Subcodes of the Projective Generalized Reed-Muller Codes Spanned by Minimum-Weight Vectors

Peng Ding
Fair Isaac and Company, Inc.
200 Smith Ranch Road
San Rafael CA 94903-1996

Jennifer D. Key*
Department of Mathematical Sciences
Clemson University
Clemson SC 29634

February 3, 2003

Abstract

We use methods of Mortimer [19] to examine the subcodes spanned by minimum-weight vectors of the projective generalized Reed-Muller codes and their duals. These methods provide a proof, alternative to a dimension argument, that neither the projective generalized Reed-Muller code of order r and of length $\frac{q^m-1}{q-1}$ over the finite field F_q of prime-power order q, nor its dual, is spanned by its minimum-weight vectors for $0 < r < m-1$ unless q is prime. The methods of proof are the projective analogue of those developed in [17], and show that the codes spanned by the minimum-weight vectors are spanned over F_q by monomial functions in the m variables. We examine the same question for the subfield subcodes and their duals, and make a conjecture for the generators of the dual of the binary subfield subcode when the order r of the code is 1.

Dedicated to R. C. Mullin[1] *on his* 65^{th} *birthday*

1 Introduction

In [17, Theorem 1] we established the range of values of r, t and m, where $0 \leq r \leq m(q-1)$, for which the generalized Reed-Muller code $\mathcal{R}_{F_q}(r,m)$ of length q^m over the field F_q of order $q = p^t$, for p a prime, is spanned by its minimum-weight vectors. The code spanned by the minimum-weight vectors had been examined previously by Delsarte [14, Theorem 10] who, viewing it as an extended cylic code, gave its dimension as the number of elements

*Both authors acknowledge support of ONR grant #N00014-00-1-0565, and the second author acknowledges support of NSF grant #9730992.

[1] The chapter on the generalized Reed-Muller codes in the book [5] by Blake and Mullin was a stimulating influence in the study of these codes.

in a defining set for the cyclic code. The interest in this question arose from this property in the codes of the designs from finite projective and affine geometry, which are p-ary subfield subcodes of the generalized Reed-Muller codes, where p is the characteristic of the geometry. The minimum-weight vectors in the codes are the incidence vectors of the blocks of the design, along with scalar multiples, and these generate (i.e. span) the corresponding subfield subcode, as was shown in work of Delsarte, Goethals and MacWilliams [13]: see [2, Chapter 5] or [3] for full references to this work. These properties were of importance in the application of majority logic decoding using the duals of these codes.

We look here at some of the non-primitive generalized Reed-Muller q-ary codes, and ask if we can use the methods of Mortimer to answer the same question. Specifically we look at those of length $\frac{q^m-1}{q-1}$, which are generally called the projective generalized Reed-Muller codes. Using the projective analogue of the methods of Mortimer we show in Theorem 2, in Section 3, that the projective generalized Reed-Muller q-ary codes of order r where $0 < r < m-1$ are only spanned by their minimum-weight vectors if q is a prime. The proof of this theorem requires a more general result, Theorem 1, which is a projective analogue of Mortimer's results, and leads to Corollary 1 which states that the subcode spanned by the minimum-weight vectors is spanned by monomials. This result and the fact that the minimum-weight vectors are known, leads to the new proof. That the subcode spanned by the minimum-weight vectors is not the full projective generalized Reed-Muller code can also be proved by using a dimension argument: see Proposition 1, and the short proof there.

We also look at the dual codes of the projective generalized Reed-Muller codes, and of the subfield subcodes. For the duals of the projective Reed-Muller q-ary codes, the results are the same as for the codes, i.e. they are not spanned by minimum-weight vectors except in the prime case. These results are in Section 4. We have some partial results for the duals of the subfield subcodes. This is an open problem, with even the minimum weight unknown in general. The dual codes are not generalized Reed-Muller codes, i.e. they are not polynomial codes. In the case where $p = 2$, and the order $r = 1$, i.e. the code is the dual of the code of points and hyperplanes of a projective geometry over F_q where $q = 2^t$, the minimum weight is known and the nature of the minimum-weight words is also known by Ding [15]: they are just the incidence vectors of the hyperovals, and of size $q + 2$. In all known cases the dual sub-field subcode is spanned by these codewords, and we formulate a conjecture that this is always the case: see Conjecture 1. These results are in Section 5.

2 Terminology and Background

The proofs in this paper are in most cases the projective parallels of the proofs and concepts in [17]. We will quote some of the definitions and results that are given in that paper, but not reproduce the proofs. Where they are used we refer the reader to the relevant proof in [17]. We remark again that the ideas of the proof here are based on those used by Mortimer [19], and used also in [3, Section 5.5].

We will use standard terminology for the structures that we need, and in particular we will follow that used in [2] and [3]. Also we will follow [17].

Traditionally, there are three approaches to the study of the generalized Reed-Muller codes: the 1-variable approach, the multivariable approach and the group-algebra approach. The various different approaches can be found in [2, Chapter 5] or in Blake and Mullin [5]. Here we mainly employ the multivariable approach.

