Codes from symmetric polynomials

Mrinmoy Datta and Trygve Johnsen

Abstract. We define and study a class of Reed-Muller type error-correcting codes obtained from elementary symmetric functions in finitely many variables. We determine the code parameters and higher weight spectra in the simplest cases.

1. Introduction

Over the last decades, good examples of error-correcting codes have been constructed using algebraic geometric techniques. The codes constructed this way are linear codes over a given finite field k, where each member of a finite dimensional vector space of functions, say V, are evaluated at a finite set of points, say S, all lying in an affine space or a projective space over the same field k. Examples are simplex codes, Reed-Muller codes ([**9**]), algebraic-geometric codes with S a curve (Goppa codes) ([**4**]) or a higher dimensional variety ([**2**]), Grassmann codes ([**8**]), and codes where the points in question represent synmmetric or skew-symmetric matrices ([**3**]).

Having defined such codes, it is imperative that one looks for their parameters such as dimensions, minimum distance, weight distributions, generalized Hamming weights etc. These questions are often related to question that are interesting from the perspective of algebraic geometry, number theory and various branches of discrete mathematics. For instance, one checks easily that the minimum distance of a code defined using methods described above is equivalent to determining the maximum possible number of zeroes that a function in V (that does not vanish identically in S) may have in S.

In this paper we study a class of codes that are motivated from the Reed-Muller codes. While defining a Reed-Muller code, one evaluates the set of all reduced polynomials of degrees bounded above by a given quantity on the whole of affine space. Instead, here we consider a subspace of the set of all symmetric polynomials and evaluate them on points from affine spaces that have pairwise distinct coordinates. As it turns out, the relative minimum distance of our codes is same as that of Reed-Muller codes. However, relative dimension of the code is not as good. To this end, we introduce a modified

2020 *Mathematics Subject Classification.* 05E45, 94B05, 05B35, 13F55.

The first named author is partially supported by a seed grant from Indian Institute of Technology Hyderabad. Both authors have been partially supported by grant 280731 from the Research Council of Norway, and by the project “Pure Mathematics in Norway" through the Trond Mohn Foundation and Tromsø Research Foundation.

family of codes that has the same relative minimum distance, but a better rate. We also show that, like the Reed-Muller codes, the new codes are also generated by minimum weight codewords. This property, in particular, makes the duals of the new codes useful.

We remark that this study has been motivated by a study of properties of Rational Normal Curves as an arc and possibility of extension of Reed-Solomon codes to an MDS code of higher length. However, we do not address these issues as they are beyond the scope of this paper.

This article is organized as follows: In Section 2, we study the number of points over finite with pairwise distinct coordinates satisfying multivariate symmetric polynomials that are linear combinations of elementary symmetric polynomials over a finite field. In Section 3, we introduce the new family of codes and study their properties, such as their dimension, minimum weight and minimum weight codewords. In Section 4, we derive upper bounds on the generalized Hamming weights of the codes. In Section 5, we work with the codes that occur from symmetric polynomials in two variables and prove several results including their generalized Hamming weights, weight distributions and higher weight spectra. In Section 6, we specially concentrate on trivariate symmetric polynomials over a field with 5 elements for the sake of illustrating the difficulties in obtaining the parameters in higher dimensions.

2. Symmetric polynomials and their distinguished zeroes

Let k be a field. In most cases, we shall restrict our attention to the case when $k = \mathbb{F}_q$, i.e. k is a finite field with q elements where q is a prime power. For a positive integer m and a nonnegative integer i, we denote by σ_m^i the i-th elementary symmetric polynomial in m variables $x_1, \dots, x_m$. It is well known that any symmetric polynomial $f \in k[x_1, \dots, x_m]$ can be written as an algebraic expression in $\sigma_m^0, \dots, \sigma_m^m$. However, in this article we are interested in symmetric polynomials that are k-linear combinations of elementary symmetric polynomials. We denote by Σ_m the k-linear subspace generated by the elementary symmetric polynomials $\sigma_m^0, \dots, \sigma_m^m$. Note that $\dim_k \Sigma_m = m + 1$.

For a given polynomial $f \in k[x_1, \dots, x_m]$, we denote by $Z_k(f)$ the set of zeroes of f in $\mathbb{A}^m(k)$, the m-dimensional affine space over k. A point $(a_1, \dots, a_m) \in \mathbb{A}^m(k)$ is said to be *distinguished* if $a_i \neq a_j$ whenever $i \neq j$. In this paper, we are interested in the distinguished zeroes of symmetric polynomials described in the last paragraph. For ease of reference, we shall denote by $\mathbb{A}_D(k)^m$ the set of all distinguished points of $\mathbb{A}^m(k)$. For a subset $S \subset k$, and a polynomial $f \in k[x_1, \dots, x_m]$, we denote by $Z_{S,D}(f)$ the set of all distinguished zeroes of f in S^m. Thus,

$$Z_{S,D}(f) := \{(a_1, \dots, a_m) \in S^m \mid f(a_1, \dots, a_m) = 0, a_i \neq a_j \text{ for all } i \neq j\}.$$

In particular, given a polynomial $f \in k[x_1, \dots, x_m]$, we denote by $Z_{k,D}(f)$ the set of distinguished zeroes of f in $\mathbb{A}^m(k)$.

