Discrete Applied Mathematics 111 (2001) 87–102

DISCRETE APPLIED MATHEMATICS

The degree of functions and weights in linear codes

Sugi Guritman, Femke Hoogweg, Juriaan Simonis *

Department of Pure Mathematics, Delft University of Technology, Faculty of Information Technology and Systems, P.O. Box 5031, 2600 GA Delft, Netherlands

Received 15 April 1999; revised 11 November 1999; accepted 13 July 2000

Abstract

Properties of the weight distribution of low-dimensional generalized Reed–Muller codes are used to obtain restrictions on the weight distribution of linear codes over arbitrary fields. These restrictions are used in non-existence proofs for ternary linear code with parameters $[74, 10, 44]$ $[82, 6, 53]$ and $[96, 6, 62]$.

Keywords: Linear code; Reed–Muller code; Polynomial degree

1. Introduction

In [18], a relationship was established between gaps in the weight distribution of binary Reed–Muller codes of low order and constraints on the weight distribution of arbitrary binary linear codes. This relationship – a generalization of an idea by Brouwer [6] – has been exploited in [9,5], where it was instrumental in non-existence proofs for several binary linear codes of dimension nine. Thus, the authors of the present paper have the reasonable hope that a similar connection between the weight distribution of generalized Reed–Muller codes and that of q-ary linear codes will yield worthwhile results. Our goal is to describe this connection and to indicate possible applications.

1.1. Outline

Section 2 contains an overview of relevant facts concerning generalized Reed–Muller codes. The reader might be aware that at least six different non-equivalent definitions of this type of codes exist, cf. Grushko [10]. We prefer the definition of Kasami et al. [12,13] that has been admirably presented by Delsarte et al. [8].

* Corresponding author.
E-mail addresses: guritman@twi.tudelft.nl (S. Guritman), j.simonis@twi.tudelft.nl (J. Simonis).

PII: S0166-218X(00)00346-2

Sections 3 and 4 are devoted to symmetric and supersymmetric functions and their supports. If these functions have low degree, they can be used to derive constraints on the (complete) weight distribution of linear codes.

Finally, in Section 5, we describe the announced link between the weight distribution of generalized Reed–Muller codes and that of arbitrary linear codes. The paper ends with some examples and applications. In particular, we prove the non-existence of ternary linear codes with parameters $[74,10,44]$, $[82,6,53]$ and $[96,6,62]$. We are convinced that a thorough computerized investigation of the ternary table in [7] will yield many more non-existence results. Our constraints are much weaker for $q>3$. But then again the same is true for the corresponding tables. So even for $q>3$ there is some hope.

2. Degree of functions and affine subsets

Let $\mathbb{F}_q$ be the finite field with q elements, and let $f:\mathbb{F}_q^k\to\mathbb{F}_q$ be any $\mathbb{F}_q$-valued function on the standard vector space $\mathbb{F}_q^k$. Since for any $\boldsymbol{w}\in\mathbb{F}_q^k$ the polynomial function

$$\prod_{i=1}^{k}(1-(x_i-w_i)^{q-1})$$

is the characteristic function $\chi_{\{\boldsymbol{w}\}}$ of the 1-element subset $\{\boldsymbol{w}\}\subseteq\mathbb{F}_q^k$, we infer that

$$f(\boldsymbol{x})=\sum_{w\in\mathbb{F}_q^k} f(\boldsymbol{w})\chi_{\{\boldsymbol{w}\}}$$

is a polynomial function. Moreover, since $a^p=a$ for all $a\in\mathbb{F}_q$, the function f has a (unique) *reduced polynomial representation* of the form

$$f(\boldsymbol{x})=\sum_{\alpha\in W} a_\alpha \boldsymbol{x}^\alpha,$$

where

$$W:=\{(\alpha_1,\alpha_2,\ldots,\alpha_k)\in\mathbb{N}^k \mid 0\leqslant\alpha_u\leqslant q-1,\ u=1,2,\ldots,k\}$$

and

$$\boldsymbol{x}^\alpha:=x_1^{\alpha_1}x_2^{\alpha_2}\cdots x_k^{\alpha_k},\quad \alpha=(\alpha_1,\alpha_2,\ldots,\alpha_k).$$

Obviously, the degree of f is invariant under affine transformations of $\mathbb{F}_q^k$. Hence, the degree $\deg(f)$ of a function $f:\mathscr{C}\to\mathbb{F}_q$ on a k-dimensional $\mathbb{F}_q$-affine space $\mathscr{C}$ is well defined. Simply put $\deg(f):=\deg(f\circ\varphi)$, where $\varphi:\mathbb{F}_q^k\to\mathscr{C}$ is any affine isomorphism. We shall exploit this in Section 5, where $\mathscr{C}$ will be a k-dimensional *affine code* of length n, i.e. a k-dimensional affine subspace of $\mathbb{F}_q^n$.

We are interested in the size of the *support* $\mathrm{supp}(f)$ of f. If $\deg(f)\leqslant r$, then f can be interpreted as a word in the rth-order q-ary *generalized Reed–Muller code* $\mathscr{R}_q(r,k)$ of length q^k, and $|\mathrm{supp}(f)|$ then is the weight of this word (cf. [8,1,2]). Quite a few facts are known about the weight set of Reed–Muller codes. For $q{:=}2$, we refer to Proposition 2 of [18]. For the general case, we quote the following results.

