Minimum-weight codewords as generators of generalized Reed-Muller codes

Peng Ding and Jennifer D. Key*†

Abstract

We establish the range of values of ρ, where $0 \leq \rho \leq m(q-1)$, for which the generalized Reed-Muller code $\mathcal{R}_{F_q}(\rho, m)$ of length q^m over the field F_q of order q is spanned by its minimum-weight vectors.

Key words: generalized Reed-Muller codes, minimum-weight vectors

1 Introduction

The codes of the designs from finite projective and affine geometry are Reed-Muller and generalized Reed-Muller p-ary 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 generalized Reed-Muller code over the prime field, as was shown in work of Delsarte, Goethals and MacWilliams: see [1, Chapter 5] or [2] for full references to this work.

We look here at the generalized Reed-Muller q-ary codes for q any prime power, and ask when these are generated by their minimum weight vectors. The work of Delsarte et al. establishes the minimum weight of any of these codes, and the exact nature of the minimum-weight vectors. Delsarte [7, Theorem 10] considers the codes generated by the minimum-weight vectors as extended cyclic codes, and gives the non-roots of the generator polynomial: see also [2, Section 4.3], Charpin [5] or Berger and Charpin [3] for more on the approach to the generalized Reed-Muller codes as extended cyclic codes.

In Section 3 we prove the following:

Theorem 1 *Let $C = \mathcal{R}_{F_q}(\rho, m)$ be the q-ary generalized Reed-Muller code of order ρ and length q^m, where $q = p^t$, p is a prime, and $0 \leq \rho \leq m(q-1)$. Then C is generated by its minimum-weight vectors if $m = 1$ or $t = 1$ or $\rho < p$ or $\rho > (m-1)(q-1)+p^{t-1}-2$. In all other cases it is not generated by its minimum-weight vectors.*

*Department of Mathematical Sciences, Clemson University, Clemson SC 29634, U.S.A.

†Support of NSF grant #9730992 and ONR grant #N00014-00-1-0565 acknowledged

We use the method and constructions of Mortimer [9] (see [2, p. 1322]) in our proof. Note also that our statement agrees with the known fact, as shown by Delsarte et al., that in the case when $\rho \equiv 0 \pmod{q-1}$, the minimum-weight vectors are constant vectors, and thus only generate a subcode of the same dimension as that of the subfield subcode, which is less than that of the generalized Reed-Muller q-ary code if q is not a prime. When $m = 1$, the codes are extended Reed-Solomon codes (see [1, Section 5.4]) and hence MDS (maximum-distance-separable) codes, easily seen to be generated by minimum-weight vectors.

We give the necessary definitions, background theory and previous results in Section 2. In Section 3 we build up a proof of the main theorem through a series of lemmas and propositions. In the final section we give some Magma [4] code for computing these dimensions, along with some supporting output.

2 Terminology and background

We will use standard terminology for the structures that we need, and in particular we will follow that used in [1, 2]. These references also contain many related results on the generalized Reed-Muller codes.

Let $q = p^t$, where p is a prime, and let V be a vector space of dimension m over the field F_q of order q. We take V to be the space F_q^m of m-tuples, with standard basis. Our codes will be q-ary codes, i.e. codes over F_q, and the ambient space will be the function space F_q^V, with the usual basis of characteristic functions of the vectors of V. We can denote the elements f of F_q^V by 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 $f \in F_q^V$ is given by

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

and the x_i take values in F_q. Since every element in F_q satisfies $a^q = a$, the polynomial functions in the m variables can be reduced modulo $x_i^q - x_i$. Furthermore, every polynomial can be written uniquely as a linear combination of the q^m monomial functions

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

For any monomial the degree ρ is the total degree, i.e. $\rho = \sum_{k=1}^{m} i_k$ and clearly $0 \leq \rho \leq m(q-1)$.

The **generalized Reed-Muller** codes can now be defined:

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. For any ρ such that $0 \leq \rho \leq m(q-1)$, the ρ^{th}-order generalized Reed-Muller code $\mathcal{R}_{F_q}(\rho, m)$ is the subspace of F_q^V (with basis the characteristic functions of vectors in V) of all reduced m-variable polynomial*

functions (reduced modulo $x_i^q - x_i$) of degree at most ρ. Thus

$$\mathcal{R}_{F_q}(\rho, m) = \langle x_1^{i_1} x_2^{i_2} \cdots x_m^{i_m} \mid \sum_{k=1}^{m} i_k \leq \rho \rangle.$$

These codes are thus codes of length q^m and the codewords are obtained by evaluating the m-variable polynomials in the subspace at all the points of the vector space $V = F_q^m$. The **Reed-Muller** codes are the generalized Reed-Muller codes when $q = 2$. Clearly, if $\rho < \nu$ then $\mathcal{R}_{F_q}(\rho, m) \subset \mathcal{R}_{F_q}(\nu, m)$.

The following result is well known and quoted in [2, Theorem 5.5], for example:

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

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

Note: The second formula, simplifying the first, is due to Neil J. Calkin.