Next we introduce a combinatorial notation for ease of reading. For positive integers n, r we denote by $\mathcal{P}(n, r)$ the number of possible arrangements of r objects taken from n distinct objects. More precisely,

$$\mathcal{P}(n,r) = \begin{cases} \binom{n}{r} r! & \text{if } r \leq n \\ 0 & \text{otherwise.} \end{cases}$$

It follows trivially that $|\mathbb{A}_D(\mathbb{F}_q)^m| = \mathcal{P}(q,m)$. We are interested in analyzing the number of distinguished zeroes of a symmetric polynomial that is a linear combinations of the elementary symmetric polynomials on certain finite grids in $\mathbb{A}^m(k)$. Before we state our main result towards this direction, let us state a few remarks on such polynomials. Let $f \in k[x_1, \dots, x_m]$ be given by

$$f = a_0 + a_1\sigma_m^1 + \cdots + a_m\sigma_m^m \tag{1}$$

where $a_0, \dots, a_m \in k$. It can be verified readily that

$$f = \left(a_0 + a_1\sigma_{m-1}^1 + \cdots + a_{m-1}\sigma_{m-1}^{m-1}\right) + x_m\left(a_1 + a_2\sigma_{m-1}^1 + \cdots + a_m\sigma_{m-1}^{m-1}\right). \tag{2}$$

For simplicity, we shall write

$$f = f_1 + x_m f_2, \tag{3}$$

where

$$f_1 = a_0 + a_1\sigma_{m-1}^1 + \cdots + a_{m-1}\sigma_{m-1}^{m-1} \quad \text{and} \quad f_2 = a_1 + a_2\sigma_{m-1}^1 + \cdots + a_m\sigma_{m-1}^{m-1}.$$

We may readily observe that a polynomial f as in equation (1) can be classified in two types:

Type I: f_1 and f_2 are linearly dependent. In this case, there exists $\alpha \in k$ such that

$$a_i = \alpha a_{i+1} \quad \text{for all} \quad i = 0, \dots, m-1.$$

If $a_m = 0$, then f is a constant polynomial. On the other hand, if $a_m \neq 0$, then

$$f = a_m(\alpha^m + \alpha^{m-1}\sigma_m^1 + \cdots + \sigma_m^m).$$

As a consequence, if f is of Type I, then $f = a_m \prod_{i=1}^{m} (\alpha + x_i)$.

Type II: f_1 and f_2 are linearly independent. It is not hard to verify that in this case f is absolutely irreducible, i.e. f is irreducible in an algebraic closure of k.

Note that, if we identify a nonzero polynomial as in (1) with the point $[a_0 : a_1 : \cdots : a_m]$ in a projective space $\mathbb{P}^m(k)$ of dimension m over the field k, then the polynomials of Type I correspond to (upto multiplication by a nonzero element of k) the k-rational points of the rational normal curve in $\mathbb{P}^m(\bar{k})$. We are now ready to state our first main result of this article.

Theorem 2.1. *Let m be a positive integer and S be a finite subset of k with $|S| \geq m$. If f is a nonzero symmetric polynomial as in* (1)*, then*

$$|Z_{S,D}(f)| \leq m\mathcal{P}(|S|-1, m-1). \tag{4}$$

This bound is attained if and only if f is a nonconstant Type I polynomial given by

$$f = c \prod_{i=1}^{m} (x_i - b)$$

for some $c \in k$ and $b \in S$. Moreover, if f is non-zero and not of the above type, then

$$|Z_{S,D}(f)| \leq m\mathcal{P}(|S|-1, m-1)) - (|S|-m)\mathcal{P}(|S|-2, m-2). \tag{5}$$

Proof. We prove the inequality (4) by induction on $|S|$. Suppose that $|S| = 1$. Then $m = 1$ and the assertion follows trivially. Suppose that the assertion is true for all $T \subset k^m$ where $|T| < |S|$ and $m \leq |T|$. We distinguish two cases:

Case 1: f is of type I. In this case, we may write

$$f = c(x_1 - b)(x_2 - b) \cdots (x_m - b)$$

for some $b \in k$. Note that $(a_1, \cdots, a_m) \in Z_{S,D}(f)$ if and only if $b \in S$ and $a_i = b$ for some i. Consequently,

$$|Z_{S,D}(f)| = \begin{cases} m\mathcal{P}(|S|-1, m-1) & \text{if } b \in S \\ 0 & \text{otherwise.} \end{cases}$$

Case II: f is of type II. Write $f = f_1 + x_m f_2$ as in equation (3). Since f_1 and f_2 are linearly independent, for every $\alpha \in k$, the polynomial $f(x_1, \ldots, x_{m-1}, \alpha)$ is a nonzero symmetric polynomial that is a linear combination of the elemetary symmetric polynomials in $m-1$ variables. are linearly independent elements of $\mathbb{S}_m$. Using induction hypothesis, we obtain,

$$\begin{aligned}
&|Z_{S,D}(f)| \\
&= \sum_{\alpha \in S} |Z_{S\setminus\{\alpha\},D}(f(x_1, \ldots, x_{m-1}, \alpha))| \\
&\leq |S|(m-1)\mathcal{P}(|S|-2, m-2) \\
&= (|S|-1)(m-1)\mathcal{P}(|S|-2, m-2) + (m-1)\mathcal{P}(|S|-2, m-2) \\
&= (m-1)\mathcal{P}(|S|-1, m-1) + (m-1)\mathcal{P}(|S|-2, m-2) \\
&= m\mathcal{P}(|S|-1, m-1) - (\mathcal{P}(|S|-1, m-1) - (m-1)\mathcal{P}(|S|-2, m-2)) \\
&= m\mathcal{P}(|S|-1, m-1) - (|S|-m)\mathcal{P}(|S|-2, m-2)).
\end{aligned}$$

This completes the proof. □

We now apply the result to the particular case when $S = \mathbb{F}_q$ to get the following corollary.

Corollary 2.2. *Let $f \in \mathbb{F}_q[x_1, \ldots, x_m]$ be as in (1). If $m \leq q$ and $f \neq 0$, then $|Z_{\mathbb{F}_q,D}(f)| \leq m\mathcal{P}(q-1, m-1)$. Moreover, the equality holds if and only if f is of Type I.*

Proof. Follows trivially from Theorem 2.1. □

Having known the maximum number of distinguished zeroes of a polynomial as in equation (1), it is important to address the following questions.