Proposition 1. *Let $\mathscr{R}_q(r,k)$ be the rth-order q-ary generalized Reed–Muller code of length q^k. Then*

1. (Ax [3]). *all weights in $\mathscr{R}_q(r,k)$ are divisible by $q^{\lfloor (k-1)/r \rfloor}$*,
2. (cf. [1]) *the* minimum weight *of $\mathscr{R}_q(r,k)$ is equal to $(q-s)q^{k-t-1}$, with $t{:=}\lfloor r//(q-1) \rfloor$ and $s{:=}r-(q-1)t$.*

Remark 2. The supports of the minimum weight codewords in $\mathscr{R}_q(r,k)$ are the unions of $q-s$ distinct and parallel $(k-t-1)$-flats which are contained in a $(k-t)$-flat of the affine space $\mathbb{F}_q^k$. A – complicated – proof of this fact can be found in [8]. (See also [4], where the result was used to determine the automorphism group of $\mathscr{R}_q(r,k)$.) Consequently, the supports of the minimum weight codewords in $\mathscr{R}_q(t(q-1),k)$ are the $(k-t)$-flats of $\mathbb{F}_q^k$.

The weight set of $\mathscr{R}_q(2,k)$ has been completely determined by McEliece:

Proposition 3 (McEliece [17]). *Let $\mathscr{R}_q(2,k)$ be the second-order q-ary generalized Reed–Muller code of length q^k. Then all weights are of the form*

$$q^k - q^{k-1} + vq^{k-1-j},$$

where $v = 0,\ \pm 1$, or $\pm(q-1)$ and $0 \leqslant j \leqslant k//2$.

The weight sets of binary Reed–Muller codes are known to contain gaps that are not covered by Proposition 1, cf. [14]. Recently, Vance found such a gap in the ternary case.

Proposition 4 (Vance [19]).

1. *There is no word of weight $3^{k-2} + 3^{\lfloor (k-1)/4 \rfloor}$ in $\mathscr{R}_3(4,k)$ for $k \geqslant 6$.*
2. *Suppose $r \geqslant 2$ and for some $l \geqslant 2r^2 - r + 1$, there is no word of weight*
$$3^{l-r} + 3^{\lfloor (l-1)/2r \rfloor}$$
in $\mathscr{R}_3(2r,l)$. Then for all $k \geqslant l$, there is no word of weight
$$3^{k-r} + 3^{\lfloor (k-1)/2r \rfloor}$$
in $\mathscr{R}_3(2r,k)$.

Since we focus on subsets of $\mathbb{F}_q$-affine spaces, the following definition makes sense.

Definition 5. Let S be any subset of a k-dimensional $\mathbb{F}_q$-affine space $\mathscr{C}$. Then the *degree* of S in $\mathscr{C}$ is the non-negative integer

$$\deg(S){:=}\min\{\deg(f) \mid \operatorname{supp}(f) = S\}.$$

3. Symmetric functions on $\mathbb{F}_q^n$

The symmetric group $\mathfrak{S}_n$ over $\{1,2,\ldots,n\}$ acts on $\mathbb{F}_q^n$ by

$$\sigma(c_1,c_2,\ldots,c_n):=(c_{\sigma(1)},c_{\sigma(2)},\ldots,c_{\sigma(n)}).$$

Let the *complete weight* of $\boldsymbol{c}:=(c_1,c_2,\ldots,c_n)\in\mathbb{F}_q^n$ be the vector $\mathrm{cw}(\boldsymbol{c}):=(\mu_a)_{a\in\mathbb{F}_q}$, where the integers μ_a are given by

$$\mu_a:=|\{i\in\{1,2,\ldots,n\}\mid c_i=a\}|.$$

The vector $(0,2,1,0,2,0,0)\in\mathbb{F}_3^7$, for instance, has the complete weight $(4,1,2)$.

The set

$$W_n:=\left\{\mu\in\mathbb{N}^{\mathbb{F}_q}\;\middle|\;\sum_{a\in\mathbb{F}_q}\mu_a=n\right\}$$

lists the complete weights in $\mathbb{F}_q^n$. Its size is $\binom{n+q-1}{q-1}$. Then the orbits of $\mathfrak{S}_n$ in $\mathbb{F}_q^n$ are the subsets

$$S_\mu:=\{\boldsymbol{c}\mid w(\boldsymbol{c})=\mu\},\quad \mu\in W_n.$$

If, for example, $q=3$ and $\mu=(1,0,2)$, then

$$S_\mu=\{(0,2,2),(2,0,2),(2,2,0)\}.$$

Now consider the action

$$(\sigma f)(\boldsymbol{c}):=f(\sigma\boldsymbol{c})$$

of $\mathfrak{S}_n$ on the $\mathbb{F}_q$-vector space of the functions $f:\mathbb{F}_q^n\to\mathbb{F}_q$. A function $f:\mathbb{F}_q^n\to\mathbb{F}_q$ is said to be *symmetric* if $\sigma f=f$ for all $\sigma\in\mathfrak{S}_n$. An example of a symmetric function on $\mathbb{F}_3^2$ is the function

$$x_1x_2^2+x_1^2x_2+2x_1+2x_2.$$

The symmetric functions constitute a vector space Sym_n. Obviously, the symmetric functions are the functions that are constant on the S_ν. So the characteristic functions $\chi(S_\mu)$ of the symmetric sets S_μ form a basis for Sym_n. Hence, $\dim Sym_n=\binom{n+q-1}{q-1}$.

We define the *complete weight* of a reduced monomial

$$\boldsymbol{x}^\alpha:=x_1^{\alpha_1}x_2^{\alpha_2}\ldots x_n^{\alpha_n},\quad \alpha=(\alpha_1,\alpha_2,\ldots,\alpha_n),$$

to be the complete weight of the exponent vector α. So the complete weight of $\boldsymbol{x}^\alpha$ is the vector $\mathrm{cw}(\alpha):=(v_0,v_1,\ldots,v_{q-1})$, where the integers v_i are given by

$$v_a:=|\{i\in\{1,2,\ldots,n\}\mid\alpha_i=a\}|.$$

If, for example, $n=7$ and $q=3$, then the complete weight of the monomial $x_2^2x_3x_4^2$ is $(4,1,2)$.