Define, for any integers, $k \geq 0$ and $q > 1$, the **q-weight** of k, written $\mathrm{wt}_q(k)$, as $\mathrm{wt}_q(k) = \sum_{\nu=0}^{\infty} k_\nu$, where $k = \sum_{\nu=0}^{\infty} k_\nu q^\nu$ is the q-ary expansion of k. Then an alternative formula for the dimension of $\mathcal{R}_{F_q}(\rho, m)$ using the q-weight can be given (see [2]): for $0 \leq \rho \leq m(q-1)$,

$$\dim(\mathcal{R}_{F_q}(\rho, m)) = |\{u \mid 0 \leq u \leq q^m - 1 \text{ and } \mathrm{wt}_q(u) \leq \rho\}|. \tag{2}$$

For any code C of length n over a field F, an **automorphism** of C is a permutation σ of the n coordinate positions that preserves C, i.e. for which, if $c = (c_1, c_2, \ldots, c_n) \in C$, then $c\sigma \in C$, where $c\sigma$ is defined by $(c\sigma)_i = c_{i\sigma^{-1}}$ for $1 \leq i \leq n$. For $0 \leq \rho \leq m(q-1)$, the automorphism group of $\mathcal{R}_{F_q}(\rho, m)$ contains the affine general linear group $AGL_m(F_q)$ (or $AGL(V)$) in its natural action on $V = F_q^m$: if $\gamma \in AGL_m(F_q)$ is given by

$$\gamma : \mathbf{v} \mapsto \mathbf{v}A + \mathbf{a}, \tag{3}$$

where $\mathbf{v}, \mathbf{a} \in V = F_q^m$ and A is a non-singular $m \times m$ matrix over F_q, then $\mathbf{v}\gamma^{-1} = \mathbf{v}A^{-1} - \mathbf{a}A^{-1}$ and for $f \in \mathcal{R}_{F_q}(\rho, m)$, $f\gamma$ is defined by

$$f\gamma(\mathbf{x}) = f(\mathbf{x}A^{-1} - \mathbf{a}A^{-1}) \tag{4}$$

where $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ and the degree in the variables x_i is preserved.

The following can be found in [1, Theorem 5.4.2]:

Result 2 *For $\rho < m(q-1)$, the dual code is given by*

$$\mathcal{R}_{F_q}(\rho, m)^{\perp} = \mathcal{R}_{F_q}(m(q-1) - 1 - \rho, m).$$

In the affine geometry $AG_m(F_q)$ defined by V the incidence vectors of the r-flats (cosets of dimension r) can be found in these codes. More generally, if $\rho = r(q-1)+s$, $0 \le s < q-1$, and for $1 \le i \le r$, $1 \le j \le s$, $w_i \in F_q$ are arbitrary and $w'_j \in F_q$ are all distinct, the polynomial

$$h(x_1, \ldots, x_m) = \prod_{i=1}^{r}(1 - (x_i - w_i)^{q-1}) \prod_{j=1}^{s}(x_{r+1} - w'_j) \tag{5}$$

has degree $r(q-1)+s = \rho$ and is zero in V unless

$$\begin{aligned} x_i &= w_i, \text{ for } i = 1, \ldots, r, \\ x_{r+1} &\neq w'_j \text{ for } j = 1, \ldots, s. \end{aligned}$$

Thus it gives a vector of weight $(q-s)q^{m-r-1}$ which consists of the sum of multiples of incidence vectors of $(q-s)$ parallel $(m-r-1)$-flats all contained in an $(m-r)$-flat in the affine geometry $AG_m(F_q)$: see [1, Theorem 5.5.3]. These are minimum-weight vectors of $\mathcal{R}_{F_q}(\rho, m)$. Taking $s = 0$ gives the incidence vector of the $(m-r)$-flat defined by the equations $X_i = w_i$ for $1 \le i \le r$.

The following result of Delsarte, Goethals and MacWilliams [6, Theorem 2.6.3] shows that all minimum-weight vectors are of the form given by the polynomial in Equation (5):

Result 3 *All the minimum-weight codewords of $\mathcal{R}_{F_q}(\rho, m)$, for any values of m, q and ρ, can be obtained from the vectors corresponding to polynomial (5) by suitable affine transformations in the affine general linear group $AGL_m(F_q)$.*

It is well known (see [2]) that the Reed-Muller code $\mathcal{R}_{F_2}(r, m)$ is generated by the characteristic vectors of the $(m-r)$-flats in the affine geometry $AG_m(F_2)$ and that these are the minimum-weight vectors of $\mathcal{R}_{F_2}(r, m)$, of weight is 2^{m-r}. Thus the Reed-Muller codes are generated by their minimum-weight vectors.

Now we consider the generalized Reed-Muller codes over any finite field F_q. Mortimer's results [9] are employed extensively in our study and for this we need the following maps:

Definition 2 *In the space F_q^V where $V = F_q^m$, for $1 \le i, j \le m$, $i \neq j$, $0 \le a_i \le q-1$ and b any integer, define the maps δ_i^b and $\varepsilon_{i,j}^b$ on the monomials $x_1^{a_1} x_2^{a_2} \ldots x_m^{a_m}$:*

$$(x_1^{a_1} x_2^{a_2} \ldots x_m^{a_m})\delta_i^b = \binom{a_i}{b} x_1^{a_1} x_2^{a_2} \ldots x_i^{a_i - b} \ldots x_m^{a_m} \tag{6}$$

$$(x_1^{a_1} x_2^{a_2} \ldots x_m^{a_m})\varepsilon_{i,j}^b = \binom{a_i}{b} x_1^{a_1} x_2^{a_2} \ldots x_i^{a_i - b} \ldots x_j^{a_j + b} \ldots x_m^{a_m}. \tag{7}$$

The maps are then extended to be linear on the space F_q^V.

Since $\binom{a_i}{b} = 0$ for $a_i < b$, δ_i^b annihilates the monomial $x_1^{a_1}x_2^{a_2}\dots x_m^{a_m}$ unless $b \le a_i$; similarly $\varepsilon_{i,j}^b$ annihilates $x_1^{a_1}x_2^{a_2}\dots x_m^{a_m}$ unless $b \le a_i$. Both δ_i^0 and $\varepsilon_{i,j}^0$ are the identity on $\mathcal{M}$ and hence on F_q^V. Notice that if δ_i^b does not annihilate a monomial and if $b \neq 0$, then it reduces the degree of the monomial, whereas $\varepsilon_{i,j}^b$ keeps the degree fixed or reduces it.