Question 2.3. *Given $f \in \mathbb{F}_q[x_1, \ldots, x_m]$ as in (1), what are the possible number of distinguished zeroes in $\mathbb{A}^m(\mathbb{F}_q)$ that f may admit?*

One can readily note that $|Z_{\mathbb{F}_q,D}(f)|$ is always divisible by $m!$. Furthermore, if f is a nonzero constant polynomial, then it has no zeroes. If f is a zero polynomial then it has $\mathcal{P}(q, m)$ distinguished zeroes. Moreover, thanks to Corollary 2.2, if f is nonzero and of Type I, then it has $m\mathcal{P}(q-1, m-1)$ distinguished zeroes. We remark that the above question is equivalent to the question of determination of the weight distribution of the code defined in Section 3. In general, it is a hard question to answer. Here we completely work out the case when $m = 2$ and leave the general question open for further research.

THEOREM 2.4. *Let q be odd, $m = 2$, and $f \in \mathbb{F}_q[x_1, x_2]$ be given by $f = a_0 + a_1(x_1 + x_2) + a_2x_1x_2$. If $\mathcal{D} := a_1^2 - a_0a_2$, then.*

$$|Z_{\mathbb{F}_q,D}(f)| = \begin{cases} 0, & \text{if } a_0 \neq 0 \text{ and } (a_1, a_2) = (0,0) \\ q-3, & \text{if } a_2 \neq 0, \mathcal{D} \in \mathbb{F}_q^2 \text{ and } \mathcal{D} \neq 0 \\ q-1, & \text{if } \{a_2 = 0 \text{ and } a_1 \neq 0\} \text{ or} \\ & \quad \{a_2 \neq 0, \mathcal{D} \notin \mathbb{F}_q^2 \text{ and } \mathcal{D} \neq 0\} \\ 2(q-1), & \text{if } a_2 \neq 0 \text{ and } \mathcal{D} = 0 \\ q(q-1), & \text{if } (a_0, a_1, a_2) = (0,0,0) \end{cases}$$

PROOF. If $f = 0$, then $|Z_{\mathbb{F}_q,D}(f)| = \mathcal{P}(q, 2)$. Conversely, it is clear from Corollary 2.2 that if $|Z_{\mathbb{F}_q,D}(f)| = \mathcal{P}(q, 2)$, then $f = 0$. So we may assume that $f \neq 0$, i.e. $(a_0, a_1, a_2) \neq (0, 0, 0)$. We distinguish the proof into several cases:

Case 1: Suppose $a_2 = 0$. If $a_1 = 0$, then f is a nonzero constant polynomial which does not have any zeroes. So we may assume that $a_1 \neq 0$. Then the polynomial $a_0 + a_1(x_1 + x_2)$ has $q-1$ distinguished zeroes.

Case 2: Suppose $a_2 \neq 0$. We may write

$$\begin{aligned} f(x_1, x_2) &= a_2x_1x_2 + a_1(x_1 + x_2) + a_0 \\ &= a_2\left(x_1x_2 + \frac{a_1}{a_2}(x_1 + x_2) + \frac{a_1^2}{a_2^2}\right) + a_0 - \frac{a_1^2}{a_2} \\ &= a_2\left(x_1 + \frac{a_1}{a_2}\right)\left(x_2 + \frac{a_1}{a_2}\right) + a_0 - \frac{a_1^2}{a_2} \end{aligned}$$

By using the change of coordinates $X_1 = x_1 + a_1/a_2$ and $X_2 = x_2 + a_1/a_2$, and we get a new polynomial

$$f'(X_1, X_2) = X_1X_2 - \frac{a_0a_2 - a_1^2}{a_2^2}.$$

It is clear that there is a one-one correspondence between the set of distinguished zeroes of f and f'. This leads us to analyzing the distinguished zeroes of the polynomial f'. Note that the number of distinguished zeroes of f' depends of the quantity $\mathcal{D}$.

Subcase 1: Suppose $\mathcal{D} = 0$. Then the polynomial $f'(X_1, X_2) = X_1X_2$ has exactly $2(q-1)$ many distinguished zeroes.

Subcase 2: Suppose $\mathcal{D} \neq 0$ and $\mathcal{D}$ is a square in $\mathbb{F}_q$. Note that the polynomial $X_1X_2 - \mathcal{D}/a_2^2$ has $q-1$ zeroes and out of them two are nondistinguished. Consequently, such a polynomial have $q-3$ distinguished zeroes.

Subcase 3: Suppose $\mathcal{D} \neq 0$ and $\mathcal{D}$ is not a square in $\mathbb{F}_q$. In this case, all the zeroes of $X_1X_2 - \mathcal{D}/a_2^2$ are distinguished. As a consequence, the number of distinguished zeroes of such a polynomial is $q-1$.

Number of distinguished zeroes	Number of polynomials
0	$q-1$
$q-3$	$\frac{q(q-1)^2}{2}$
$q-1$	$\frac{q(q-1)(q+1)}{2}$
$2(q-1)$	$q(q-1)$
$q(q-1)$	1

Table 1. Number of polynomials with given number of distinguished zeroes when q is odd

This completes the proof. □

Remark 2.5. It is not very difficult to count the number of polynomials that have $0, q-3, q-1, 2(q-1)$, and $q(q-1)$ distinguished zeroes. It is trivial to see that there are $q-1$ nonzero constant polynomials admitting no zeroes and exactly one polynomial, namely the zero polynomial, admitting $q(q-1)$ distinguished zeroes. In order to count the number of polynomials $a_0 + a_1(x_1 + x_2) + a_2x_1x_2$, or equivalently, the tuples (a_0, a_1, a_2) satisfying the conditions $a_2 \neq 0$ and $\mathcal{D}$ is a nonzero square in $\mathbb{F}_q$, we note that there are $(q-1)/2$ possible values for $\mathcal{D}$, and for each of these choices, the $q(q-1)$ choices of (a_1, a_2) (namely $q-1$ choices for a nonzero value of a_2 and q choices for a_1) determines a_0 uniquely. This results in a total of $q(q-1)^2/2$ many polynomials admitting $q-3$ zeroes. The computation of the other possible number of polynomials with given number of distinguished zeroes are left to the reader. The complete picture is depicted in the Table 1.