Let $q = p^t$, where p is a prime, and let V be a vector space of dimension m over F_q. We take V to be the space F_q^m of m-tuples, with standard basis. Denote by $PG_{m-1}(F_q)$, or $PG(V)$, the projective geometry of V. Our codes will be q-ary codes, and the ambient space will be the function space F_q^V. Each element f of F_q^V can be given as a function of m variables, i.e. if $x = (x_1, x_2, \ldots, x_m) \in V$, then $f \in F_q^V$ is given by

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

Clearly, f is a linear combination of the following linearly independent monomial functions:

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

A monomial $m = x_1^{i_1} x_2^{i_2} \ldots x_m^{i_m} \in \mathcal{M}$ with total degree

$$r = \sum_{k=1}^{m} i_k \equiv 0 \pmod{q-1},$$

can be evaluated on the representatives of the points of $PG_{m-1}(F_q)$, since for any $\lambda \in F_q^\times$ and $\mathbf{x} \in PG_{m-1}(F_q)$,

$$m(\lambda \mathbf{x}) = \lambda^r m(\mathbf{x}) = m(\mathbf{x}).$$

The **projective generalized Reed-Muller** codes can now be defined as follows (see [3, Definition 5.35]):

Definition 1 *Let $V = F_q^m$ be the vector space of m-tuples, for $m \geq 1$, over the finite field F_q of order q, where $q = p^t$ and p is a prime. Let $\mathcal{P}$ be the set of points of $PG(V)$. For any r such that $0 \leq r < m$, the r^{th}-order projective generalized Reed-Muller code $\mathcal{P}_{F_q}(r, m)$ is the subspace of $F_q^{\mathcal{P}}$ spanned by the following m-variable polynomial functions, reduced modulo $x_i^q - x_i$:*

$$\mathcal{P}_{F_q}(r, m) = \langle x_1^{i_1} x_2^{i_2} \cdots x_m^{i_m} \mid \sum_{k=1}^{m} i_k \equiv 0 \pmod{q-1},\ \sum_{k=1}^{m} i_k \leq r(q-1) \rangle,$$

where these polynomials are only evaluated on a set of vectors representative of the set of points $\mathcal{P}$ of $PG(V)$.

These codes are thus codes of length $n = \frac{q^m - 1}{q-1}$ and the codewords have the form $(f(P_1), \ldots, f(P_n))$, for any $f \in \mathcal{P}_{F_q}(r, m)$, and some ordering of the set $\mathcal{P} = \{P_1, \ldots, P_n\}$ of projective points. Clearly, if $r < \nu$ then $\mathcal{P}_{F_q}(r, m) \subseteq \mathcal{P}_{F_q}(\nu, m)$. The punctured Reed-Muller code $\mathcal{R}_{F_2}(r, m)^*$ (see Chapter 5 [2]) is $\mathcal{P}_{F_2}(r, m)$. It is well known that $\mathcal{R}_{F_2}(r, m)$

is spanned by the incidence vectors of $(m-r-1)$-dimensional subspaces in $PG_{m-1}(F_2)$, hence so is $\mathcal{P}_{F_2}(r,m)$.

A projective linear transformation $\gamma \in PGL_m(F_q)$, the projective general linear group, is given by

$$\gamma : \mathbf{v} \mapsto \mathbf{v}A,$$

where $\mathbf{v} \in V = F_q^m$ and A is a non-singular $m \times m$ matrix over F_q. Then

$$\mathbf{v}\gamma^{-1} = \mathbf{v}A^{-1}$$

and for $f \in \mathcal{P}_{F_q}(r,m)$, $f\gamma$ is defined by

$$f\gamma(\mathbf{x}) = f(\mathbf{x}A^{-1})$$

where $\mathbf{x} = (x_1, x_2, \ldots, x_m)$. It follows from the proof of Lemma 4 in [17] that $f\gamma$ can be **obtained** from f by transformations of type $\varepsilon_{i,j}^b$, where $\varepsilon_{i,j}^b$ is given by (following Definition 2 [17])

$$(x_1^{a_1}x_2^{a_2}\ldots x_m^{a_m})\varepsilon_{i,j}^b = \binom{a_i}{b} x_1^{a_1}x_2^{a_2}\ldots x_i^{a_i-b}\ldots x_j^{a_j+b}\ldots x_m^{a_m},$$

and thus the degree of $f\gamma$ is the same as that of f or reduced by multiples of $(q-1)$. Therefore $f\gamma \in \mathcal{P}_{F_q}(r,m)$, so that $\mathcal{P}_{F_q}(r,m)$ is invariant under $PGL_m(F_q)$.

Since $PGL_m(F_q)$ contains a Singer cycle whose action is regular on the projective points, it follows that the projective generalized Reed-Muller code $\mathcal{P}_{F_q}(r,m)$ is a cyclic code with length $n = \frac{q^m-1}{q-1}$, and hence it has a generator polynomial which is in the ideal corresponding to $\mathcal{P}_{F_q}(r,m)$ in the polynomial ring $F_q[x]/(x^n-1)$. The dimension can be obtained from these facts and the following holds (see [3, Proposition 5.36]):

Result 1 *The dimension of $\mathcal{P}_{F_q}(r,m)$ is*

$$|\{j \mid 0 \le j \le \frac{q^m-1}{q-1},\ \mathrm{wt}_q(j(q-1)) \le r(q-1)\}|.$$

Here the weight $\mathrm{wt}_q(j)$ is defined as follows:

Definition 2 *For any integers, $k \ge 0$ and $q > 1$, the **q-weight** of k, written $\mathrm{wt}_q(k)$, is*

$$\mathrm{wt}_q(k) = \sum_{\nu=0}^{\infty} k_\nu,$$

where $k = \sum_{\nu=0}^{\infty} k_\nu q^\nu$ is the q-ary expansion of k.