Mortimer [9] (see [2, Lemma 5.32]) proves the following result:

Result 4 *The collection of transformations $\varepsilon_{i,j}^b$ acts transitively on the set of all monomials of fixed degree (ignoring scalar multiples) when $q = p$ is a prime.*

The code C generated by the minimum-weight codewords of $\mathcal{R}_{F_q}(\rho, m)$ is invariant under $AGL(V)$. In fact this is true for the code generated by vectors of any fixed given weight in $\mathcal{R}_{F_q}(\rho, m)$. We will refer to minimum-weight codewords or vectors as **minimum words**. We will also use the notation

$$(x_1^{a_1}x_2^{a_2}\dots x_m^{a_m})f \simeq x_1^{b_1}x_2^{b_2}\dots x_m^{b_m}$$

if the monomial on the left is mapped by f to a non-zero scalar multiple of the monomial on the right. We will say that the monomial on the right is **obtained** from the monomial on the left by the transformation f.

The following result due to Mortimer [9] (see [2, Theorem 5.31]) plays an important role in our argument.

Result 5 *Let H be a subspace of F_q^V where $V = F_q^m$, q is a prime power and $m \ge 1$. Then H is invariant under the affine general linear group $AGL(V)$ if and only if*

- *H is invariant under the transformations δ_i^b and $\varepsilon_{i,j}^b$ for $i \neq j$ and $1 \le i, j \le m$ and $0 \le b \le q-1$, and*
- *H is spanned by monomials.*

Corollary 2 *The code generated by the minimum-weight codewords of $\mathcal{R}_{F_q}(\rho, m)$, for any $m \ge 1$, any prime-power q and $0 \le \rho \le m(q-1)$, has a monomial basis.*

The dimension of the code generated by the minimum-weight vectors follows from Delsarte [7, Theorem 10]:

Result 6 *For $m \ge 2$, $q = p^t$ where p is a prime, if $\rho = r(q-1) + s$, where $0 \le r \le m-1$, $0 \le s < q-1$, then the subcode of $\mathcal{R}_{F_q}(\rho, m)$ generated by the minimum-weight codewords has dimension*

$$\Big|\bigcup_{0 \le j \le s} \{z \mid 1 \le z < q^m \text{ such that } \mathrm{wt}_q(p^k z) \ge (m-r)(q-1) - [p^k j] \text{ for } 0 \le k < t\}\Big|,$$

where $[y]$ denotes the residue of y modulo $q-1$.

When $q = p^t$ is not a prime we will need to use p-ary expansions: if n and m are integers with p-ary expansions $n = \sum_{s=0}^{\infty} n_s p^s$ and $m = \sum_{s=0}^{\infty} m_s p^s$, respectively, we will write $(n)_p \succeq (m)_p$ if $n_s \geq m_s$ for all $s \geq 0$.

Result 7 (Lucas's Theorem) *For p a prime, let a and b be positive integers with p-ary expansions $a = \sum_{s=0}^{v} a_s p^s$ and $b = \sum_{s=0}^{v} b_s p^s$. Then*

$$\binom{a}{b} \equiv \prod_{s=0}^{v} \binom{a_s}{b_s} \pmod{p}.$$

In the proofs in the next section we will need the following definition:

Definition 3 *Given a monomial $x_1^{a_1} x_2^{a_2} \dots x_m^{a_m}$, 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 $x_1^{a_1} x_2^{a_2} \dots x_m^{a_m}$, denoted by* cdeg_k*, is defined by*

$$\mathrm{cdeg}_k(x_1^{a_1} x_2^{a_2} \dots x_m^{a_m}) = \sum_{i=1}^{m} a_{i,k}. \tag{8}$$

Given any integer b with p-ary expansion $b = \sum_{i=0}^{\infty} b_i p^i$, where $0 \leq b_i \leq p-1$, we define

$$\bar{b} = min\{i \mid b_i \neq 0\}. \tag{9}$$

3 Minimum-weight words as generators

In this section we will prove our main theorem through a series of lemmas and propositions.

Proposition 3 *For any ρ, m and $q = p$ a prime, $\mathcal{R}_{F_p}(\rho, m)$ is generated by its minimum-weight codewords.*

Proof: Suppose $\rho = r(p-1) + s$, where $0 \leq s < p-1$, and let C be the code generated by the minimum words of $\mathcal{R}_{F_p}(\rho, m)$. Then C is clearly invariant under $AGL(V)$ and so Result 5 applies. It can be seen that the monomial $x_1^{p-1} x_2^{p-1} \dots x_r^{p-1} x_{r+1}^{s'}$, for any $s' \leq s$, is one term in the polynomial function of Equation (5) that gives a minimum word. From Result 5, it must be a monomial in the monomial basis of C. All the monomials transformed from it by some transformation of type δ_i^b are in C as well. For any a such that $0 \leq a \leq p-1$, we have $\binom{p-1}{a} \neq 0$, and hence, given a monomial $x_1^{i_1} x_2^{i_2} \dots x_r^{i_r} x_{r+1}^{s'}$ where $0 \leq i_1, i_2, \dots, i_r \leq p-1, 0 \leq s' \leq s$, we have

$$(x_1^{p-1} x_2^{p-1} \dots x_r^{p-1} x_{r+1}^{s}) \delta_{r+1}^{s-s'} \delta_r^{p-1-i_r} \dots \delta_1^{p-1-i_1} \simeq x_1^{i_1} x_2^{i_2} \dots x_r^{i_r} x_{r+1}^{s'}.$$

Therefore C must contain the monomial $x_1^{i_1}x_2^{i_2}\dots x_r^{i_r}x_{r+1}^{s'}$. Hence C contains monomials with degrees ranging from 0 to ρ. It follows from Result 4 that C contains all the monomial of degree up to ρ. Hence C is precisely $\mathcal{R}_{F_p}(\rho,m)$ by Definition 1. □

Note: This can also be deduced, in this case where $q=p$ is a prime, from Delsarte's result for the formula of the dimension of the code spanned by the minimum words: see Equation (2) and Result 6.