We remark that, in the particular case when $q = 3$, then the nonzero constant polynomials as well as the polynomials satisfying the conditions $a_2 \neq 0$ and $\mathcal{D}$ a nonzero square in $\mathbb{F}_q$ admit no distinguished zeroes. We now study the case when q is even. The proof is essentially similar, but the difference lies in the fact that every element of $\mathbb{F}_q$ is a square in $\mathbb{F}_q$. We include the complete proof for the ease of the reader.

Theorem 2.6. *Let $q \geq 4$ be even, $m = 2$, and $f \in \mathbb{F}_q[x_1, x_2]$ be given by $f = a_0 + a_1(x_1 + x_2) + a_2x_1x_2$. If $\mathcal{D} := a_1^2 - a_0a_2$, then.*

$$|Z_{\mathbb{F}_q,D}(f)| = \begin{cases} 0, & \textit{if } \{a_0 \neq 0 \textit{ and } (a_1, a_2) = (0,0)\} \\ & \quad \textit{or } \{a_1 \neq 0 \textit{ and } (a_0, a_2) = (0,0)\} \\ q, & \textit{if } a_0a_1 \neq 0 \textit{ and } a_2 = 0 \\ q-2, & \textit{if } a_2 \neq 0, \textit{ and } \mathcal{D} \neq 0 \\ 2(q-1), & \textit{if } a_2 \neq 0 \textit{ and } \mathcal{D} = 0 \\ q(q-1), & \textit{if } (a_0, a_1, a_2) = (0,0,0) \end{cases}$$

Proof. If $f = 0$, then $|Z_{\mathbb{F}_q,D}(f)| = \mathcal{P}(q,2)$. As in Proposition 2.4, it is clear from Corollary 2.2 that if $|Z_{\mathbb{F}_q,D}(f)| = \mathcal{P}(q,2)$, then $f = 0$. So we may assume that $f \neq 0$, i.e. $(a_0, a_1, a_2) \neq (0,0,0)$. We again distinguish the proof into several cases:

Case 1: Suppose $a_2 = 0$. If $a_1 = 0$, then f is a nonzero constant polynomial which does not have any zeroes. So we may assume that $a_1 \neq 0$.

Number of distinguished zeroes	Number of polynomials
0	$2(q-1)$
q	$(q-1)^2$
$q-2$	$q(q-1)^2$
$2(q-1)$	$q(q-1)$
$q(q-1)$	1

Table 2. Number of polynomials with given number of distinguished zeroes when q is even

Subcase 1: If $a_0 \neq 0$, then all the zeroes of $a_0 + a_1(x_1 + x_2)$ are distinguished. Consequently, $|Z_{\mathbb{F}_q,D}(f)| = q$.

Subcase 2: Then the zeroes of the polynomial $a_1(x_1 + x_2)$ are not distinguished. Thus $|Z_{\mathbb{F}_q,D}(f)| = 0$.

Case 2: Suppose $a_2 \neq 0$. As in Proposition 2.4, after a suitable change of coordinates, we get a polynomial

$$f'(X_1, X_2) = X_1X_2 - \frac{a_0a_2 - a_1^2}{a_2^2},$$

with $|Z_{\mathbb{F}_q,D}(f)| = |Z_{\mathbb{F}_q,D}(f')|$.

Subcase 1: Suppose $\mathcal{D} = 0$. Then the polynomial X_1X_2 has exactly $2(q-1)$ many distnguished zeroes.

Subcase 2: Suppose $\mathcal{D} \neq 0$. Since q is even, D is a square in $\mathbb{F}_q$. Note that the polynomial $X_1X_2 - \mathcal{D}/a_2^2$ has $q-1$ zeroes and out of them only one is nondistinguished. Consequently, such a polynomial have $q-2$ distinguished zeroes.

This completes the proof. □

Again, it is not very difficult to compute the number of polynomials that admits a given number of distinguished zeroes in the case when q is even. We leave the explicit computations to the readers, but present the data in Table 2.

3. Reed-Muller type codes from symmetric polynomials

Throughout this section, we will denote by $\mathbb{F}_q$ a finite field with q elements where q is a power of a prime number. As in Section 2, we denote by Σ_m the vector space consisting of all symmetric polynomials as in (1). As noted before, Σ_m is a vector space of dimension $m+1$ over $\mathbb{F}_q$. Let $n = \mathcal{P}(q, m)$.

Definition 3.1. We fix an ordering $\{P_1, \dots, P_n\}$ of elements in $\mathbb{A}^m_D$. Define an evaluation map

$$\mathrm{ev} : \Sigma_m \to \mathbb{F}_q^n, \quad \text{given by} \quad f \mapsto (f(P_1), \dots, f(P_n)).$$

It is readily seen that ev is a linear map and consequently the image, $\mathcal{C}_m$ of ev is a code.

We discuss some properties of this code in the following proposition:

Proposition 3.2. *If $m < q$, then the code $\mathcal{C}_m$ is a nondegenerate $[n, k, d]$ code, where $n = \mathcal{P}(q, m)$, $k = m + 1$ and $d = (q - m)\mathcal{P}(q - 1, m - 1)$. Furthermore, the code $\mathcal{C}(d, m)$ is generated by minimum weight codewords.*