As in the case of the generalized Reed-Muller code, codewords in $\mathcal{P}_{F_q}(r,m)$ may have geometric significance, and the incidence vectors of some projective subspaces can be found in the codes. For example, the polynomial

$$p(x_1, x_2, \ldots x_m) = \prod_{i=1}^{r}(1 - x_i^{q-1}) \tag{1}$$

has degree $r(q-1)$ and is zero in $PG_{m-1}(F_q)$ unless

$$x_i = 0, \text{ for } i = 1, \ldots, r.$$

Thus it gives a vector of weight $\frac{q^{m-r}-1}{q-1}$ which is the incidence vector of an $(m-r-1)$-dimensional projective subspace. In fact, Equation (1) gives a minimum-weight codeword of $\mathcal{P}_{F_q}(r,m)$. More precisely, the following holds, from [13, Theorem 3.5.1, 3.6.1]:

Result 2 *For any m, q, and r, the minimum weight of $\mathcal{P}_{F_q}(r,m)$ is $(q^{m-r}-1)/(q-1)$. Further, all the minimum-weight codewords are scalar multiples of the incidence vectors of the $(m-r-1)$-dimensional projective subspaces of $PG_{m-1}(F_q)$, and can be obtained from the vectors corresponding to the polynomial in Equation (1) by suitable projective transformation in the projective general linear group $PGL_m(F_q)$.*

3 Minimum-weight generators

In this section we will examine the subcodes of the projective generalized Reed-Muller codes spanned by the minimum-weight vectors, showing that they are spanned by monomials, but that they are not equal to the full code, in general, unless q is a prime. First we need a projective parallel of Theorem 5.31 in [3] (that result is due originally to Mortimer [19]).

Theorem 1 *Let H be a subspace of F_q^V where $V = F_q^m$, and suppose that the degree of each monomial term of a polynomial function $f \in F_q^V$ is divisible by $q-1$. Then H is invariant under $PGL(V)$ if and only if*

- *H is invariant under transformations of the type $\varepsilon_{i,j}^b$;*
- *H is spanned by monomials.*

Proof: Suppose that H is invariant under transformations of type $\varepsilon_{i,j}^b$. From the proof of Lemma 4 in [17] (or see [3, Theorem 5.30]), we know that H is invariant under transvections, in particular under linear transformations given by

$$\gamma_{i,j}^u : (x_1, x_2, \ldots, x_m) \mapsto (x_1, \ldots, x_i - ux_j, \ldots, x_m).$$

The group $PGL(V)$ is generated by transvections and dilations η_i^u defined by

$$\eta_i^u : (x_1, x_2, \ldots, x_m) \mapsto (x_1, \ldots, ux_i, \ldots, x_m)$$

for $i = 1, 2, \ldots, m$, where u is a non-zero element in F_q. Suppose also that H is spanned by monomials. Each η_i^u maps each monomial to a scalar multiple of itself, hence H is invariant under η_i^u. Therefore H is invariant under $PGL(V)$.

Conversely, suppose that H is invariant under $PGL(V)$. It can be seen that H is invariant under the transformation

$$\lambda_i^k = -\sum_{u\in F_q^\times} u^k \eta_i^u,$$

for $0 \le k \le q-1$, and $1 \le i \le m$. Then

$$\begin{aligned}(x_1^{a_1}x_2^{a_2}\dots x_m^{a_m})\lambda_i^k &= (-\sum_{u\in F_q^\times} u^{k-a_i})x_1^{a_1}x_2^{a_2}\dots x_m^{a_m} \\ &= \begin{cases} x_1^{a_1}x_2^{a_2}\dots x_m^{a_m} & \text{if } k\equiv a_i \pmod{(q-1)} \\ 0 & \text{otherwise}\end{cases}.\end{aligned}$$

Suppose that H is not spanned by monomials; then there exists a polynomial function $f \in H$ such that each monomial term of f is not in H. Moreover f can be chosen with a minimal number of monomial terms which are not in H. Choosing the monomial term g of f which contains a maximal number of exponents which are not $q-1$ or 0, we can assume that

$$g = x_1^{a_1}x_2^{a_2}\dots x_r^{a_r}x_{r+1}^{q-1}\dots x_{r+s}^{q-1}$$

where $0 < a_i < q-1$.

We observe that $(f)\lambda_1^{a_1}\dots\lambda_r^{a_r} \in H$ and contains the terms of f which contain x_i raised to the exponent a_i for $i = 1, 2, \dots, r$. By the minimality of the number of terms of f, we have $f = (f)\lambda_1^{a_1}\dots\lambda_r^{a_r}$. Thus every monomial of f begins with $x_1^{a_1}x_2^{a_2}\dots x_r^{a_r}$, and x_i has exponent $q-1$ or 0 for $r < i \le r+s$.

Now choose a monomial term g' in f with maximal number of exponents $q-1$, and assume that

$$g' = x_1^{a_1}x_2^{a_2}\dots x_r^{a_r}x_{r+1}^{q-1}\dots x_{r+s'}^{q-1}.$$

The polynomial function $(f)\varepsilon_{r+1,1}^{q-1}\varepsilon_{r+2,1}^{q-1}\dots\varepsilon_{r+s',1}^{q-1}$ is in H and contains only terms of f with exponent $q-1$ for x_i where $i = r+1, r+2, \dots, r+s'$. According to the minimality of the number of terms of f, each monomial of f has exponent $q-1$ for x_i when $r+1 \le i \le r+s'$. On the other hand, by the maximality of the number of exponents $q-1$ of g', we can conclude that every monomial term of f is g'. This contradicts our hypothesis and completes the proof. □

Let C be the code spanned by the minimum-weight codewords in $\mathcal{P}_{F_q}(r,m)$. Clearly C is invariant under $PGL_m(F_q)$. According to Theorem 1, we have the following corollary:

Corollary 1 *The code C spanned by the minimum-weight codewords of $\mathcal{P}_{F_q}(r,m)$, for any $m \ge 1$ and $0 \le r \le (m-1)$, has a monomial basis.*

We know that a minimum-weight codeword can be given by Equation (1), and hence all the monomials on the right hand side of the equation are in C. These have the form

$$x_{i_1}^{q-1}x_{i_2}^{q-1}\dots x_{i_k}^{q-1} \tag{2}$$

for $1 \leq i_1, i_2, \ldots, i_k \leq r$.