Now we consider the generalized Reed Muller code $\mathcal{R}_{F_q}(\rho,m)$ where $q=p^t$ is not a prime. Then $q-1=\sum_{i=0}^{t-1}(p-1)p^i$ and thus $(q-1)_p \succeq (a)_p$ for $0\le a\le q-1$. It follows from Lucas's theorem that $\binom{q-1}{a} \not\equiv 0 \pmod p$. In $\mathcal{R}_{F_q}(\rho,m)$, where $\rho=r(q-1)+s$, $x_1^{q-1}x_2^{q-1}\dots x_r^{q-1}x_{r+1}^{s}$ is one term in the polynomial of Equation (5). Using the same argument as in the proof of Proposition 3, we can conclude that the monomials of type

$$x_1^{i_1}x_2^{i_2}\dots x_r^{i_r}x_{r+1}^{s'},\ 0\le i_1,i_2,\dots,i_r\le q-1,\ 0\le s'\le s, \tag{10}$$

are in the monomial basis of the code C generated by the minimum words of $\mathcal{R}_{F_q}(\rho,m)$.

Lemma 4 *Let $\mathcal{B}$ be the monomial basis of the code C generated by minimum words of $\mathcal{R}_{F_q}(\rho,m)$. Any monomial in $\mathcal{B}$ can be obtained from some monomial of type (10) having the same or greater degree, by some transformations of type $\varepsilon_{i,j}^b$.*

Proof: Since C is invariant under $AGL_m(F_q)$, it follows from Results 3 and 5 that any monomial $M(\mathbf{x})$ in $\mathcal{B}$ must be a monomial term in a polynomial that is mapped from the polynomial $h(\mathbf{x})$ of Equation (5) by some transformation in $AGL_m(F_q)$. Any element of $AGL_m(F_q)$ is the product of a translation and a linear transformation.

We consider the following translation for any fixed i and $u\in F_q$:

$$\sigma_i^u : (x_1,x_2,\dots,x_m)\longmapsto (x_1,x_2,\dots,x_{i-1},x_i-u,x_{i+1},\dots,x_m). \tag{11}$$

The polynomial of Equation (5) can be written as $h(x_1,x_2,\dots,x_m)=\sum_j h_j x_i^j$ where the h_j are polynomials independent of x_i. Then it follows that $h\sigma_i^u(\mathbf{x})$ (see notation in Equation 4) satisfies the following:

$$\begin{aligned} h\sigma_i^u(\mathbf{x}) &= \sum_j h_j(x_i+u)^j = \sum_j h_j \sum_b \binom{j}{b} x_i^{j-b}u^b \\ &= \sum_b u^b \sum_j \binom{j}{b} h_j x_i^{j-b} = \sum_b u^b (h(\mathbf{x}))\delta_i^b. \end{aligned}$$

Obviously the monomials in $(h(\mathbf{x}))\delta_i^b$ are of type (10) and thus the translations map $h(\mathbf{x})$ to polynomials that contain only monomial terms of type (10).

Now for any fixed i,j, $i\ne j$, consider the transvection $\lambda_{i,j}$ where

$$\lambda_{i,j} : (x_1,x_2,\dots,x_m)\longmapsto (x_1,x_2,\dots,x_i-x_j,\dots,x_m), \tag{12}$$

i.e. $(x_1, \ldots, x_m)\lambda_{i,j} = (y_1, \ldots, y_m)$ where $y_k = x_k$ for $k \neq i$ and $y_i = x_i - x_j$. For a polynomial f we write $f(x_1, \ldots, x_m) = \sum_{r,s} f_{r,s} x_i^r x_j^s$, where the $f_{r,s}$ are polynomials independent of x_i and x_j. Then it follows directly that

$$f\lambda_{i,j}(\mathbf{x}) = \sum_{r,s} f_{r,s}(x_i + x_j)^r x_j^s = \sum_{r,s} f_{r,s} \sum_b \binom{r}{b} x_i^{r-b} x_j^{s+b}$$
$$= \sum_b \sum_{r,s} \binom{r}{b} f_{r,s} x_i^{r-b} x_j^{s+b} = \sum_b (f(\mathbf{x}))\varepsilon_{i,j}^b.$$

Thus the monomials that can be obtained from $h(\mathbf{x})$ by translations or transvections are those that can be obtained from the monomials in $h(\mathbf{x})$ by the maps δ_i^b and the $\varepsilon_{i,j}^b$. For any nonsingular matrix A, ignoring scalar products, A can be written as the product of matrices of the transformations (12). Thus it can be seen from the above procedures that any monomial $M(\mathbf{x})$ in $\mathcal{B}$ is obtained from some monomial of type (10) of no smaller degree by some transformations of type $\varepsilon_{i,j}^b$. □