Proof. The statement on the length of the code is trivial, while the fact that the code is nondegenerate follows readily by observing that $\mathrm{ev}(1) = (1, \dots, 1) \in C_m$. To show that C_m is of dimension $m+1$, it is enough to show that the map ev is injective. To this end, let $f \in \Sigma_m$ with $\mathrm{ev}(f) = (0, \dots, 0)$. Then $|Z_{\mathbb{F}_q,D}(f)| = \mathcal{P}(q, m)$. But from Corollary 2.2, we see that, if $f \neq 0$, then $|Z_{\mathbb{F}_q,D}(f)| \leq m\mathcal{P}(q-1, m-1)$. Since $m < q$, we have $m\mathcal{P}(q-1, m-1) < \mathcal{P}(q, m)$. This implies $f = 0$. Consequently, the map ev is injective. The assertion on the minimum distance follows from Corollary 2.2. Moreover, it is clear from the last assertion of Corollary 2.2 that the minimum weight codewords of $\mathcal{C}_m$ are given by $\mathrm{ev}(f)$ where f is a Type I polynomial. Thus, to show that $\mathcal{C}_m$ is generated by minimum weight codewords, it is now enough to prove that Σ_m is spanned by a set of $m + 1$ Type I polynomials. Since $m + 1 \leq q$, we may choose $\alpha_1, \dots, \alpha_{m+1} \in \mathbb{F}_q$ that are distinct. For each $i = 1, \dots, m + 1$, we define

$$f_i = (x_1 + \alpha_i) \cdots (x_m + \alpha_i).$$

Since $\alpha_1, \dots, \alpha_{m+1}$ are distinct, it follows from the Vandermonde determinant formula that $f_1, \dots, f_{m+1}$ are linearly independent. Since $\dim_{\mathbb{F}_q} \Sigma_m = m + 1$, they span the vector space Σ_m. This completes the proof. □

Remark 3.3. We note that the relative minimum distance of $\mathcal{C}_m$ is the same as that of the generalized Reed-Muller codes of order m.

The code $\mathcal{C}_m$ is made by evaluating each of the functions in Σ_m at the points of $\mathbb{A}^m_D$. But the points of $\mathbb{A}^m_D$ constitute a disjoint union of S_m-orbits, each of cardinality $m!$, where the symmetric group S_m in m letters acts freely by permuting the coordinates. This motivates us in defining a code of smaller length, namely, by constructing a smaller evaluation set, say R_D, consisting of one point from each of the S_m orbits mentioned above. Again we fix an ordering of the elements in the set R_D, say $Q_1, \dots, Q_N$, where $N = \binom{q}{m}$.

We now consider the restriction of the evaluation map, still denoted by ev:

$$\mathrm{ev} : \Sigma_m \to \mathbb{F}_q^N \quad \text{given by} \quad f \mapsto (f(Q_1), \dots, f(Q_N)).$$

Let $\mathcal{C}'_m$ denote the image of R_D under the map ev. The following proposition follows readily from Proposition 3.2.

Proposition 3.4. *If $m < q$, then $\mathcal{C}'_m$ is a nondegenerate $[N, K, D]$ linear code where $N = \binom{q}{m}$, $K = m + 1$ and $D = \binom{q}{m} - \binom{q-1}{m-1}$.*

Proof. The assertions on length and dimension is readily obtained as in the case with Proposition 3.2. The assertion on minimum distance is deduced from Corollary 2.2 and the fact that the weight of any codeword $\mathrm{ev}(f) \in \mathcal{C}'_m$ is given by $\binom{q}{m} - \frac{1}{m!}|Z_{\mathbb{F}_q,D}(f)|$. □

4. Generalized Hamming weights

Ever since their introduction by V. Wei in [**10**], the computation of generalized Hamming weights of several codes have been in the center of interest of many mathematicians and coding theorists. The study of generalized Hamming weights of several evaluation codes has paved the way for a lot of research articles such as [**1, 5, 6**] among others.

In this section, we derive some natural upper bounds on the generalized Hamming weights of the codes $\mathcal{C}_m$ and $\mathcal{C}'_m$. At the outset, we remark that it is enough to derive any parameters related to the Hamming weight of codewords for one of the codes. Since, the codes $\mathcal{C}_m$ are somewhat more natural to work with, we choose to restrict our attention to them.

Proposition 4.1. *Fix positive integers $1 \le r \le m+1 \le q$ and denote by d_r the r-th generalized Hamming weight of $\mathcal{C}_m$. We have*

$$d_r \le \mathcal{P}(q,m) - m!\binom{q-r}{m-r}.$$

Proof. Since $1 \le r \le q$, there exist distinct elements $b_1, \dots, b_r \in \mathbb{F}_q$. For $i = 1, \dots, r$, we consider the polynomials

$$f_i := (x_1 - b_i) \cdots (x_m - b_i).$$

Note that $f_1, \dots, f_r$ are linearly independent and as a consequence $\mathrm{ev}(f_1), \dots, \mathrm{ev}(f_r)$ span an r dimensional subspace, say E_r of $\mathcal{C}_m$. It follows that

$$d_r \le |\operatorname{Supp}(E_r)| = \mathcal{P}(q,m) - |Z_{S,D}(f_1, \dots, f_r)|,$$

where, as usual, for any subspace $V \subset \mathbb{F}_q^n$,

$$\operatorname{Supp}(V) = \{i \mid \exists (a_1, \dots, a_n) \in V, a_i \neq 0\}.$$

Now, an element $(a_1, \dots, a_m) \in Z_{S,D}(f_1, \dots, f_r)$ if and only if for each $i = 1, \dots, r$, there exists $j_i \in \{1, \dots, m\}$ such that $a_{j_i} = b_i$. A simple counting argument now completes the proof. □

Remark 4.2. We note that the determination of the r-th generalized Hamming weight of $\mathcal{C}_m$ (resp. $\mathcal{C}'_m$) is equivalent to computing the maximum number of common zeroes of r linearly independent elements of Σ_m in $\mathcal{A}_D^m(\mathbb{F}_q)$ (resp. R_D). It follows trivially that $d_r(\mathcal{C}_m) = m! d_r(\mathcal{C}'_m)$. The following corollary is now immediate:

Corollary 4.3. $d_r(\mathcal{C}'_m) \le \binom{q}{m} - \binom{q-r}{m-r}$.

The following proposition shows that the bounds obtained in Proposition 4.1 is exact for the largest two values of r.

Proposition 4.4. *We have*

(a) $d_{m+1}(\mathcal{C}_m) = m! d_{m+1}(\mathcal{C}'_m) = m!\binom{q}{m}$.
(b) $d_m(\mathcal{C}_m) = m! d_m(\mathcal{C}'_m) = m!\left(\binom{q}{m} - 1\right)$.