The set

$$V_n := \left\{ \mu \in \mathbb{N}^q \,\middle|\, \sum_{a=0}^{q-1} v_a = n \right\}$$

lists the complete weights of the reduced monomials over $\mathbb{F}_q$ in n variables. Note that the only difference between W_n and V_n is that the vectors in the former set are parametrized by $\mathbb{F}_q$ and those in the latter by $\{0, 1, 2, \ldots, q-1\}$.

The $\binom{n+q-1}{q-1}$ polynomials

$$\varphi_v(\boldsymbol{x}) := \sum_{\mathrm{cw}(\alpha)=v} \boldsymbol{x}^\alpha, \quad v \in V_n,$$

constitute another basis of Sym_n. It is straightforward to express the φ_v as linear combinations of the $\chi(S_\mu)$.

Proposition 6. *$\varphi_v = \sum c_v^\mu \chi(S_\mu)$, with*

$$c_\mu^v = \sum_M \prod_{i \in \mathbb{F}_q} \binom{\mu_i}{m_{i,0} \quad m_{i,1} \quad \cdots \quad m_{i,q-1}} i^{\sum_{j=0}^{q-1} m_{i,j} \cdot j}. \tag{1}$$

(*The summation is over all arrays M of non-negative integers $m_{i,j}$, $i \in \mathbb{F}_q$ and $j \in \{0, 1, \ldots, \lambda\}$, that satisfy the conditions*

$$\sum_{i \in \mathbb{F}_q} m_{i,j} = v_j, \quad j = 0, 1, \ldots, q-1,$$

and

$$\sum_{j=0}^{q-1} m_{i,j} = \mu_i, \quad i \in \mathbb{F}_q.)$$

Proof. Choose a fixed vector $\boldsymbol{u} \in S_\mu$. Then c_μ^v is the value of φ_v on $\boldsymbol{u}$. Let us calculate the contribution of a monomial $\boldsymbol{x}^\alpha$ of φ_v to c_μ^v. Let us define

$$m_{i,j} := |\{a \in \{1, 2, \ldots, n\} \mid u_a = i \wedge \alpha_a = j\}|.$$

Then

$$\boldsymbol{u}^\alpha = \prod_{i \in \mathbb{F}_q} \prod_{j=0}^{q-1} (i^j)^{m_{i,j}} = \prod_{i \in \mathbb{F}_q} i^{\sum_{j=0}^{q-1} m_{i,j} \cdot j}$$

if we interpret 0^0 as 1. The number of exponent vectors that produce the same numbers $m_{i,j}$ as α is equal to the product of multinominals

$$\prod_{i \in \mathbb{F}_q} \binom{\mu_i}{m_{i,0} \quad m_{i,1} \quad \cdots \quad m_{i,q-1}}. \qquad \square$$

Admittedly, expression (1) is unwieldy for general q. But in the binary and ternary cases, we can derive more manageable formulas. For q:=2, the complete weight μ is of the form $(n-a,a)$, where a is the standard Hamming weight of $\boldsymbol{x} \in S_\mu$, and ν is of the form $(n-b,b)$, where b is the degree of φ_ν. Replacing μ by a and ν by b, we can reduce (1) to

$$c_a^b = \binom{a}{b},$$

cf. [18]. Now consider the *ternary* case. Put $\mu{:=}(n-a_1-a_2,a_1,a_2)$ and $\nu{:=}(n-b_1+b_2,b_1,b_2)$. Then (1) becomes

$$\begin{aligned} c_\mu^\nu &= \sum_{u,v} (-1)^u \begin{pmatrix} & a_1 & \\ a_1-b_1-b_2+u+v & b_1-u & b_2-v \end{pmatrix} \begin{pmatrix} & a_2 & \\ a_2-u-v & u & v \end{pmatrix} \\ &= \sum_{u,w} (-1)^u \binom{a_1}{b_1+b_2-w} \binom{a_2}{w} \binom{w}{u} \binom{b_1+b_2-w}{b_1-u} \end{aligned}$$

if we substitute $w=u+v$. We give some examples, with $\mu{:=}(n-a_1-a_2,a_1,a_2)$.

ν	φ_ν	c_μ^ν
$(n-1,1,0)$	$\sum x_i$	a_1-a_2
$(n-1,0,1)$	$\sum x_i^2$	a_1+a_2
$(n-2,0,2)$	$\sum x_i^2x_j^2$	$a_1+a_2-(a_1+a_2)^2$
$(n-2,2,0)$	$\sum x_ix_j$	$\binom{a_1}{2}+\binom{a_2}{2}-a_1a_2$

We see that for $\nu=(n-1,0,1),(n-2,0,2)$ the c_μ^ν actually depend on the *Hamming weight* a_1+a_2. In other words, the functions $\sum x_i^2$, $\sum x_i^2x_j^2$ are *constant* on the sets

$$\{\boldsymbol{x} \mid w(\boldsymbol{x})=a\},$$

where $w(\boldsymbol{x})$ denotes the (Hamming) weight of $\boldsymbol{x} \in \mathbb{F}_3^n$. This kind of "supersymmetric" functions will be discussed in the next section.

4. Supersymmetric functions on $\mathbb{F}_q^n$

The Hamming spheres

$$S_i{:=}\{\boldsymbol{x} \mid w(\boldsymbol{x})=i\}, \quad i=0,1,\ldots,n,$$

of $\mathbb{F}_q^n$ are the orbits of the monomial group $\mathfrak{M}_n$. By definition, this is the transformation group of $\mathbb{F}_q^n$ generated by the coordinate permutations and the transformations of the form

$$(x_1,x_2,\ldots,x_n) \mapsto (ax_1,x_2,\ldots,x_n),$$

with $a \in \mathbb{F}_q \setminus \{0\}$.

Remark 7. Note that the subscript i of S_i denotes an *integer* and not a vector of length q, as was the case in the preceding section. In the current section we shall always use S_i in its new sense.