Example 1 In the code $\mathcal{R}_{F_4}(3,2)$, the incidence polynomial (5) is $h(x_1, x_2) = 1 - (x_1 - \alpha)^3$ for some $\alpha \in F_4$. Here $m = 2$, $r = 1$ and $s = 0$. According to Lemma 4, all the monomials of degree 2 in the code generated by minimum-weight codewords must be obtained from x_1^2 or x_1^3 by transformations of type (7). It is easy to verify that the monomial $x_1x_2 \in \mathcal{R}_{F_4}(3,2)$ cannot be obtained in this way, since, for example, $x_1^2\varepsilon_{1,2}^1 = \binom{2}{1}x_1x_2 = 0$. Thus $\mathcal{R}_{F_4}(3,2)$ is not generated by its minimum-weight vectors. Note that the binary subfield subcode of $\mathcal{R}_{F_4}(3,2)$ is generated by its minimum-weight vectors, and a basis of nine vectors is given in [1, Example 5.7.1, page 187]. These involve the nine monomials $\{1, x_1, x_1^2, x_1^3, x_2, x_2^2, x_2^3, x_1x_2^2, x_1^2x_2\}$, which form a basis for the code generated by the minimum-weight vectors over F_4. □

Lemma 5 *Given two monomials* $M_A = x_1^{a_1}x_2^{a_2}\ldots x_m^{a_m}$ *and* $M_B = x_1^{b_1}x_2^{b_2}\ldots x_m^{b_m}$, *if* $\mathrm{cdeg}_k(M_A) = \mathrm{cdeg}_k(M_B)$ *for* $0 \leq k \leq t-1$ *then* M_B *can be obtained from* M_A *by transformations of type* $\varepsilon_{i,j}^b$.

Proof: (Refer to Definition 3 for the notation here.) Clearly $\deg(M_A) = \deg(M_B)$ since $\mathrm{cdeg}_k(M_A) = \mathrm{cdeg}_k(M_B)$ for $0 \leq k \leq t-1$. As before, letting $a_{i,k}$ and $b_{i,k}$ be the k-th p-ary digits of a_i and b_i respectively, we have $\sum_{l=1}^m a_{l,k} = \sum_{l=1}^m b_{l,k}$ for $0 \leq k \leq t-1$. Fix k in the range $0 \leq k \leq t-1$. The proof will follow if we can prove that $a_{l,k}$ can be changed to $b_{l,k}$ by transformations of the type $\varepsilon_{i,j}^b$ for $1 \leq l \leq m$. Without loss of generality, assume that

$$a_{1,k} \geq b_{1,k},\ a_{2,k} \geq b_{2,k},\ \ldots,\ a_{d,k} \geq b_{d,k},$$

and

$$a_{d+1,k} < b_{d+1,k},\ a_{d+2,k} < b_{d+2,k},\ \ldots,\ a_{m,k} < b_{m,k}.$$

Then

$$\sum_{i=1}^{d}(a_{i,k}-b_{i,k})=\sum_{i=1}^{m-d}(b_{d+i,k}-a_{d+i,k}).$$

For $0<i<d+1$ and $a_{i,k}>b_{i,k}$, there exists j such that $d<j\le m$ and $a_{j,k}<b_{j,k}$, and

$$(M_A)\varepsilon_{i,j}^{p^k}=\binom{a_i}{p^k}x_1^{a_1}x_2^{a_2}\ldots x_i^{(a_i-p^k)}\ldots x_j^{(a_j+p^k)}\ldots x_m^{a_m}\neq 0,$$

by Lucas's theorem, and reduces $a_{i,k}$ by 1 and increases $a_{j,k}$ by 1. If this procedure is applied repeatedly, then $a_{i,k}$ can be reduced to $b_{i,k}$. If we reduce all the $a_{i,k}$ to $b_{i,k}$ for all $0<i<d+1$, then simultaneously $a_{j,k}$ is increased to $b_{j,k}$ for all $d<j\le m$ by the above procedure. This can be done for each value of k. □

Example 2 For $q=2^4$, $m=4$, let A_k and B_k be the k-component-degrees of $M_A=x_1^3x_2^5x_3^2x_4^8$ and $M_B=x_1^7x_2x_3^{10}$ respectively, for $0\le k\le 3$. It is easy to check that $A_k=B_k$ for all k and $A_0=2$, $A_1=2$, $A_2=1$, $A_3=1$. It follows from Lemma 5 that there exist transformations of type $\varepsilon_{i,j}^b$ such that $x_1^7x_2x_3^{10}$ can be obtained from $x_1^3x_2^5x_3^2x_4^8$ by these transformations. For instance, $(x_1^3x_2^5x_3^2x_4^8)\varepsilon_{2,1}^4\varepsilon_{4,3}^8\simeq x_1^7x_2x_3^{10}$. □

Lemma 6 *Let $M=x_1^{a_1}x_2^{a_2}\ldots x_m^{a_m}$ and let A_k denote the k-component degree of M. For any integer b and any k such that $0\le k\le t-1$, if $k\le\bar{b}$ then $\mathrm{cdeg}_k(M\varepsilon_{i,j}^b)\le A_k$ for $1\le i,j\le m$.*

Proof: (Recall that $\bar{b}$ is defined in Equation (9).) Fix i,j in the range. If $M\varepsilon_{i,j}^b=0$, then the claim is trivially true. If $M\varepsilon_{i,j}^b\neq 0$, then $a_i\succeq b$. If $k<\bar{b}$, the k-th digit of a_i-b is the same as that of a_i, and the k-th digit of a_j+b is the same as that of a_j. If $k=\bar{b}$, the k-th digit of a_i-b is less than that of a_i by b_k, and the k-th digit of a_j+b is greater than that of a_j by at most b_k. This gives the stated result. □

Lemma 7 *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 $0\le k\le t-1$. Suppose that $A_k=B_k$, for $0\le k\le l-1$ and $A_l<B_l$ for some $l\le t-1$. Then M_B cannot be obtained from M_A by transformations of the type $\varepsilon_{i,j}^b$.*

Proof: We use induction on l. If $l=0$, then $A_0<B_0$. From Lemma 6, A_0 cannot be increased by any transformations $\varepsilon_{i,j}^b$ since $0\le\bar{b}$.