Proof. Part (a) follows trivially since $(1, \dots, 1) \in \mathcal{C}_m$ and hence $\mathcal{C}_m$ is a nondegenerate code. We prove the part (b) for the code $\mathcal{C}'_m$.

A generator matrix for $\mathcal{C}'_m$ is a parity check matrix for its dual code. Such a matrix $M = (m_{i,j})$ can be formed by setting $m_{i,j} =$ the value of σ_{i-1} at point number j in $\mathbb{R}_{\mathbb{F}_q}$, for some fixed order of the points in $\mathbb{R}_{\mathbb{F}_q}$. Another way to put it is that $m_{i,j} =$ the value of σ_{i-1} at a chosen point in orbit number j of S_m in $\mathbb{A}_D(\mathbb{F}_q)^m$, for some fixed order of the orbits in $\mathbb{A}_D(\mathbb{F}_q)^m$. Any two columns of this matrix are equal if and only if they are equal up to a non-zero, multiplicative constant. This is because their first entries are both $1(=\sigma_0)$. The last observation immediately shows that no column of M is zero. Moreover any two columns are different. This is because the elementary, symmetric functions $\sigma_1, \cdots, \sigma_m$ separate orbits of S_m on $\mathbb{A}_D(\mathbb{F}_q)^m$. (If

$$X^m - \sigma_1 X^{m-1} + \cdots + (-1)^m \sigma_m = (X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_m),$$

then the α_i are unique up to order, since $\mathbb{F}_q[X]$ is a UFD). Hence no two two columns are parallel vectors either (i.e. no two columns are equivalent up to a non-zero multiplicative constant). Hence the minimum distance of the dual code of $\mathcal{C}'$ is at least 3. By Wei duality

$$d_m(\mathcal{C}') = \text{ length } (\mathcal{C}') - 1 = \binom{q}{m} - 1.$$

This completes the proof. □

Propositions 3.4 and 4.4 give all 3 generalized Hamming weights d_r for $\mathcal{C}'_m$ and $\mathcal{C}_m$ for the case $m = 2$. If $m = q - 1$, then $\mathcal{C}'_m$ fills the whole ambient space $\mathbb{F}_q^q$, and everything is trivial. It is a challenge, though, to give good results in the intermediate cases $3 \leq m \leq m - 2$.

5. The case $m = 2$.

As it is clear from the work done in previous sections, we are interested in computing the basic parameters such as length, dimension, minimum distance, generalized Hamming weights and the weight distributions for the codes $\mathcal{C}_m$ and $\mathcal{C}'_m$. In this section, we completely determine these parameters for the codes when $m = 2$. To begin with, we derive from Proposition 3.2 that $\mathcal{C}_m$ is an $[n, k, d]$ code, where

$$n = q(q-1), \quad k = 3, \quad \text{and} \quad d = (q-1)(q-2).$$

Furthermore, it follows from Propositions 3.4 and 4.4 that

$$(d_1, d_2, d_3) = ((q-1)(q-2), q(q-1) - 2, q(q-1)),$$

where d_1, d_2, d_3 denote the first, second and third generalized Hamming weights for the code $\mathcal{C}_2$. We now proceed to determine the weight distribution for the code $\mathcal{C}_2$. To this end we introduce the following notation:

Definition 5.1. Let w and r be integers satisfying $0 \leq w \leq q(q-1)$ and $1 \leq r \leq 3$. Define

(a) $A_w :=$ the number of codewords of $\mathcal{C}_2$ of Hamming weight w.

(b) $A_w^{(r)} :=$ the number of r-dimensional subcodes of $\mathcal{C}_2$ of support weight w.

Let $c \in \mathcal{C}_2$ be a codeword. Then $c = \mathrm{ev}(f)$ for some $f \in \Sigma_2$. It follows that c is a codeword of Hamming weight w if and only if $|Z_{\mathbb{F}_q,D}(f)| = q(q-1) - w$. One can now readily compute the values of A_w from Tables 1 and 2 for all values of w. We have the following results:

Proposition 5.2. *If q is odd, and $q \geq 5$, then we have*

$$A_w = \begin{cases} 1, & \text{if } w = 0 \\ q(q-1), & \text{if } w = (q-1)(q-2) \\ \frac{q(q-1)(q+1)}{2}, & \text{if } w = q(q-1) - (q-1) \\ \frac{q(q-1)^2}{2}, & \text{if } w = q(q-1) - (q-3) \\ (q-1), & \text{if } w = q(q-1) \\ 0, & \text{otherwise.} \end{cases}$$

We remark that for $q = 3$, we have $A_0 = 1, A_2 = 6,\ A_4 = 12$ and $A_6 = 8$.

Proposition 5.3. *If q is even, and $q \geq 4$, then we have*

$$A_w = \begin{cases} 1, & \text{if } w = 0 \\ q(q-1), & \text{if } w = (q-1)(q-2) \\ q(q-1)^2, & \text{if } w = q(q-1) - (q-2) \\ (q-1)^2, & \text{if } w = q(q-1) - 1 \\ 2(q-1), & \text{if } w = q(q-1) \\ 0, & \text{otherwise.} \end{cases}$$

We now turn our attention towards computing $A_w^{(i)}$-s for all values of $1 \leq w \leq q(q-1)$ and $i = 1, 2, 3$ for the code $\mathcal{C}_2$. To this end, we have the following result:

Proposition 5.4. *For $1 \leq w \leq q(q-1)$ and $i = 1, 2, 3$ we have*

$$A_w^{(i)} = \begin{cases} \frac{A_w}{q-1}, & \text{if } \quad i = 1 \\ \frac{q(q-1)}{2}, & \text{if } \quad w = q(q-1) - 2 \text{ and } i = 2 \\ \frac{q^2+3q+2}{2}, & \text{if } \quad w = q(q-1) \text{ and } i = 2 \\ 1, & \text{if } \quad w = q(q-1) \text{ and } i = 3, \\ 0, & \text{otherwise.} \end{cases}$$