From Result 2 we have the following lemma which is similar to Lemma 4 in [17]

Lemma 1 *Let $\mathcal{B}$ be the monomial basis of the code C spanned by minimum-weight codewords of $\mathcal{P}_{F_q}(r,m)$. Any monomial in $\mathcal{B}$ can be obtained from a monomial of type (2) with the same degree by some transformations of type $\varepsilon^b_{i,j}$.*

In the case when $q = p$ is prime, the answer to our question is known from [3, Theorem 5.41]:

Result 3 *For p a prime, $\mathcal{P}_{F_p}(r,m)$, for $0 \leq r \leq m-1$, is spanned by the incidence vectors of all $(m-r-1)$-dimensional subspaces of $PG_m(F_p)$, and these (and their scalar multiples) are the minimum-weight codewords.*

We now consider $\mathcal{P}_{F_q}(r,m)$ where $q = p^t$ and $t > 1$. First we notice, from an example, that $\mathcal{P}_{F_q}(r,m)$, unlike the prime case, is not necessarily spanned by its minimum-weight codewords.

Example 1 In the code $\mathcal{P}_{F_4}(1,3)$, the incidence polynomial (1) is

$$p(x_1,x_2,x_3) = 1 - x_1^3.$$

According to Lemma 1, all the monomials of degree 3 must be obtained from x_1^3 by transformations of type $\varepsilon^b_{i,j}$. It is easy to verify that the monomial $x_1x_2x_3$ is not in the code C spanned by the minimum-weight vectors since $(x_1^3)\varepsilon^1_{1,2}\varepsilon^1_{1,3} = 0$. □

It is clear that the extreme cases, $\mathcal{P}_{F_q}(0,m)$ and $\mathcal{P}_{F_q}(m-1,m)$, are spanned by minimum-weight codewords. For the rest, we need first the following definition (Definition 3) and lemma (Lemma 7), respectively, from [17]:

Definition 3 *Given a monomial $x_1^{a_1}x_2^{a_2}\ldots x_m^{a_m}$, where $0 \leq a_i \leq q-1$ for $1 \leq i \leq m$ and $q = p^t$, suppose that the p-ary expansion of a_i is $a_i = \sum_{j=0}^{t-1} a_{i,j}p^j$, where $0 \leq a_{i,j} \leq p-1$. For $0 \leq k \leq t-1$, the k-**component-degree** of $x_1^{a_1}x_2^{a_2}\ldots x_m^{a_m}$, denoted by cdeg_k, is defined by*

$$\mathrm{cdeg}_k(x_1^{a_1}x_2^{a_2}\ldots x_m^{a_m}) = \sum_{i=1}^{m} a_{i,k}.$$

Result 4 *Let $M_A = x_1^{a_1}x_2^{a_2}\ldots x_m^{a_m}$ and $M_B = x_1^{b_1}x_2^{b_2}\ldots x_m^{b_m}$ be two monomials and let A_k, B_k be their k-component-degrees respectively, for $0 \leq k \leq t-1$. Suppose that $A_k = B_k$, for $0 \leq k \leq l-1$ and $A_l < B_l$ for some $l \leq t-1$. Then M_B cannot be obtained from M_A by transformations of the type $\varepsilon^b_{i,j}$.*

We can now prove the theorem:

Theorem 2 *Let $q = p^t$ where $t > 1$. The projective generalized Reed-Muller code $\mathcal{P}_{F_q}(r, m)$, for $0 < r < m - 1$, is not spanned by its minimum-weight codewords.*

Proof: Assume that C is the code spanned by minimum-weight codewords of $\mathcal{P}_{F_q}(r, m)$. Let $\mathcal{B}$ be the monomial basis of C. It follows from Lemma 1 that any monomial in $\mathcal{B}$ can be obtained by transformations of type $\varepsilon^b_{i,j}$ from a monomial of type (2), i.e. from some

$$x_{i_1}^{q-1} x_{i_2}^{q-1} \ldots x_{i_k}^{q-1}$$

for $1 \le i_1, i_2, \ldots, i_k \le r$. Consider the monomial

$$M = x_1^{q-1} x_2^{q-1} \ldots x_{r-1}^{q-1} x_r^{q-1-p^{t-1}} x_{r+1}^{p^{t-1}-1} x_{r+2},$$

where $\deg(M) = r(q-1)$. The largest 0-component degree (see Definition 3) of monomials of type (2) is $r(p-1)$, and the 0-component degree of M is $(r+1)(p-1)+1$. By Result 4, M cannot be obtained from any monomial of type (2). Therefore $M \notin \mathcal{B}$ and $C \neq \mathcal{P}_{F_q}(r, m)$. □

4 Dual codes

We now turn to the dual codes $\mathcal{P}_{F_q}(r, m)^\perp$. These are not generalized Reed-Muller codes, and the following holds (see [3, Theorem 5.38]):

Result 5 *For $0 \le r \le m - 1$,*

$$\mathcal{P}_{F_q}(r, m)^\perp = \mathcal{P}_{F_q}(m - r - 1, m) \cap (F_q \boldsymbol{\jmath})^\perp.$$

(Here $\boldsymbol{\jmath}$ denotes the all-one vector.) Thus $\mathcal{P}_{F_q}(r, m)^\perp$ is $\mathcal{P}_{F_q}(m - r - 1, m)$ with the vector $\boldsymbol{\jmath}$ removed, i.e. excluding the monomial of degree 0.