Definition 8. A function $f : \mathbb{F}_q^n \to \mathbb{F}_q$ is said to be *supersymmetric* if $\sigma f = f$ for all $\sigma \in \mathfrak{M}_n$.

Since the supersymmetric functions are the functions that are constant on the Hamming spheres, they form an $(n+1)$-dimensional subspace $SSym_n$ of the vector space Sym_n. Let us describe another basis.

For any subset $I \subseteq \{1,2,\ldots,n\}$ the monomial $\prod_{i\in I} x_i$ will be denoted by $\boldsymbol{x}_I$. Then we consider the $n+1$ supersymmetric functions

$$\varphi_j := \sum_{|I|=j} (\boldsymbol{x}_I)^{q-1}, \quad j = 0,1,\ldots,n.$$

Remark 9. Analogous to Remark 7, we observe that the subscript of φ_j is an integer. There is no chance of confusion with the notation of the preceding section because here we only use φ_j with its new meaning.

Proposition 10. *For $j = 0,1,\ldots,n$, we have*

$$\varphi_j = \sum_{i=0}^{n} \binom{i}{j} \chi(S_i) \tag{2}$$

and

$$\chi(S_j) = \sum_{i=0}^{n} (-1)^{i+j} \binom{i}{j} \varphi_i. \tag{3}$$

Hence the φ_j constitute a basis for the vector space $SSym_n$.

Proof. Let I be the support of a vector $\boldsymbol{c} \in \mathbb{F}_q^n$. Then the monomial $(x_J)^{q-1}$ takes the value 1 on $\boldsymbol{c}$ if $J \subseteq I$ and the value 0 otherwise. This accounts for Formula (2). Formula (3) then follows from the standard binomial inversion formula

$$\sum_{j=0}^{n} (-1)^{i+j} \binom{i}{j} \binom{j}{k} = \begin{cases} 1 & \text{if } i = k, \\ 0 & \text{otherwise.} \end{cases} \qquad \square$$

Example 11. Take q:=3. Then

$$\begin{bmatrix} 1 \\ \varphi_1 \\ \varphi_2 \\ \varphi_3 \\ \varphi_4 \\ \varphi_5 \\ \varphi_6 \\ \varphi_7 \\ \varphi_8 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 0 & 0 & 0 & 0 & 1 & 2 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} \chi(S_0) \\ \chi(S_1) \\ \chi(S_2) \\ \chi(S_3) \\ \chi(S_4) \\ \chi(S_5) \\ \chi(S_6) \\ \chi(S_7) \\ \chi(S_8) \end{bmatrix}$$

describes the first nine supersymmetric functions in terms of the $\chi(S_i)$. If $n < 8$, we put $\chi(S_i)$:=0 for $i = n+1,\dots,8$.

Definition 12. A subset $I \subseteq \{0,1,\dots,n\}$ is said to have *period m* if it is a union of sets of the form

$$\{u \in \{0,1,\dots,n\} \mid u \equiv a \bmod m\}.$$

If I has period m, then the union of Hamming spheres

$$S_I := \bigcup_{i \in I} S_i \subseteq \mathbb{F}_q^n$$

is also said to have period m.

For example, the subset $\{1,3,6,8,11,13,16\} = \{1,6,11,16\} \cup \{3,8,13\}$ of $\{0,1,\dots,16\}$ has period 5.

Henceforth, let p denote the characteristic of the field $\mathbb{F}_q$. In the sequel we shall investigate the degree of sets S_I of period p^r. We shall need a result of Lucas' in the following form.

Lemma 13 (Lucas [15]). *Let p be a prime, and let $a := a_1 + a_2 p^r$, $b := b_1 + b_2 p^r$ be non-negative integers with $0 \leqslant a_1, b_1 < p^r$. Then*

$$\binom{a}{b} \equiv \binom{a_1}{b_1}\binom{a_2}{b_2} \bmod p.$$

Proposition 14. *If S_I has period p^r, then* $\deg(S_I) \leqslant (q-1)(p^r - 1)$.

Proof. Obviously, it suffices to prove the statement for sets I of the form

$$\{u \in \{0,1,\dots,n\} \mid u \equiv a \bmod p^r\}.$$

In the following, put $\chi(S_j)$:=0 and φ_j:=0 if $j > n$.

If $i < p^r$, then

$$\begin{aligned}\varphi_i &= \sum_{j=0}^{n} \binom{j}{i} \chi(S_j)\\ &= \sum_{j \geqslant 0} \binom{j}{i} \chi(S_j)\\ &= \sum_{a=0}^{p^r-1} \sum_{b \geqslant 0} \binom{a}{i} \binom{b}{0} \chi(S_{a+bp^r})\\ &= \sum_{a=0}^{p^r-1} \binom{a}{i} \sum_{u \equiv a(p^r)} \chi(S_u).\end{aligned}$$

Now, apply the binomial inversion formula

$$\sum_{u \equiv a(p^r)} \chi(S_u) = \sum_{i=0}^{p^r-1} (-1)^{a+i} \binom{i}{a} \varphi_i. \qquad \square$$

The product of supersymmetric functions is supersymmetric. In fact, the vector space $SSym_n$ is an algebra. In the next section, we shall use a certain factorization of the function $\sum_{i=0}^{p^r-1} (-1)^i \varphi_i$.