Proof. The assertions concerning the cases when $i = 1$ and $i = 3$ are clear. To prove the claims concerning the cases when $i = 2$, we must analyze the possible number of distinguished points on the intersection of two curves given by $f_1, f_2 \in \Sigma_2$ such that f_1 and f_2 are linearly independent. Suppose that

$$f_1(x, y) = a_0 + a_1(x + y) + a_2xy \quad \text{and} \quad f_2(x, y) = b_0 + b_1(x + y) + b_2xy.$$

We claim that f_1 and f_2 have no common factors. To see this, first note that, f_1 is not a nonzero constant multiple of f_2 since they are linearly independent. However, if f_1 has a factor of degree one, then $f_1 = c(x - a)(y - a)$ for some $a, c \in \mathbb{F}_q$. The fact that f_1 and f_2 have a common factor, now readily implies that $f_2 = d(x - a)(y - a)$ for some $d \in \mathbb{F}_q$. This is a contradiction. Now the projective closures of the zero sets $V(f_1)$ and $V(f_2)$ are given by homogeneous polynomials F_1 and F_2 of degree 2, namely

$$F_1 = a_0z^2 + a_1(x + y)z + a_2xy \quad \text{and} \quad F_2 = b_0z^2 + b_1(x + y)z + b_2xy.$$

By Bezout's theorem, the projective curves given by F_1 and F_2 intersect at exactly 4 points over the algebraic closure, counting multiplicities. We also observe that they have two points on the line $z = 0$ in common, namely $[0 : 1 : 0]$ and $[1 : 0 : 0]$. Hence they have at most 2 points in common in the affine space $\mathbb{A}^2(\mathbb{F}_q)$. To this end, we observe that if $V(f_1)$ and $V(f_2)$ have points in common in $\mathbb{A}^2_D(\mathbb{F}_q)$, then by symmetry, the points will be of the form (α, β) and (β, α) for some $\alpha, \beta \in \mathbb{F}_q$ with $\alpha \neq \beta$. Thus the affine curves $V(f_1)$ and $V(f_2)$ either do not intersect in $\mathbb{A}^2_D(\mathbb{F}_q)$ or they intersect in exactly 2 points. It is thus evident that $A^{(2)}_w = 0$ for all values of w other that $q(q-1)$ and $q(q-1)-2$. We now compute $A^{(2)}_w$ for $w = q(q-1)$ and $w = q(q-1)-2$. It is enough to compute the same for $w = q(q-1)-2$. The elements of Σ_2 that contain the above points form a 2 dimensional linear system of curves, which in turn gives us a two dimensional subcode that has weight $q(q-1)-2$. On the other hand, there are $q(q-1)/2$ ways of choosing two such points from $\mathbb{A}^2(\mathbb{F}_q)$. This shows that $A^{(2)}_{q(q-1)-2} = q(q-1)/2$. Since there are a total of q^2+q+1 number of 2 dimensional subcodes of $\mathcal{C}_2$, the assertion on $A^{(2)}_{q(q-1)}$ follows trivially. □

Let $(\mathcal{C}_2)^{(s)} = \mathcal{C}_2 \otimes_{\mathbb{F}_q} \mathbb{F}_{q^s}$ for $s \geqslant 1$. It is a linear code over $\mathbb{F}_Q$, for $Q = q^s$, with the same generator matrix as $\mathcal{C}_2$ itself. In [**7**], one gives a relation between the higher weight spectra of a linear code and the usual weight spectrum (only counting individual words of each weight), for such an extension code over larger, finite fields. Denote the number of codewords of weight w for $(\mathcal{C}_2)^{(s)}$ by $P_w(Q)$. Then:

$$P_w(Q) = \sum_{r=0}^{k} A^{(r)}_w \prod_{i=0}^{r-1}(q^s - q^i) = \sum_{r=0}^{k} A^{(r)}_w \prod_{i=0}^{r-1}(Q - q^i).$$

This gives:

Corollary 5.5. *For $(\mathcal{C}_2)^{(s)}$ we have, if $q \geq 7$ is odd :*

$$P_0(Q) = 1,\ P_{n-2(q-1)}(Q) = q(Q-1),\ P_{n-(q-1)}(Q) = \frac{q^2+q}{2}(Q-1),$$

$$P_{n-(q-3)}(Q) = \frac{q^2-q}{2}(Q-1),\ P_{n-2}(Q) = \frac{q^2-q}{2}(Q-1)(Q-q),$$

$$P_n(Q) = (Q-1)(Q^2 + \frac{-q^2+q+2}{2}Q + \frac{q^3-3q^2-2q+2}{2}).$$

We leave it to the reader to find analogous formulas for $q = 3, 5$, and for even $q \geq 4$.

6. The cases $m \geq 3$.

If $m = 3$, the only unknown generalized Hamming weight of $\mathcal{C}_m = \mathcal{C}_3$ is d_2, since we know that $d_1 = 6\binom{q}{3} - 6\binom{q-1}{2}, d_3 = 6\binom{q}{3} - 6,$ and $d_4 = 6\binom{q}{3}$, by the results above. Furthermore we know from Proposition 2.1, as for general m, that there are precisely $q(q-1)$ codewords of minimal weight, namely $\tau(c(x_1 - b)\cdots(x_m - b))$, for q choices of b, and $q-1$ choices of non-zero c.

The case $q = 4$ is a special case of the trivial case $m = q - 1$ mentioned at the end of Section 4, with $d_r(\mathcal{C}_3) = 6r$ for all r.

In order to illustrate the complexity, we give our only example below, of a more non-trivial result for $m = 3$. We leave it to further research to find good results for $m \geq 3$ in general.