Assume that the result holds for $0\le l\le d-1$ and suppose $A_k=B_k$ for $0\le k\le d-1$, and $A_d<B_d$. If M_B can be obtained from M_A, then A_d can be increased to B_d by some transformations of the type $\varepsilon_{i,j}^c$. Thus for some c and i,j, $M_C=M_A\varepsilon_{i,j}^c$ has d-component degree C_d where $B_d\ge C_d>A_d$, and M_B can be obtained from M_C by further transformations. It follows from Lemma 6 that $d>\bar{c}$ and for some l such that

$\bar{c} \leq l \leq d-1$, $C_l < A_l = B_l$, and for $k < l$, $C_k = A_k = B_k$. By the induction hypothesis, M_B cannot be obtained from M_C, contradicting our assumption. This completes the proof. □

The generalized Reed-Muller code $\mathcal{R}_{F_q}(\rho, 1)$ is an extended Reed-Solomon code and is an MDS code; thus it is clearly generated by its minimum-weight codewords. Thus from now on we can assume that $m > 1$.

Proposition 8 *For any m and $q = p^t$, if $\rho < p$ then $\mathcal{R}_{F_q}(\rho, m)$ is generated by its minimum-weight codewords.*

Proof: Since $\rho < p < q$, the polynomial of Equation (5) is $\prod_{j=1}^{\rho}(x_1 - w'_j)$. It follows from Lemma 4 that all the monomials in the code generated by the minimum words are the monomials which can be obtained from 1, x_1, x_1^2,..., x_1^ρ by transformations of type $\varepsilon_{i,j}^b$. Since $\binom{a}{b} \neq 0$ if $a > b$ and $a < p$, $b < p$, all the monomials with degree no greater than ρ can be obtained by transformations of type $\varepsilon_{i,j}^b$. □

Proposition 9 *For $m \geq 2$, and $q = p^t$, if $p \leq \rho < q$ then $\mathcal{R}_{F_q}(\rho, m)$ is not generated by its minimum-weight codewords.*

Proof: Since $\rho \leq q - 1$, the polynomial of Equation (5) is $\prod_{j=1}^{\rho}(x_1 - w'_j)$ if $\rho < q - 1$, or $1 - (x_1 - w_1)^{q-1}$ if $\rho = q - 1$. The type (10) monomials are x_1^r for $0 \leq r \leq \rho$. For the monomial $x_1^{p-1}x_2$, $\mathrm{cdeg}_0(x_1^{p-1}x_2) = p$ which is greater than $\mathrm{cdeg}_0(x_1^r)$ for $r \leq q-1$. It follows from Lemma 6 that $x_1^{p-1}x_2$ cannot be obtained from x_1^r for any $r \leq q-1$ by transformations of the type $\varepsilon_{i,j}^b$. According to Lemma 4, the monomial $x_1^{p-1}x_2$ is not in the code generated by the minimum-weight codewords in $\mathcal{R}_{F_q}(\rho, m)$. □

Proposition 10 *For $m \geq 3$, if $\rho = r(q-1)+s$, where $0 < r \leq m-2$ and $0 \leq s \leq q-2$, then $\mathcal{R}_{F_q}(\rho, m)$ is not generated by its minimum-weight codewords.*

Proof: Since $0 < r \leq m-2$ and $2(p-1) \leq p^2 - p$, $x_1^{p-1}x_2^{p-1}\ldots x_{r+1}^{p-1}x_{r+2}^{p-1}$ is a monomial in $\mathcal{R}_{F_q}(\rho, m)$ and its 0-component-degree is $(r+2)(p-1)$. According to Lemma 7, $x_1^{p-1}x_2^{p-1}\ldots x_{r+1}^{p-1}x_{r+2}^{p-1}$ cannot be transformed from monomials of type (10) by transformations $\varepsilon_{i,j}^b$, since $x_1^{i_1}x_2^{i_2}\ldots x_r^{i_r}x_{r+1}^s$ has 0-component-degree strictly less than $(r+2)(p-1)$ for any $i_1, i_2, \ldots, i_r, s$. Therefore $x_1^{p-1}x_2^{p-1}\ldots x_{r+1}^{p-1}x_{r+2}^{p-1}$ is not in the code generated by the minimum-weight codewords in $\mathcal{R}_{F_q}(\rho, m)$ by Lemma 4. □

Proposition 11 *If $m \geq 2$, $q = p^t$ and $\rho = (m-1)(q-1) + s$ where $0 \leq s < p^{t-1} - 1$ then $\mathcal{R}_{F_q}(\rho, m)$ is not generated by its minimum-weight codewords.*

Proof: Let $r = p^{t-1} - 1 = \sum_{i=0}^{t-2}(p-1)p^i$. The monomial $x_1^r x_2^r \dots x_m^r$ is in $\mathcal{R}_{F_q}(\rho, m)$ and has the maximum k-component-degree where $0 \le k \le t-2$. Since $r > s$, the $(t-2)$-component-degree of $x_1^r x_2^r \dots x_m^r$ must be greater than that of any monomial of type (10) in the code and hence it cannot be obtained from type (10) monomials by transformations of type $\varepsilon_{i,j}^b$, by Lemma 7. Thus the monomial $x_1^r x_2^r \dots x_m^r$ is not in the code generated by the minimum-weight codewords in $\mathcal{R}_{F_q}(\rho, m)$. □

Proposition 12 *For $m \ge 2$ and $q = p^t$, if $\rho = (m-1)(q-1) + s$ where $s \ge p^{t-1} - 1$, then $\mathcal{R}_{F_q}(\rho, m)$ is generated by its minimum-weight codewords.*

Proof: For any monomial $M = x_1^{d_1} x_2^{d_2} \dots x_m^{d_m}$ with degree no greater than ρ, if we can show that it can be obtained from some monomial of type (10) with the same or greater degree less than ρ by transformations of type $\varepsilon_{i,j}^b$, then the stated result is proved. If $d_m = 0$ this is clear.