The minimum weight and nature of the minimum-weight vectors of these codes can be deduced from [13] and the affine case [2, Theorem 5.7.5], although it is not explicitly stated in these references for the projective codes:

Result 6 *The minimum weight of $\mathcal{P}_{F_q}(r, m)^\perp$, where $q = p^t$, is $2q^r$. Any minimum-weight vector is a scalar multiple of the difference of the incidence vectors of two r-dimensional projective subspaces of $PG_{m-1}(F_q)$ which intersect in an $(r - 1)$-dimensional subspace.*

Again we look at the code spanned by the minimum-weight vectors. Since this is clearly fixed by the full projective group, this code will again be spanned by monomials. We deal first with the case $q = p$. For this we need another result from Mortimer [19]: see [3, Lemma 5.3.2] or [17, Result 4].

Result 7 *The collection of transformations $\varepsilon^b_{i,j}$ acts transitively on the set of all monomials of fixed degree (ignoring scalar multiples) when $q = p$ is a prime.*

Theorem 3 *For p a prime, $\mathcal{P}_{F_p}(r,m)^{\perp}$ is spanned by its minimum-weight codewords.*

Proof: Let C be the code spanned by all the minimum-weight codewords of $\mathcal{P}_{F_p}(r,m)^{\perp}$. Since C is invariant under $PGL_m(F_p)$, Theorem 1 applies and thus C is spanned by monomials and invariant under transformations of type $\varepsilon^b_{i,j}$.

Consider the following two polynomials,

$$p_1(x_1,x_2,\dots,x_m) = \prod_{i=1}^{m-r-1}(1-x_i^{p-1})$$

and

$$p_2(x_1,x_2,\dots,x_m) = \prod_{i=1}^{m-r-2}(1-x_i^{p-1})(1-x_{m-r}^{p-1}).$$

The incidence vector corresponding to $p_1(x_1,x_2,\dots,x_m)$ is given by the equations

$$x_1 = x_2 = x_3 \dots = x_{m-r-1} = 0,$$

and that for $p_2(x_1,x_2,\dots,x_m)$ is given by the equations

$$x_1 = x_2 = x_3 = \dots = x_{m-r-2} = 0, \quad \text{and} \quad x_{m-r} = 0.$$

These are both r-dimensional subspaces of $PG_m(F_q)$ and their intersection is an $(r-1)$-dimensional subspace. It follows from Result 6 that the polynomial (p_1-p_2) gives a minimum weight codeword of $\mathcal{P}_{F_p}(r,m)^{\perp}$. The polynomial (p_1-p_2) contains the following monomial terms:

$$\begin{array}{l} x_{m-r}^{p-1}, \\ x_1^{p-1}x_{m-r}^{p-1}, \\ x_1^{p-1}x_2^{p-1}x_{m-r}^{p-1}, \\ \vdots \\ x_1^{p-1}x_2^{p-1}\dots x_{m-r-2}^{p-1}x_{m-r}^{p-1}. \end{array}$$

Therefore the monomial basis of C contains all the monomials above. Clearly the degrees of all these monomials cover all the possible degrees of monomials of $\mathcal{P}_{F_p}(r,m)^{\perp}$. It follows from Result 7 that C contains all the monomials of $\mathcal{P}_{F_p}(r,m)^{\perp}$ and thus $C = \mathcal{P}_{F_p}(r,m)^{\perp}$. □

In contrast, and as a corollary to Theorem 2, we have:

Corollary 2 *Let $q = p^t$ where $t > 1$. The dual projective generalized Reed-Muller code $\mathcal{P}_{F_q}(r,m)^{\perp}$, for $0 < r < m-1$, is not spanned by its minimum-weight codewords, i.e. it is not spanned by the differences of the incidence vectors of two r-dimensional projective subspaces of $PG_{m-1}(F_q)$ that intersect in an $(r-1)$-dimensional subspace.*

Proof: Suppose $\mathcal{P}_{F_q}(r,m)^{\perp}$ is spanned by its minimum words. Since

$$\mathcal{P}_{F_q}(r,m)^{\perp} = \mathcal{P}_{F_q}(m-r-1,m) \cap (F_q\boldsymbol{\jmath})^{\perp},$$

$\mathcal{P}_{F_q}(m-r-1,m)$ can be obtained by adding the vector $\boldsymbol{\jmath}$ to $\mathcal{P}_{F_q}(r,m)^{\perp}$. Fix any r-dimensional subspace H and any $(r-1)$-dimensional subspace K inside it. Let $\mathcal{S}$ be the set of all r-dimensional subspaces that contain K. Denoting the incidence vector of a set X of points by v^X (see [2]), let

$$v = \sum_{L\in\mathcal{S}} (v^H - v^L).$$

Then $\boldsymbol{\jmath} + v = v^H$, and so we have $\mathcal{P}_{F_q}(m-r-1,m)$ spanned by the minimum-weight vectors, which contradicts Theorem 2. □

5 Subfield subcodes

We now look at the subfield subcodes of the projective generalized Reed-Muller codes, and more particularly at their duals. In general, subfield subcodes are defined as follows:

Definition 4 *Let C be a linear code over a field E and let F be a subfield of E. The set of vectors in C, all of whose coordinates lie in F, is called the* **subfield subcode** *of C over F, and denoted by $C_{E/F}$.*

One easily verifies that $C_{E/F}$ is a linear code, and a permutation of coordinate places which preserves C also preserves $C_{E/F}$. We are interested here only in the case where $E = F_q$ and $F = F_p$, where $q = p^t$ and p is a prime. The subfield subcode of $\mathcal{P}_{F_q}(r,m)$ is denoted by $\mathcal{P}_{F_q/F_p}(r,m)$. $\mathcal{P}_{F_q/F_p}(r,m)$ is invariant under $PGL_m(F_q)$, and hence is a cyclic code.