Lemma 15. *If $a < p^r$, then $\varphi_a \varphi_{bp^r} = \varphi_{a+bp^r}$.*

Proof. Note that

$$\chi(S_i)\chi(S_j) = \begin{cases} \chi(S_i) & \text{if } i = j,\\ 0 & \text{otherwise.} \end{cases}$$

Hence, we infer that

$$\begin{aligned}\varphi_a \varphi_{bp^r} &= \left(\sum_{i=0}^{n} \binom{i}{a} \chi(S_i) \right) \left(\sum_{j=0}^{n} \binom{j}{bp^r} \chi(S_j) \right)\\ &= \sum_{i=0}^{n} \binom{i}{a} \binom{i}{bp^r} \chi(S_i)\\ &= \sum_{i=0}^{n} \binom{i}{a+bp^r} \chi(S_i) = \varphi_{a+bp^r}.\end{aligned}$$

Here, we use Lucas' Lemma again: if $i = u + vp^r$, with $0 \leqslant u < p^r$, then

$$\begin{aligned}\binom{i}{a}\binom{i}{bp^r} &= \binom{u}{a}\binom{v}{0}\binom{i}{0}\binom{v}{b}\\ &= \binom{u}{a}\binom{v}{b}\\ &= \binom{i}{a+bp^r}. \qquad \square\end{aligned}$$

Corollary 16.

$$\begin{aligned}\sum_{u\equiv 0(p^{r+s})} \chi(S_u) &= \sum_{i=0}^{p^{r+s}-1} (-1)^i \varphi_i\\ &= \left(\sum_{i=0}^{p^r-1}(-1)^i\varphi_i\right)\left(\sum_{i=0}^{p^s-1}(-1)^i\varphi_{ip^r}\right)\\ &= \left(\sum_{u\equiv 0(p^r)}\chi(S_u)\right)\left(\sum_{i=0}^{p^s-1}(-1)^i\varphi_{ip^r}\right).\end{aligned}$$

5. Weight restrictions for affine codes

Let $\mathscr{C} \subseteq \mathbb{F}_q^n$ be a k-dimensional q-ary affine code of length n, i.e. a coset of a k-dimensional linear code in $\mathbb{F}_q^n$. For $\mu \in W_n$, put

$$\mathscr{A}_\mu(\mathscr{C}) := \{c \in \mathscr{C} \mid \mathrm{cw}(c) = \mu\} = S_\mu \cap \mathscr{C}.$$

Then the non-negative integers $A_\mu(\mathscr{C}) := |\mathscr{A}_\mu(\mathscr{C})|$ are said to constitute the *complete weight distribution* of the code $\mathscr{C}$.

If φ is a function of degree r on $\mathbb{F}_q^n$, its restriction ψ to $\mathscr{C}$ obviously is a function of degree $\leqslant r$ on the k-dimensional affine space $\mathscr{C}$. So ψ defines a word in the Reed–Muller code $\mathscr{R}_q(r,k)$. As a matter of fact, the degree of ψ may be less than r. For example, if $\varphi = \alpha\beta$ and if α is constant on $\mathscr{C}$, then $\deg\psi \leqslant \deg\beta$.

Now it is important to note that if φ is *symmetric*, the support of ψ is a (disjoint) union of sets of the form $\mathscr{A}_\mu(\mathscr{C})$. Putting

$$I_\varphi := \{\mu \in W_n \mid \varphi(\boldsymbol{c}) \neq 0 \text{ for } \boldsymbol{c} \in \mathscr{A}_\mu(\mathscr{C})\},$$

we have

$$\mathrm{supp}\,\psi = \bigcup_{\mu\in I_\varphi} \mathscr{A}_\mu(\mathscr{C})$$

and

$$|\mathrm{supp}\,\psi| = \sum_{\mu\in I_\varphi} A_\mu(\mathscr{C}).$$

Since ψ is a word of weight $|\mathrm{supp}\,\psi|$ in the Reed–Muller code $\mathscr{R}_q(\deg\psi, k)$, we immediately obtain the following result.

Theorem 17. *Let φ be a symmetric function on $\mathbb{F}_q^n$, and let $\mathscr{C} \subseteq \mathbb{F}_q^n$ be a k-dimensional affine code. Then*

$$\sum_{\mu\in I_\varphi} A_\mu(\mathscr{C})$$

is a weight in the Reed–Muller code $\mathscr{R}_q(\deg\psi, k) \subseteq \mathscr{R}_q(\deg r, k)$, where ψ is the restriction of φ to $\mathscr{C}$.

If $\mathscr{C}$ is *linear*, this theorem, in combination with Propositions 1, 3 and 4, can be used to strengthen the MacWilliams identities for the complete weight distributions of $\mathscr{C}$ and $\mathscr{C}^\perp$ (see [16]). We do not pursue this further here, but turn to the Hamming weight distribution.

Let us define

$$\mathscr{A}_i(\mathscr{C}) := \{c \in \mathscr{C} \mid w(c) = i\}, \quad i = 0, 1, \ldots, n$$

and

$$A_i(\mathscr{C}) := |\mathscr{A}_i(\mathscr{C})|.$$

Then the sequence $A_0(\mathscr{C}), A_1(\mathscr{C}), \ldots, A_n(\mathscr{C})$ is called the (*Hamming*) *weight distribution* of $\mathscr{C}$. For a supersymmetric function $\varphi \in SSym_n$, we define

$$I_\varphi := \{i \in \{0, 1, \ldots, n\} \mid \varphi(\boldsymbol{c}) \neq 0 \text{ for } \boldsymbol{c} \in \mathscr{A}_i(\mathscr{C})\}.$$

Then Theorem 17 specializes to the following result.

Theorem 18. *Let φ be a supersymmetric function on $\mathbb{F}_q^n$, and let $\mathscr{C} \subseteq \mathbb{F}_q^n$ be a k-dimensional affine code. Then*

$$\sum_{i\in I_\varphi} A_i(\mathscr{C})$$

is a weight in the Reed–Muller code $\mathscr{R}_q(\deg\psi, k) \subseteq \mathscr{R}_q(\deg r, k)$, where ψ is the restriction of φ to $\mathscr{C}$.