Suppose that $\deg(M) = (m-1)(q-1) + s'$ where $0 \le s' \le s$. The monomial $x_1^{q-1} x_2^{q-1} \dots x_{m-1}^{q-1} x_m^{s'}$ is of type (10). Since $\binom{q-1}{a} \ne 0$ for $0 \le a \le q-1$, it follows that

$$(x_1^{q-1} x_2^{q-1} \dots x_{m-1}^{q-1} x_m^{s'}) \varepsilon_{1,m}^{q-1-d_1} \varepsilon_{2,m}^{q-1-d_2} \dots \varepsilon_{m-1,m}^{q-1-d_{m-1}} \simeq M.$$

If $\deg(M) < (m-1)(q-1)$ let $M'_t = x_1^{d_1} x_2^{d_2} \dots x_{m-1}^{d_{m-1}}$ and write

$$d_m = \deg(M) - \deg(M'_t) = f_{t-1} p^{t-1} + r_{t-1}, \quad 0 \le r_{t-1} \le p^{t-1} - 1 \le s.$$

If $\mathrm{cdeg}_{t-1}(M'_t) + f_{t-1} \le (m-1)(p-1)$, we construct a monomial $M'_{t-1} = x_1^{d'_1} x_2^{d'_2} \dots x_{m-1}^{d'_{m-1}}$ from M'_t by adding $f_{t-1} p^{t-1}$ to the degree of M'_t such that $\mathrm{cdeg}_{t-1}(M'_{t-1}) = f_{t-1} + \mathrm{cdeg}_{t-1}(M'_t)$, and $\mathrm{cdeg}_i(M'_{t-1}) = \mathrm{cdeg}_i(M'_t)$ for $0 \le i \le t-2$. Since $r_{t-1} \le s$, the monomial $M'_{t-1} x_m^{r_{t-1}}$ is of type (10) and clearly $d'_j \succeq d'_j - d_j$ for $1 \le j \le m-1$. Thus

$$(M'_{t-1} x_m^{r_{t-1}}) \varepsilon_{1,m}^{d'_1 - d_1} \varepsilon_{2,m}^{d'_2 - d_2} \dots \varepsilon_{m-1,m}^{d'_{m-1} - d_{m-1}} \simeq M,$$

and the proof is complete.

If $\mathrm{cdeg}_{t-1}(M'_t) + f_{t-1} > (m-1)(p-1)$, we construct $M'_{t-1} = x_1^{d'_1} x_2^{d'_2} \dots x_{m-1}^{d'_{m-1}}$ by adding $((m-1)(p-1) - \mathrm{cdeg}_{t-1}(M'_t)) p^{t-1}$ to the degree of M'_t such that $\mathrm{cdeg}_{t-1}(M'_{t-1}) = (m-1)(p-1)$, and $\mathrm{cdeg}_i(M'_{t-1}) = \mathrm{cdeg}_i(M'_t)$ for $0 \le i \le t-2$. Then write

$$\deg(M) - \deg(M'_{t-1}) = f_{t-2} p^{t-2} + r_{t-2}, \quad 0 \le r_{t-2} \le p^{t-2} - 1 \le s.$$

Now we construct M'_{t-2} from M'_{t-1} by the same procedure we used to construct M'_{t-1} from M'_t, except that we now only increase $\mathrm{cdeg}_{t-2}(M'_{t-1})$: using the same argument as above we see that if $\mathrm{cdeg}_{t-2}(M'_{t-1}) + f_{t-2} \le (m-1)(p-1)$, then the proof is done, and if $\mathrm{cdeg}_{t-2}(M'_{t-1}) + f_{t-2} > (m-1)(p-1)$, we need to construct M'_{t-3}. Because $\deg(M) \le (m-1)(q-1)$, the recursive construction will terminate and produce the monomial we need. □

The following example illustrates the algorithm we use in proving Proposition 12.

Example 3 In $\mathcal{R}_{F_{27}}(86,4)$ we have $m=4$, $r=t=3$, $s=3^2-1$, $(m-1)(q-1)=78$ and $(m-1)(p-1)=6$. A monomial of type (10) has the form $x_1^{i_1}x_2^{i_2}x_3^{i_3}x_4^{i_4}$,where $0\le i_1,i_2,i_3\le 26$, and $0\le i_4\le 8$. The monomial $M=x_1^{10}x_2^{25}x_3^{25}x_4^{25}$ is not of type (10); here $\deg(M)=85=3\times 26+7>78$, so Proposition 12 yields

$$(x_1^{26}x_2^{26}x_3^{26}x_4^{7})\varepsilon_{1,4}^{16}\varepsilon_{2,4}^{1}\varepsilon_{3,4}^{1}\simeq M.$$