In [14] Delsarte proves the following (see also [2, Theorem 5.7.9]):

Result 8 *For $q = p^t$, where p is a prime, $\mathcal{P}_{F_q/F_p}(r,m+1)$ is spanned by its minimum-weight codewords over F_p, and these are the incidence vectors of the $(m-r)$-dimensional subspaces of $PG_m(F_q)$.*

Thus by Result 8, $\mathcal{P}_{F_q/F_p}(r,m+1)$ is the code over F_p of the design $PG_{m,m-r}(F_q)$ of points and $(m-r)$-dimensional subspaces of $PG_m(F_q)$.

The p-**rank** of the design $PG_{m,m-r}(F_q)$ is defined to be the dimension of its p-ary code, i.e. the dimension of $\mathcal{P}_{F_q/F_p}(r,m)$. From the fact that the codes are cyclic, we have the dimension as in the case of Result 1 for the q-ary codes (see [3, Theorem 5.47]):

Result 9 *If $q = p^t$, the dimension of $\mathcal{P}_{F_q/F_p}(r,m)$ is*

$$|\{j \mid 0 \le j \le \frac{q^m-1}{q-1},\ \mathrm{wt}_q(jp^i(q-1)) \le r(q-1)\,\text{for all } i \text{ satisfying } 0 \le i \le t-1\}|,$$

where $jp^i(q-1)$ is reduced modulo q^m-1.

This result, along with Result 2 and Result 8, allows us to deduce Theorem 2 independently. We restate it as a proposition and give the short proof.

Proposition 1 *Let $q = p^t$ where $t > 1$. The projective generalized Reed-Muller code $\mathcal{P}_{F_q}(r, m)$, for $0 < r < m - 1$, is not spanned by its minimum-weight codewords.*

Proof: Consider the p-ary code of the design of points and $(m - r - 1)$-dimensional subspaces of $PG_{m-1}(F_q)$. An incidence matrix of this design generates the subfield subcode $\mathcal{P}_{F_q/F_p}(r, m)$ over F_p , and the code C spanned by the minimum-weight codewords of $\mathcal{P}_{F_q}(r, m)$ over F_q. Since the matrix has all entries 0 or 1, it follows that the rank of the matrix is the same over the fields F_p and F_q. Thus the dimension of C is that of $\mathcal{P}_{F_q/F_p}(r, m)$, and given by Result 9.

Now we show that for $1 \leq r \leq m - 2$, the dimension of $\mathcal{P}_{F_q}(r, m)$ is greater than the dimension of $\mathcal{P}_{F_q/F_p}(r, m)$ by exhibiting an integer u in the range that satisfies Result 2 but not Result 9. If we let $u = q^{r+1} - 1 + q^r p - q^{r-1}p = (q - 1)(\frac{q^r-1}{q-1} + q^{r-1}p)$ then $u \leq q^m - 1$ and $up^{t-1} \leq q^m - 1$, and it is easy to show that $\mathrm{wt}_q(u) = r(q - 1)$ but that $\mathrm{wt}_q(p^{t-1}u) = (r + 1)(q - 1)$. □

Note: The code C spanned by the minimum-weight vectors of $\mathcal{P}_{F_q}(r, m)$ and the code $\mathcal{P}_{F_q/F_p}(r, m)$ have the same generator matrix but the codes, over different fields, and their weight distributions, are quite different. For example, using Magma [6], we computed these codes for $q = 4$, $r = 1$, and $m = 3$. For C, a 4-ary code, the weight distribution is:

```
[<0, 1>, <5, 63>, <8, 630>, <9, 2100>, <11, 20160>, <12, 23940>,
<13, 125370>, <14, 60480>, <15, 262080>, <16, 107793>, <17, 291060>,
<18, 60480>, <19, 80640>, <20, 8820>, <21, 4959> ],
```

whereas for $\mathcal{P}_{F_4/F_2}(1, 3)$, which is the binary code for the projective plane of order 4, the weight distribution is:

```
[<0, 1>, <5, 21>, <8, 210>, <9, 280>, <12, 280>, <13, 210>,
<16, 21>, <21, 1> ].
```

Notice however that both have the property that there are no words having weight between the minimum of $q + 1$ and $2q$, and in fact the full projective generalized Reed-Muller code $\mathcal{P}_{F_4}(1, 3)$ has this property too. This gap in the weight distribution has been observed for the p-ary codes of projective planes, and proved for all planes of order up to and including 9, and all desarguesian planes of prime order: see Chouinard [8, 9] for a full account.

The code of the design $PG_{m,m-1}(F_q)$ of points and hyperplanes is of special interest, since the design is symmetric. The p-rank of $PG_{m,1}(F_q)$ is given by the following formula: see, for example, [2, Theorem 5.7.1].

Result 10 *If $q = p^t$, the p-rank of the design $PG_{m,m-1}(F_q)$ of points and hyperplanes of $PG_m(F_q)$ is $\binom{m+p-1}{m}^t + 1$.*

We now turn to the dual subfield subcodes. It is easy to see that if C is a code over E and F a subfield, then $(C^{\perp})_{E/F} \subseteq C^{\perp}_{E/F}$. However, even the minimum weight of these codes is not known in general. Only the binary case, i.e. $q = 2^t$ and $p = 2$, is solved. Calkin, Key and de Resmini [7, Theorem 1] proved the following result:

Result 11 *The minimum weight of the dual of the binary code of the design of points and r-dimensional 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 $(q+2)q^{m-r-1}$.*

In this result, when $r = m-1$, the minimum weight is $q+2$. In [15], Ding shows that the minimum-weight vectors are all incidence vectors of hyperovals.