Remark 19. If $\mathscr{C}$ is *linear*, then not every weight in $\mathscr{R}_q(\deg r, k)$ is a candidate for a specific sum $\sum_{i\in I_\varphi} A_i(\mathscr{C})$. Since $(q-1) \mid A_i(\mathscr{C})$ for all $i \neq 0$, we have

$$\sum_{i\in I_\varphi} A_i(\mathscr{C}) \equiv \begin{cases} 1 \bmod (q-1) & \text{if } 0 \in I_\varphi, \\ 0 \bmod (q-1) & \text{if } 0 \notin I_\varphi. \end{cases}$$

We end this paper by listing a few consequences of the preceding theorem. In the sequel, p denotes the characteristic of the field $\mathbb{F}_q$. The results are formulated for linear codes.

Proposition 20. *Let $\mathscr{C}$ be a k-dimensional q-ary linear code. Then the integers $\sum_{i\not\equiv u(p)} A_i(\mathscr{C})$ are weights in $\mathscr{R}_q(q-1,k)$. Hence*
1. $\sum_{i\not\equiv u(p)} A_i(\mathscr{C})$ *is divisible by* $q^{\lfloor (k-1)/(q-1)\rfloor}$ *for* $u=0,1,\ldots,p-1$,
2. $\sum_{i\not\equiv u(p)} A_i(\mathscr{C}) \geqslant q^{k-1}$ *for* $u=1,2,\ldots,p-1$, *and*
3. *if* $\sum_{i\not\equiv 0(p)} A_i(\mathscr{C}) \neq 0$, *then* $\sum_{i\not\equiv 0(p)} A_i(\mathscr{C}) > q^{k-1}$.

Proof. The supersymmetric functions $\varphi_1 - u$, $u=0,1,\ldots,p-1$, have degree $q-1$. The intersection of their support with $\mathscr{C}$ is $\bigcup_{i\not\equiv u(p)} \mathscr{A}_i(\mathscr{C})$. Now apply Theorem 18 and Proposition 1. The $>$ sign in part 3 is a consequence of Remark 19. □

Corollary 21. *Taking the complement in $\mathscr{C}$, we immediately find that*
1. $\sum_{i\equiv u(p)} A_i(\mathscr{C})$ *is divisible by* $q^{\lfloor (k-1)/(q-1)\rfloor}$ *for* $u=0,1,\ldots,p-1$,
2. $\sum_{i\equiv u(p)} A_i(\mathscr{C}) \leqslant q^k - q^{k-1}$ *for* $u=1,2,\ldots,p-1$, *and*
3. *if* $\sum_{i\equiv 0(p)} A_i(\mathscr{C}) \neq q^k$, *then* $\sum_{i\not\equiv 0(p)} A_i(\mathscr{C}) < q^k - q^{k-1}$.

In the ternary case, we can use McEliece's Proposition 3.

Proposition 22. *If $\mathscr{C}$ is a ternary linear code of dimension k, then the integers $\sum_{i\not\equiv u(3)} A_i(\mathscr{C})$, $u=0,1,2$, are weights in the Reed–Muller code $\mathscr{R}_3(2,k)$, i.e. they are of the form*

$$3^k - 3^{k-1} + v3^{k-1-j},$$

where $v=0,\pm 1$, or ± 2 and $0\leqslant j\leqslant k/2$. Hence

$$\sum_{i\equiv 0(3)} A_i(\mathscr{C}) \in \{q^{k-1}, q^{k-1} \pm 2\cdot 3^{k-1-j}\ (0\leqslant j\leqslant k/2)\}$$

and

$$\sum_{i\equiv u(3)} A_i(\mathscr{C}) \in \{q^{k-1} \pm 3^{k-1-j}\ (0\leqslant j\leqslant k/2)\}, \quad u=1,2.$$

Example 23. Let us consider a putative ternary linear $[39,6,24]$-code $\mathscr{C}$. Using the standard residual code argument, we see that its weight set is contained in

$$\{0,24,27,28,29,30,33,36,37,38,39\}.$$

Moreover, the non-existence of $[38,6,24]$-codes and $[37,5,24]$-codes implies that the dual distance of $\mathscr{C}$ is at least 3. Linear programming with the full set of MacWilliams identities now gives that

$$\sum_{i\not\equiv 0(3)} A_i(\mathscr{C}) = A_{28} + A_{29} + A_{37} + A_{38} \leqslant 242.$$

Since $242 < 3^5$, the preceding proposition implies that

$$A_{28} + A_{29} + A_{37} + A_{38} = 0.$$

Hence all weights in $\mathscr{C}$ must be divisible by three. By similar arguments one can prove that the same holds for the putative ternary codes with parameters $[66,6,42]$, $[79,6,51]$ and $[93,6,60]$.

Proposition 24. *No ternary linear codes with parameters* $[74,10,44]$ *or* $[82,6,53]$ *exist.*

Proof. We apply the usual linear program with respect to the MacWilliams equations and information on the dual distance and non-existence of residual codes from the table in [7]. If we add the constraints from Proposition 22, we infer that all weights must be congruent to 0 or 2 modulo 3. But then we can use a result of Hill and Lizak [11] which states that an $[n,k,d]_q$-code with $\gcd(d,q)=1$ and with all weights congruent to 0 or d modulo q can be extended to an $[n+1,k,d+1]_q$-code. The table in [7], however, tells us that there are no codes with parameters $[75,10,45]_3$ or $[83,6,54]_3$. □

Proposition 25. *Let* $\mathscr{C}$ *be a* k*-dimensional* q*-ary linear code, and let* $I(u) := \{up^r + x + yp^{r+1} \mid 0 \leqslant x < p^r \wedge y \geqslant 0\}$. *Then the integers* $\sum_{i \notin I(u)} A_i(\mathscr{C})$ *are weights in* $\mathscr{R}_q((q-1)p^r, k)$. *Hence*

1. $\sum_{i \notin I(u)} A_i(\mathscr{C})$ *is divisible by* $q^{\lfloor (k-1)/(q-1)p^r \rfloor}$ *for* $u = 0,1,\ldots,p-1$,
2. $\sum_{i \not\equiv I(u)} A_i(\mathscr{C}) \geqslant q^{k-p^r}$ *for* $u = 1,2,\ldots,p-1$, *and*
3. *if* $\sum_{i \not\equiv I(0)} A_i(\mathscr{C}) \neq 0$, *then* $\sum_{i \not\equiv I(0)} A_i(\mathscr{C}) > q^{k-p^r}$.

