{18}+109821287136823405m^{17}+2544108153603922750m^{16}+4843941217548046705 0m^{15}+7253951829332523452 65m^{14}+7424483412511957542595m^{13}+2797689422436570693 8500m^{12}-2857380469951732049 89700m^{11}+4445548431210952741527280m^{10}-6305712569088753866405360m^9+4999046722726020563570 4000m^8+1380998790843077317708 36800m^7+4163810217047868980679 69024m^6+2360348597925294762783209472m^5+5382361320799704175230566400m^4+1610790006518547401556172 8000m^3+3225783601346384138747 9040000m^2+4491864056282863422210 0480000m+50814724101952310083584000000)$

$$q = 9,\ r = 1$$

$\frac{2}{8!}(m+2)(m+1)(m^6+33m^5+445m^4+3135m^3+7114m^2+9432m+10080)$

$$q = 9,\ r = 2$$

$\frac{2}{16!}(m\ +\ 1)(m^{15}\ +\ 135m^{14}\ +\ 8365m^{13}\ +\ 315315m^{12}\ +\ 8078707m^{11}\ +\ 148873725m^{10}\ +\ 2036157695m^9 + 21021002145m^8 + 143137602608m^7 + 538812794520m^6 + 1275930459440m^5\ +\ 3608050577040m^4\ +\ 7656330893184m^3\ +\ 13485570405120m^2\ +\ 15114532608000m\ +\ 10461394944000)$

$$q = 9,\ r = 3$$

$\frac{2}{16!}(m\ +\ 3)(m\ +\ 2)(m\ +\ 1)(m^{21}\ +\ 294m^{20}\ +\ 40775m^{19}\ +\ 3547110m^{18}\ +\ 217077546m^{17}\ +\ 9935114364m^{16}\ +\ 352888691950m^{15}\ +\ 9963304105020m^{14}\ +\ 226720656078581m^{13}\ +\ 4175171164790094m^{12}\ +\ 61915308721874475m^{11}\ +\ 730273881191085630m^{10}\ +\ 6125341298104500496m^9\ +\ 25536649010991259344m^8\ +\ 26885942701524930800m^7\ +\ 42425748486919351344 0m^6\ +\ 17410993976855703893 76m^5\ +\ 31578575140197423959 04m^4\ +\ 12683891387466885888000m^3 + 25475132724320072908800m^2 + 34014467173874761728000m + 51704033477769953280000)$

$$q = 16,\ r = 1$$

$\frac{2}{15!}(m+1)(m^{14}+119m^{13}+6461m^{12}+211939m^{11}+4687683m^{10}+73870797m^9+854224943m^8+7093943857m^7 + 40012868896m^6 + 123817477784m^5 + 293768734896m^4 + 511468133904m^3 + 689704398720m^2 + 621631584000m + 326918592000)$

$$q = 25,\ r = 1$$

$\frac{2}{24!}(m+4)(m+3)(m+2)(m+1)(m^{20}+290m^{19}+39615m^{18}+3388650m^{17}+203522946m^{16}+9121022580m^{15}\ +\ 316404601630m^{14}\ +\ 8697685698500m^{13}\ +\ 192374726145381m^{12}\ +\ 3456380926339770m^{11}\ +\ 50707508702323395m^{10}\ +\ 608324168861056050m^9\ +\ 5955504667302749896m^8\ +\ 4730620757624308856 0m^7\ +\ 3018076000552789413 60m^6\ +\ 1522207900529046496800m^5 + 5386524779294396971776m^4 + 1176197859040619738880 0m^3 + 1584900849818713190400 0m^2 + 1682858170759772160000 0m + 1292600836944248832000 0)$

References

[1] E. F. Assmus, Jr. and J. D. Key. Polynomial codes and finite geometries. To appear (1998) in Handbook of Coding Theory, edited by V. S. Pless and W. C. Huffman.

[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] Ian F. Blake and Ronald C. Mullin. *The Mathematical Theory of Coding*. New York: Academic Press, 1975.

[4] Andries E. Brouwer and Henny A. Wilbrink. Block designs. In F. Buekenhout, editor, *Handbook of Incidence Geometry*, pages 349–382. Elsevier, 1995. Chapter 8.

[5] P. Delsarte. *BCH* bounds for a class of cyclic codes. *SIAM J. Appl. Math.*, 19:420–429, 1970.

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

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

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

[9] P. Dembowski. *Finite Geometries*. Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 44. Berlin, Heidelberg, New York: Springer-Verlag, 1968.

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

[11] N. Hamada. The rank of the incidence matrix of points and d-flats in finite geometries. *J. Sci. Hiroshima Univ. Ser. A-I*, 32:381–396, 1968.

[12] N. Hamada. On the p-rank of the incidence matrix of a balanced or partially balanced incomplete block design and its applications to error correcting codes. *Hiroshima Math. J.*, 3:153–226, 1973.

[13] J. W. P. Hirschfeld. *Finite Projective Spaces of Three Dimensions*. Oxford: Clarendon Press, 1985. Oxford Mathematical Monographs.

[14] J. D. Key and M. J. de Resmini. Even sets for projective geometries over F_4. In preparation.

[15] Alexander Pott. On abelian difference set codes. *Des. Codes Cryptogr.*, 2:263–271, 1992.