Assmus and Key [1] asked if $\mathcal{P}_{F_{2^t}/F_2}(1,3)^{\perp}$ is spanned by the incidence vectors of hyperovals in the projective plane $PG_2(F_{2^t})$, i.e. by minimum-weight codewords. In [7, Note 2, p. 110], this question is extended to any dimension. We formally state this as a conjecture as follows:

Conjecture 1 *For $m \geq 2$, the dual code of the binary code of the design $PG_{m,m-1}(F_{2^t})$, i.e. $\mathcal{P}_{F_{2^t}/F_2}(1, m+1)^{\perp}$, is spanned over F_2 by the incidence vectors of hyperovals.*

When $t = 1$, it follows from Theorem 3 that this conjecture is true, since in this case the hyperoval is simply the sum of two lines that intersect in one point. Pott [20] proved the conjecture when $m = 2$ by using group character theory and the discrete Fourier transform. Here we give an alternative proof which gives a stronger answer to the conjecture when $m = 2$.

Recall that the projective space $PG_m(F_q)$,where $q = p^t$, admits a cyclic Singer group G of order $n = \frac{q^{m+1}-1}{q-1}$. The symmetric design $PG_{m,m-1}(F_q)$ is the development of a difference set D, which is geometrically a hyperplane, in G. It is clear that D is a

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

difference set. By Hall's multiplier theorem (see [2, Theorem 4.6.4]) p is a multiplier. We use the following which is quoted in [2, Proposition 4.4.1]:

Result 12 *Let D be a difference set for a group G and let ν be a multiplier. Then there is at least one difference set in the development of D that is fixed by ν, i.e. there is a $g \in G$ such that $(gD)\nu = gD$.*

The code C over F_p of the design $PG_{m,m-1}(F_q)$ is a cyclic code, and hence it corresponds to an ideal in the polynomial ring

$$F_p[x]/(x^n - 1).$$

where $n = \frac{q^{m+1}-1}{q-1}$. Since G is cyclic, it is clear that $F_p[G]$ is isomorphic to $F_p[x]/(x^n - 1)$ by the map

$$w \mapsto x \tag{3}$$

where w is a generator of G.

Lemma 2 *Let $p = 2$. If C is an ideal of $F_2[x]/(x^n - 1)$ where n is odd, and $c(x)$ is the idempotent generator of C, then the polynomial*

$$1 + x^n c(x^{-1}) \tag{4}$$

is the idempotent generator of $C^\perp$.

Proof: Let $g(x)$ be the generator polynomial of C and $h(x)$ the check polynomial, i.e. $g(x)h(x) = x^n - 1$ in $F_2[x]$. Since $x^n - 1$ has no multiple zeros, we have $(g(x), h(x)) = 1$, and hence there exist polynomials $a(x)$ and $b(x)$ such that

$$a(x)g(x) + b(x)h(x) = 1. \tag{5}$$

It follows that the idempotent generator $c(x)$ is given by

$$c(x) = a(x)g(x) = 1 + b(x)h(x),$$

since for any codeword $p(x)g(x)$,

$$\begin{aligned} c(x)p(x)g(x) &= p(x)g(x) + b(x)h(x)p(x)g(x) \\ &\equiv p(x)g(x) \pmod{(x^n - 1)}. \end{aligned}$$

Replacing x by x^{-1} in Equation (5), we have

$$a(x^{-1})g(x^{-1}) + b(x^{-1})h(x^{-1}) = 1,$$

hence

$$x^n a(x^{-1})g(x^{-1}) + x^{deg(g)}b(x^{-1})x^{deg(h)}h(x^{-1}) \equiv 1 \pmod{(x^n - 1)}.$$

We know that the reciprocal polynomial $x^{deg(h)}h(x^{-1})$ is the generator polynomial of $C^\perp$. From the construction of $c(x)$, it follows that the idempotent generator of $C^\perp$ is

$$1 + x^n a(x^{-1})g(x^{-1}) = 1 + x^n c(x^{-1}),$$

as asserted. □

Theorem 4 *The code $\mathcal{P}_{F_{2^t}/F_2}(1,3)^\perp$ has a polynomial, which corresponds to a minimum-weight codeword, as the idempotent generator.*

Proof: Let G be a Singer group for $PG_2(F_{2^t})$. $\mathcal{P}_{F_{2^t}/F_2}(1,3)$ is the code of the symmetric design $PG_{2,1}(F_{2^t})$. This design is the development of a $(2^{2t} + 2^t + 1, 2^t + 1, 1)$ difference set D, which is geometrically a line, for the Singer group G. It follows from Hall's multiplier theorem that 2 is a multiplier, and according to Result 12, there exists a difference set D' which is the development of D such that $D'^2 = D'$. Naturally D' can be identified with $L = \sum_{g \in D'} g$ in the group algebra $F_2[G]$. Letting $l(x)$ be the corresponding polynomial of L under the map from Equation (3), it is clear that $l(x)^2 = l(x)$, and thus $l(x)$ is the idempotent generator of $\mathcal{P}_{F_{2^t}/F_2}(1,3)$. By Lemma 2, the polynomial

$$1 + x^n l(x^{-1}), \tag{6}$$

where $n = 2^{2t} + 2^t + 1$, is the idempotent of $\mathcal{P}_{F_{2^t}/F_2}(1,3)^\perp$. Clearly the codeword corresponding to the polynomial from Equation (6) has weight $2^t + 2$ which is the minimum weight of $\mathcal{P}_{F_{2^t}/F_2}(1,3)^\perp$, and hence it is the incidence vector of a hyperoval. □

The conjecture for $m = 2$ follows immediately from the last theorem.