Proof. Consider support of the supersymmetric functions $\varphi_{p^r} - u$ of degree $(q-1)p^r$. □

Corollary 26. *Taking the complement in* $\mathscr{C}$ *leads to the following equivalent formulation.*

1. $\sum_{i \equiv I(u)} A_i(\mathscr{C})$ *is divisible by* $q^{\lfloor (k-1)/(q-1)p^r \rfloor}$ *for* $u = 0,1,\ldots,p-1$,
2. $\sum_{i \equiv I(u)} A_i(\mathscr{C}) \leqslant q^k - q^{k-p^r}$ *for* $u = 1,2,\ldots,p-1$, *and*
3. *if* $\sum_{i \equiv I(0)} A_i(\mathscr{C}) \neq q^k$, *then* $\sum_{i \not\equiv I(0)} A_i(\mathscr{C}) < q^k - q^{k-p^r}$.

Corollary 27. *If all weights in the* k*-dimensional* q*-ary linear code* $\mathscr{C}$ *are divisible by* p^r, *then*

1. $\sum_{i \equiv u(p)} A_{ip^r}(\mathscr{C})$ *is divisible by* $q^{\lfloor (k-1)/(q-1)p^r \rfloor}$ *for* $u = 0,1,\ldots,p-1$,
2. $\sum_{i \equiv u(p)} A_{ip^r}(\mathscr{C}) \leqslant q^k - q^{k-p^r}$ *for* $u = 1,2,\ldots,p-1$, *and*
3. *if* $\sum_i A_{ip^{r+1}}(\mathscr{C}) \neq q^k$, then $\sum_i A_{ip^{r+1}}(\mathscr{C}) < q^k - q^{k-p^r}$.

Proposition 28. *If* $\mathscr{C}$ *is a* q*-ary linear code of dimension* k, *then the integers* $\sum_{i \equiv u(p^r)} A_i(\mathscr{C})$, $u = 0,1,\ldots,p-1$, *are weights in the Reed–Muller code* $\mathscr{R}_q((q-1)(p^r-1),k)$. *So*

1. $\sum_{i \equiv u(p^r)} A_i(\mathscr{C})$ *is divisible by* $q^{\lfloor (k-1)/(q-1)(p^r-1) \rfloor}$.
2. *If* $\sum_{i \equiv u(p^r)} A_i(\mathscr{C}) \neq 0$, *then* $\sum_{i \equiv u(p^r)} A_i(\mathscr{C}) \geqslant q^{k-p^r+1}$.

Proof. Use Propositions 14 and 1. □

Remark 29. In the case $q{:=}3$ and $r{:=}1$, we also might put Vance's Proposition 4 to good use.

Proposition 30. *If all weights in the k-dimensional q-ary linear code $\mathscr{C}$ are divisible by p^r, then*

$$\sum_{i\equiv 0(p^{r+s})} A_i(\mathscr{C}) \geqslant q^{k-p^r(p^s-1)}.$$

Proof. Using Corollary 16, we see that the restriction of the function $\sum_{i=0}^{p^{r+s}-1}(-1)^i\varphi_i$ to $\mathscr{C}$ actually has degree $\leqslant (q-1)p^r(p^s-1)$. Now apply part 2 of Proposition 1. (The integer $\sum_{i\equiv 0(p^{r+s})} A_i(\mathscr{C})$ cannot be zero, because a linear code always contains the zero vector.) □

Example 31. If all weights in the k-dimensional ternary linear code $\mathscr{C}$ are divisible by 3, then

$$\sum_{i\equiv 0(9)} A_i(\mathscr{C}) \geqslant 3^{k-6}.$$

Finally, we use Remark 2 in combination with preceding results on lower bounds to obtain the following results.

Proposition 32 (Cf. Proposition 20)**.** *If $\mathscr{C}$ is a k-dimensional linear code over $\mathbb{F}_q$ such that for some $u \in \{1, 2, \ldots, p-1\}$ we have*

$$\sum_{i\not\equiv u(p)} A_i(\mathscr{C}) = q^{k-1},$$

then

$$\{\boldsymbol{c} \in \mathscr{C} \mid w(\boldsymbol{c}) \not\equiv u(p)\}$$

is a linear subcode of $\mathscr{C}$ of dimension $k-1$.

We use this proposition in proving the following non-existence result.

Proposition 33. *No ternary linear* $[96, 6, 62]$*-code exists.*

Proof. The dual distance of such a code $\mathscr{C}$ is at least 3 and by the usual arguments we can reduce the possible weights to

$$[0, 62, 63, 66, 67, 68, 69, 71, 72, 75, 76, 77, 78, 80, 81, 84, 85, 86, 87, 90, 95].$$

Then Proposition 22 together with linear programming with respect to the MacWilliams equations lead to the following four possibilities for the numbers $A^{(u)} := \sum_{i \equiv u(3)} A_i(\mathscr{C})$:

$A^{(0)}$	$A^{(1)}$	$A^{(2)}$
81	162	486
243	0	486
405	0	324
729	0	0

Since no ternary $[97, 6, 63]$-code exists, the trick [11] by Hill and Lizak eliminates all but the first case. Then the preceding proposition tells us that the words of weight congruent to 0 or 1 modulo 3 constitute a 1-codimensional subcode $\mathscr{D}$. Let $\boldsymbol{x}$ be a word with $w(\boldsymbol{x}) \equiv 1 \bmod 3$ and $\boldsymbol{y}$ a word with $w(\boldsymbol{y}) \equiv 2 \bmod 3$. Since $\boldsymbol{x} \in \mathscr{D}$ and $\boldsymbol{y} \notin \mathscr{D}$, both $\boldsymbol{x}+\boldsymbol{y}$ and $\boldsymbol{x}-\boldsymbol{y}$ are in the complement of $\mathscr{D}$. Hence, $w(\boldsymbol{x}+\boldsymbol{y}) \equiv 2 \bmod 3$ and $w(\boldsymbol{x}-\boldsymbol{y}) \equiv 2 \bmod 3$. This contradicts the well-known ternary formula

$$w(\boldsymbol{x}) + w(\boldsymbol{y}) + w(\boldsymbol{x}+\boldsymbol{y}) + w(\boldsymbol{x}-\boldsymbol{y}) \equiv 0 \bmod 3. \qquad \square$$

Proposition 34. *If $\mathscr{C}$ is a k-dimensional linear code over $\mathbb{F}_q$ such that*

$$\sum_{i \equiv 0(p^r)} A_i(\mathscr{C}) = q^{k-p^r+1},$$

then

$$\{\boldsymbol{c} \in \mathscr{C} \mid w(\boldsymbol{c}) \equiv 0(p^r)\}$$

is a linear subcode of $\mathscr{C}$ of dimension $k - p^r + 1$.

Example 35. A quaternary linear code $\mathscr{C}$ of dimension k contains at least 4^{k-1} words whose weights are divisible by 2. If $\mathscr{C}$ contains exactly 4^{k-1} such words, then these constitute a linear subcode of codimension 1.

Proposition 36. *If $\mathscr{C}$ is a k-dimensional linear code over $\mathbb{F}_q$ such that all weights are divisible by p^r and such that*

$$\sum_{i \equiv 0(p^{r+s})} A_i(\mathscr{C}) = q^{k-p^r(p^s-1)},$$

then

$$\{\boldsymbol{c} \in \mathscr{C} \mid w(\boldsymbol{c}) \equiv 0(p^{r+s})\}$$

is a linear subcode of $\mathscr{C}$ of dimension $k - p^r(p^s - 1)$.

Example 37. If all weights in a k-dimensional quaternary linear code $\mathscr{C}$ are divisible by 2, then $\mathscr{C}$ contains at least 4^{k-2} words whose weights are divisible by 4. If

$\mathscr{C}$ contains exactly 4^{k-2} such words, then these constitute a linear subcode of co-dimension 2.

Acknowledgements

The authors would like to thank Pascale Charpin for providing a copy of the key reference [17].

References

[1] E.F. Assmus Jr., J.D. Key, Designs and Their Codes, Cambridge University Press, Cambridge, 1992.
[2] E.F. Assmus Jr., J.D. Key, Polynomial codes and finite geometries, in: V.S. Pless, W.C. Huffman (Eds.), Handbook of Coding Theory, Elsevier, Amsterdam, 1998.
[3] J. Ax, Zeroes of polynomials over finite fields, Amer. J. Math. 86 (1964) 255–261.
[4] T.P. Berger, P. Charpin, The automorphism group of the generalized Reed–Muller codes, Discrete Math. 117 (1993) 1–17.
[5] I. Boukliev, S. Guritman, V. Vavrek, Some bounds for the minimum length of binary linear codes of dimension nine, IEEE Trans. Inform. Theory 46 (2000) 1053–1056.
[6] A.E. Brouwer, The linear programming bound for binary linear codes, IEEE Trans. Inform. Theory 39 (1993) 677–680.
[7] A.E. Brouwer, Bounds on the size of linear codes, in: V.S. Pless, W.C. Huffman (Eds.), Handbook of Coding Theory, Elsevier, Amsterdam, 1998.
[8] P. Delsarte, J.-M. Goethals, F.J. MacWilliams, On generalized Reed–Muller codes and their relatives, Inform. and Control 16 (1970) 403–442.
[9] S. Dodunekov, S. Guritman, J. Simonis, Some new results on the minimum length of binary linear codes of dimension nine, IEEE Trans. Inform. Theory 45 (1999) 2543–2546.
[10] I.I. Grushko, O shesti obobshcheniyakh kodov Rida-Mallera po nedwoichniy sluchay, in: Kodirovanie i Peredacha Diskretnykh Soobshcheniy v Sistemakh Svyazi, Akademia Nauk SSSR, Institut Problem Peredachi Informatsii, Moscow, 1976, pp. 61–73.
[11] R. Hill, P. Lizak, Extensions of linear codes, Proceedings of the International Symposium on Information and Theory, Whistler, Canada, 1995, p. 345.
[12] T. Kasami, S. Lin, W.W. Peterson, New generalization of the Reed–Muller codes – Part I: primitive codes, IEEE Trans. Inform. Theory 14 (1968) 189–199.
[13] T. Kasami, S. Lin, W.W. Peterson, Polynomial codes, IEEE Trans. Inform. Theory 14 (1968) 807–814.
[14] T. Kasami, N. Tokura, S. Azumi, On the weight enumeration of weights less then 2.5d of Reed–Muller codes, Inform. Control 30 (1976) 380–396.
[15] M.E. Lucas, Sur les congruences des nombres Euleriennes, et des coefficients différentials des fonctions trigonométriques, suivant un nombre premier, Bull. Soc. Math. France 6 (1878) 49–54.
[16] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes, 2nd reprint, North-Holland, Amsterdam, 1983.
[17] R.J. McEliece, Quadratic forms over finite fields and second-order Reed–Muller codes, JPL Space Programs Summary 37-58-III (1969) 28–33.
[18] J. Simonis, Restrictions on the weight distribution of binary linear codes imposed by the structure of Reed–Muller codes, IEEE Trans. Inform. Theory 40 (1994) 194–196.
[19] T.D. Vance, A gap in GRM code weight distributions, Des. Codes Cryptogr. 19 (2000) 27–43.