Example 6.1. If $q = 5$, one can show that $d_2(\mathcal{C}_3) = 42$ (and hence $(d_1, d_2, d_3, d_4) = (24, 42, 54, 60)$). One may prove the equivalent statement $d_2(\mathcal{C}'_3) = \frac{42}{m!} = \frac{42}{6} = 7$ as follows: A generator matrix $M = (m_{i,j})$ of $\mathcal{C}_3$, as described above, with $m_{i,j} = \sigma_{i-1}(P_j)$ becomes

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 3 & 4 & 0 & 0 & 1 & 2 & 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 & 3 & 2 & 1 & 4 & 4 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 3 & 2 & 4 \end{bmatrix}$$

when the $P_j = \{a_j, b_j, c_j\} \subset \{0, 1, 2, 3, 4\}$ are ordered lexicographically with respect to the ordering of $\mathbb{F}_5$. The columns of M may be interpreted as points of projective 3-space $Proj(\mathbb{F}_5[y_0, y_1, y_2, y_3]) = \mathbb{P}^3$ over $\mathbb{F}_5$, and one sees that $d(\mathcal{C}_3) = 10-$ the maximal number of points from $P_1, \cdots, P_{10}$ that are contained in a (projective) plane $(= 10 - 6 = 4)$, $d_2(\mathbb{C}_3) = 10-$ the maximal number of points from $P_1, \cdots, P_{10}$ that are contained in a line, $d_2(\mathbb{C}_3) = 10-$ the maximal number of points from $P_1, \cdots, P_{10}$ that are contained in a point $(= 10 - 1 = 9)$. There are $q^3 + q^2 + q + 1 = 156$ planes in $\mathbb{P}^3$, and among them we have the 5 (call them $W_0 = 0, \cdots, W_4 = 0$) that correspond to (totally) reducible elements of Σ_5, and that contain $\binom{q-1}{m-1} = 6$ of the 10 points. We see directly from the matrix description that $W_0 = y_3 = 0$ is one of them (corresponding to totally reducible elements $c(x_1 - 0)(x_2 - 0)(x_3 - 0)$, for arbitrary non-zero c. A computer analysis, or a by-hand calculation, shows that there is no plane (corresponding to irreducible elements of Σ_m that contain exactly 5 (column) points (of M), although the last part of Proposition 2.1, which is obviously not sharp in this case, allows it. Moreover there are exactly $\binom{5}{2} = 10$ planes that contain exactly 4 of 10 of the points (For each unordered pair W_i, W_j, with $i \neq j$, there is exactly one such plane $V_{i,j} = 0$ of type $= W_i + gW_j = 0$, with $g \neq 0$).

This also proves that no more than 3 of the (column) points (of M) are on a line. First, two planes $W_i = 0$ and $W_j = 0$, with $i \neq j$, are well known to intersect in exactly 3 points, by the proof of Proposition 4.1.

If two distinct planes of type $V_{i,j} = 0$ contained the same 4 points, add any point outside L, which is the intersection of those two planes. Then those 5 points would span a plane. This plane would have to be one of the $W_i = 0$, since no other planes contains at least 5 points, as we have seen. But a plane of type $W_i = 0$ does not contain 4 points on a line, so that is impossible.

The assertion that a plane of type $W_i = 0$ does not contain 4 points on a line, follows from symmetry, and showing that this is true for $W_0 = y_3 = 0$. One shows this for $W_0 = y_3 = 0$ by direct inspection of the 15 choices of 4 of the 6 leftmost columns of M, or by arguing that if you remove the zeroes in the bottom row from these columns, then these 6 columns are among the $10 = \binom{5}{2}$ columns of the analogous matric M for the case $q = 5$ and $m = 2$. Since $d(\mathcal{C}_2) = 6 - 3 = 3$, at most 3 of these points are on a line.

If a plane of type $V_{i,j} = 0$ and a plane of type $W_k = 0$ contained 4 common points (in their intersection, a line L), we again have four points in a plane of type $W_i = 0$, a contradiction.

Hence the maximal number of column points of M on a line is 3, and $d_2(\mathcal{C}_3) = \binom{q}{3} - \binom{q-2}{3-2} = 10 - 3 = 7$, for $q = 5$. As a byproduct of this analysis we observe that in addition to $q(q-1) = 20$ words of minimal weight 4 there are exactly $(q-1)\binom{q}{2} = 40$ codewords of "subminimal" weight, in this case 6, in $\mathcal{C}_3$ for $q = 5$.

References

[1] P. Beelen and M. Datta, *Generalized Hamming weights of affine Cartesian codes*, Finite Fields Appl. 51 (2018), pp. 130–145.

[2] P. Beelen, M.Datta and M. Homma *A proof of Sørensen's conjecture on Hermitian surfaces*, Proc. Amer. Math. Soc. 149 (2021), pp. 1431-1441

[3] P. Beelen, P. Singh *Linear codes associated to skew-symmetric determinantal varieties*, Finite Fields and Their Applications 58, July 2019, pp. 32-45.

[4] V. D. Goppa *Geometry and Codes*, ISBN: 978-94-015-6870-8, Springer Verlag, 1988.

[5] S. R. Ghorpade and G. Lachaud, *Higher weights of Grassmann codes*, in Coding theory, cryptography and related areas (Guanajuato, 1998), pp. 122–131, Springer, Berlin, 2000.

[6] P. Heijnen and R. Pellikaan, *Generalized Hamming weights of q-ary Reed-Muller codes*, IEEE Trans. Inform. Theory 44 (1998), no. 1, pp. 181–196.

[7] R. Jurrius, *Weight enumeration of codes from finite spaces*, Des. Codes Cryptogr. 63, pp. 321-330, 2012.

[8] D. Nogin, *The minimum weight of the Grassmann codes $C(k, n)$*, Discr. Appl. Math. 28 (1990), pp. 149–156

[9] E. Weiss, *Generalized Reed-Muller Codes*, Information and Control 5, (1962) pp.213-222

[10] V. Wei, Generalized Hamming weights for linear codes, *IEEE Trans. Inform. Theory* 37 (1991), no. 5, pp. 1412 - 1418.

Department of Mathematics Indian Institute of Technology Hyderabad

Email address: mrinmoy.datta@math.iith.ac.in

Department of Mathematics and Statistics, UiT-The Arctic University of Norway N-9037 Tromsø, Norway

Email address: trygve.johnsen@uit.no