Next we turn to the case $m = 3$.

Theorem 5 *The code $\mathcal{P}_{F_{2^t}/F_2}(1,4)^\perp$ has a basis consisting of incidence vectors of hyperovals in $PG_3(F_{2^t})$, i.e. a basis of minimum-weight vectors.*

Proof: The idea of the proof follows a result of Bagchi and Sastry [4] (or see [2, Theorem 5.8.3]), in which a basis for the code of the design is explicitly given by using an ovoid in $PG_3(F_{2^t})$.

The dimension of the binary code of the design $PG_{3,2}(F_{2^t})$ of points and hyperplanes in $PG_3(F_{2^t})$ is $4^t + 1$ (see Result 10), so the dimension of its dual is $\frac{2^{4t}-1}{2^t-1} - (4^t + 1)$. Let $\mathcal{O}$ be any ovoid in $PG_3(F_{2^t})$; then $\mathcal{O}$ consists of $2^{2t} + 1$ points and, by the definition of an ovoid, every line meets $\mathcal{O}$ in at most two points. Further, the union of the tangent lines at any point of $\mathcal{O}$ is a plane. Any plane meets $\mathcal{O}$ either in one point (a tangent plane) or in an oval (a secant plane), consisting of $2^t + 1$ points. The number of tangent planes is $4^t + 1$, so the number of secant planes is $\frac{2^{4t}-1}{2^t-1} - (4^t + 1)$. If we can prove that the incidence vectors of these ovals together with their nuclei (i.e. hyperovals consisting of $2^t + 2$ points in the secant planes), are linearly independent, then they must form a basis, since there is precisely the correct number of them.

Given any point P not on $\mathcal{O}$ the tangent lines through P are in a plane: see [2, Theorem 5.8.3]. It follows that any two secant planes meet $\mathcal{O}$ in distinct ovals with distinct nuclei. Thus clearly the $\frac{2^{4t}-1}{2^t-1} - (4^t + 1)$ hyperovals from the distinct secant planes will have linearly independent incidence vectors, and we have the result. □

Note: We have not been able to extend this to higher values of m, although we have some computational results to confirm our conjecture.

6 Concluding remarks

It is clear from our somewhat sporadic results for the dual subfield codes that not a great deal is known about the minimum-weight generators for these codes. In fact even the minimum weight is unknown in general. Some other results for the minimum weight of the dual of the subfield subcode can be found in [10, 11, 12, 18]. We did some computations using Magma [6] for the dual codes of the designs $PG_{2,1}(F_9)$ and $PG_{2,1}(F_{25})$, i.e. the desarguesian projective planes of orders 9 and 25 respectively. In these case we know the minimum weight of the dual and the nature of the minimum-weight vectors: order 9 is in [18] and order 25 in [10]. The minimum weight is 15 and 45 respectively. Using Magma we found that in each case a minimum-weight vector, orbited under a Singer cycle, gave a set of vectors that contained a basis for the dual code. Thus the minimum-weight vectors span the dual subfield subcode in these cases too. We might hazard the observation that the subfield subcodes and their duals seem to be spanned by minimum-weight vectors, whereas the projective generalized Reed-Muller codes and their duals are not, in general, except in the prime case.

In Ding [16], the trace code, related to the subfield subcode, is examined and some partial results obtained.

References

[1] E. F. Assmus, Jr. and J. D. Key. Baer subplanes, ovals and unitals. In Dijen Ray-Chaudhuri, editor, *Coding Theory and Design Theory, Part I*, pages 1–8. New York: Springer-Verlag, 1990. The IMA Volumes in Mathematics and its Applications, Volume 20.

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

[3] E. F. Assmus, Jr. and J. D. Key. Polynomial codes and finite geometries. In V. S. Pless and W. C. Huffman, editors, *Handbook of Coding Theory*, pages 1269–1343. Amsterdam: Elsevier, 1998. Volume 2, Part 2, Chapter 16.

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

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

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

[7] Neil J. Calkin, Jennifer D. Key, and Marialuisa J. de Resmini. Minimum weight and dimension formulas for some geometric codes. *Des. Codes Cryptogr.*, 17:105–120, 1999.

[8] K. Chouinard. On weight distributions of codes of planes of order 9. Ars Combin., to appear.

[9] K. Chouinard. *Weight distributions of codes from planes.* PhD thesis, University of Virginia, 2000.

[10] K. L. Clark. *Improved bounds for the minimum weight of the dual codes of some classes of designs.* PhD thesis, Clemson University, 2000.

[11] K. L. Clark and J. D. Key. Geometric codes over fields of odd prime power order. *Congr. Numer.*, 137:177–186, 1999.

[12] K. L. Clark, J. D. Key, and M. J. de Resmini. Dual codes of translation planes. Submitted.

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

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

[15] Peng Ding. Sets of even type of minimum size in the design of $PG_{m,m-1}(F_q)$. *Congr. Numer.*, 140:195–198, 1999.

[16] Peng Ding. *Minimum weight generators for generalized Reed-Muller codes.* PhD thesis, Clemson University, 2000.

[17] Peng Ding and Jennifer D. Key. Minimum-weight codewords as generators of generalized Reed-Muller codes. *IEEE Trans. Inform. Theory*, 46:2152–2158, 2000.

[18] J. D. Key and M. J. de Resmini. Ternary dual codes of the planes of order nine. *J. Statist. Plann. Inference*, 95:229 – 236, 2001.

[19] Brian Mortimer. *Some problems on permutation groups: affine groups and modular permutation representations.* PhD thesis, Westfield College, University of London, 1977.

[20] Alexander Pott. Applications of the DFT to abelian difference sets. *Arch. Math.*, 51:283–288, 1988.