Now consider $M=x_1^{12}x_2^{18}x_3^{21}x_4^{26}$ of degree $77=2\times 26+25<78$. Then $M_3'=x_1^{12}x_2^{18}x_3^{21}$ and

$$\deg(M)-\deg(M_3')=26=2\times 9+8,\quad \mathrm{cdeg}_2(M_3')+2=7>6.$$

Thus we add 1×9 to the degree to obtain $M_2'=x_1^{21}x_2^{18}x_3^{21}$ and

$$\deg(M)-\deg(M_2')=17=5\times 3+2,\quad \mathrm{cdeg}_1(M_2')+5=7>6.$$

Thus we add 4×3 to the degree to obtain $M_1'=x_1^{24}x_2^{24}x_3^{24}$ and

$$\deg(M)-\deg(M_1')=5\times 1+0,\quad \mathrm{cdeg}_0(M_1')+5=5<6.$$

So finally we add 5×1 to the degree to obtain $M_0'=x_1^{26}x_2^{26}x_3^{25}$, and obtain

$$(M_0'x_4^{0})\varepsilon_{1,4}^{14}\varepsilon_{2,4}^{8}\varepsilon_{3,4}^{4}\simeq M.$$

□

The propositions of this section, along with the observation that $\mathcal{R}_{F_q}(m(q-1),m)$ is trivially seen to be generated by its minimum-weight codewords, it being the full space, completes the proof of Theorem 1.

Note:
1. If $\rho=r(q-1)$ then the minimum-weight vectors of $\mathcal{R}_{F_q}(\rho,m)$ are the incidence vectors of the $(m-r)$-flats, and the code generated by them is a subfield subcode: see [1, Chapter 5]. This is only equal to $\mathcal{R}_{F_q}(\rho,m)$ if q is a prime. Our theorem agrees with this.
2. The dual code of $\mathcal{R}_{F_q}(\rho,m)$ may be generated by its minimum words while $\mathcal{R}_{F_q}(\rho,m)$ is not. For example, $\mathcal{R}_{F_9}(12,2)$ is generated by its minimum words, but $\mathcal{R}_{F_9}(12,2)^{\perp}=\mathcal{R}_{F_9}(3,2)$ is not. In fact if $m>1$ and q is not prime, only in the case $q=4$ will $\mathcal{R}_{F_q}(\rho,m)$ be generated by its minimum words if and only if its dual is generated by its minimum words.
3. Actual bases of minimum-weight vectors are known only in some specific cases: see Gao and Key [8] for a discussion, and where the case $\mathcal{R}_{F_p}(p-1,m)$ is solved.

4 Computations

We tested our results using the formulae for the dimensions as given in Section 2 with Magma [4]. For the dimension of the generalized Reed-Muller code we used the simplified form of Result 1 and the Magma function:

```
//Gives the dimension of R_GF(q)(r,m)
grmD:=func<q,r,m|&+[(-1)^k*Binomial(m,k)*
        Binomial(r-k*q+m,r-k*q):k in [0..m]]>;
```

and for the dimension of the code spanned by the minimum-weight vectors we used Delsarte's Result 6 and the Magma function:

```
//Gives the q-weight of u
qwt:=func<u,q|  &+[Intseq(u,q)[j]: j in [1..#Intseq(u,q)]]>;

/*Gives the dimension of the code spanned by the minimum weight
vectors of R_GF(q)(r,m) for r <m(q-1), where q=p^e*/
GRMmw:=function(p,e,r,m);
q:=p^e;  nrts:={};
      for j:=0 to (r mod (q-1)) do
         for t:=1 to q^m-1 do
         s:={};
            for k:=0 to e-1 do
            d:=(m-(r div (q-1)))*(q-1)-(j*p^k mod (q-1));
                if qwt(t*p^k,q) ge d then
                s:=s join {k};
                end if;
            end for;
                if #s eq e then
                nrts:=nrts join {t};
                end if;
         end for;
      end for;
return #nrts;
end function;
```

Some output using these Magma functions:

```
dims:=[[r,grmD(9,r,2),GRMmw(3,2,r,2)]:r in [0..15]];
> dims;
[ [ 0, 1, 1 ], [1, 3, 3 ], [2, 6, 6 ], [3, 10, 8 ], [4, 15, 12 ], [5, 21,
18 ], [6, 28, 21 ], [7, 36, 27 ], [8, 45, 36 ], [9, 53, 50 ], [10, 60,
60 ], [11, 66, 66 ], [12, 71, 71 ], [13, 75, 75 ], [14, 78, 78 ], [15,
80, 80 ] ]
dims:=[[r,grmD(8,r,3),GRMmw(2,3,r,3)]:r in [0..20]];
> dims;
[ [ 0, 1, 1 ], [1, 4, 4 ], [2, 10, 7 ], [3, 20, 16 ], [4, 35, 19 ], [5, 56,
```

```
28 ], [6, 84, 37 ], [7, 120, 64 ], [8, 162, 127 ], [9, 208, 172 ], [10,
256, 231 ], [11, 304, 258 ], [12, 350, 298 ], [13, 392, 328 ], [14, 428,
373 ], [15, 456, 443 ], [16, 477, 474 ], [17, 492, 492 ], [18, 502, 502
], [19, 508, 508 ], [20, 511, 511 ] ]
```

Notice that the values of r for which the dimensions become the same agrees with our theorem.

Acknowledgement

The authors thank the reviewers for their careful reading and constructive comments.

References

[1] 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).

[2] 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.

[3] Thierry Berger and Pascale Charpin. The automorphism group of Generalized Reed-Muller codes. *Discrete Math.*, 117:1–17, 1993.

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

[5] Pascale Charpin. Open problems on cyclic codes. In V. S. Pless and W. C. Huffman, editors, *Handbook of Coding Theory*, pages 963–1063. Amsterdam: Elsevier, 1998. Volume 1, Part 1, Chapter 11.

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

[8] S. Gao and J. D. Key. Bases of minimum-weight vectors for codes from designs. *Finite Fields Appl.*, 4:1–15, 1998.

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