DOI: 10.2478/auom-2020-0014
An. Şt. Univ. Ovidius Constanţa **Vol. 28(1),2020, 205–217**

On the generalized Hamming weights of certain Reed–Muller-type codes

Manuel González-Sarabia, Delio Jaramillo, and Rafael H. Villarreal

Abstract

There is a nice combinatorial formula of P. Beelen and M. Datta for the r-th generalized Hamming weight of an affine cartesian code. Using this combinatorial formula we give an easy to evaluate formula to compute the r-th generalized Hamming weight for a family of affine cartesian codes. If $\mathbb{X}$ is a set of projective points over a finite field we determine the basic parameters and the generalized Hamming weights of the Veronese type codes on $\mathbb{X}$ and their dual codes in terms of the basic parameters and the generalized Hamming weights of the corresponding projective Reed–Muller-type codes on $\mathbb{X}$ and their dual codes.

1 Introduction

Let $K = \mathbb{F}_q$ be a finite field and let C be an $[m, \kappa]$-*linear code* of *length* m and *dimension* κ, that is, C is a linear subspace of K^m with $\kappa = \dim_K(C)$. The multiplicative group of K is denoted by K^*. The *dual code* of C is given by

$$C^{\perp} := \{b \in K^m \colon \langle b, c\rangle = 0 \ \forall\ c \in C\},$$

where $b = (b_1, \ldots, b_m)$, $c = (c_1, \ldots, c_m)$, and $\langle b, c\rangle = \sum_{i=1}^{m} b_i c_i$ is the inner product of a and b.

Key Words: Reed-Muller-type codes, generalized Hamming weights, linear code, Veronese code.
2010 Mathematics Subject Classification: Primary 13P25; Secondary 94B27.
Received: 29.05.2019.
Accepted: 15.07.2019.

Fix an integer $1 \leq r \leq \kappa$. Given a subcode D of C (that is, D is a linear subspace of C), the *support* $\chi(D)$ of D is the set of non-zero positions of D, that is,

$$\chi(D) := \{i \mid \exists\, (a_1, \ldots, a_m) \in D,\ a_i \neq 0\}.$$

The r-th *generalized Hamming weight* of C, denoted $\delta_r(C)$, is the size of the smallest support of an r-dimensional subcode [14, 16, 29]. Generalized Hamming weights have been extensively studied; see [2, 4, 9, 13, 15, 21, 25, 27, 30, 31] and the references therein. The study of these weights is related to trellis coding, t–resilient functions, and was motivated by some applications from cryptography [29]. If $r = 1$, $\delta_1(C)$ is the *minimum distance* of C and is denoted $\delta(C)$.

In this note we give explicit formulas for the generalized Hamming weights of certain projective Reed-Muller-type codes and study the basic parameters (length, dimension, minimum distance) and the generalized Hamming weights of Veronese type codes and their dual codes.

These linear codes are constructed as follows. Let $\mathbb{P}^{s-1}$ be a projective space over K, let $\mathbb{X} = \{[P_1], \ldots, [P_m]\}$ be a subset of $\mathbb{P}^{s-1}$ where $m = |\mathbb{X}|$ is the cardinality of the set $\mathbb{X}$, $P_i \in K^s$ for all i, and let $S = K[t_1, \ldots, t_s] = \oplus_{d=0}^{\infty} S_d$ be a polynomial ring with the standard grading, where S_d is the K-vector space generated by the homogeneous polynomials in S of degree d. Fix a degree $d \geq 1$. For each i there is $h_i \in S_d$ such that $h_i(P_i) \neq 0$. Indeed suppose $P_i = (a_1, \ldots, a_s)$, there is at least one $k \in \{1, \ldots, s\}$ such that $a_k \neq 0$. Setting $h_i = t_k^d$ one has that $h_i \in S_d$ and $h_i(P_i) \neq 0$. Consider the evaluation map

$$\mathrm{ev}_d : S_d \longrightarrow K^m, \quad h \mapsto \left(\frac{h(P_1)}{h_1(P_1)}, \ldots, \frac{h(P_m)}{h_m(P_m)}\right).$$

This is a linear map between the K-vector spaces S_d and K^m. The *Reed–Muller–type-code* of order d associated to $\mathbb{X}$ [5, 11], denoted $C_{\mathbb{X}}(d)$, is the image of ev_d, that is

$$C_{\mathbb{X}}(d) = \left\{\left(\frac{h(P_1)}{h_1(P_1)}, \ldots, \frac{h(P_m)}{h_m(P_m)}\right) : h \in S_d\right\}.$$

The r-th generalized Hamming weight $\delta_r(C_{\mathbb{X}}(d))$ of $C_{\mathbb{X}}(d)$ is sometimes denoted by $\delta_{\mathbb{X}}(d, r)$. If $r = 1$, $\delta_{\mathbb{X}}(d, r)$ is the minimum distance of $C_{\mathbb{X}}(d)$ and is denoted by $\delta_{\mathbb{X}}(d)$. The map ev_d is independent of the set of representatives $P_1, \ldots, P_m$ that we choose for the points of $\mathbb{X}$, and the basic parameters of $C_{\mathbb{X}}(d)$ are independent of $h_1, \ldots, h_m$ [19, Lemma 2.13] and so are the generalized Hamming weights of $C_{\mathbb{X}}(d)$ [8, Remark 1].

The basic parameters of $C_{\mathbb{X}}(d)$ are related to the algebraic invariants of the quotient ring $S/I(\mathbb{X})$, where $I(\mathbb{X})$ is the vanishing ideal of $\mathbb{X}$ (see for example

[10, 20, 22]). Indeed, the dimension of $C_{\mathbb{X}}(d)$ is given by the Hilbert function $H_{\mathbb{X}}$ of $S/I(\mathbb{X})$, that is,

$$H_{\mathbb{X}}(d) := \dim_K(S_d/I(\mathbb{X})_d) = \dim_K(C_{\mathbb{X}}(d)),$$

the length $m = |\mathbb{X}|$ of $C_{\mathbb{X}}(d)$ is the degree or the multiplicity of $S/I(\mathbb{X})$. Moreover, the regularity index of $H_{\mathbb{X}}$ is the regularity of $S/I(\mathbb{X})$ [28, pp. 226, 346] and is denoted $\operatorname{reg}(S/I(\mathbb{X}))$. By the Singleton bound [27] one has $\delta_{\mathbb{X}}(d) = 1$ for $d \geq \operatorname{reg}(S/I(\mathbb{X}))$. Recall that the a-invariant of $S/I(\mathbb{X})$, denoted $a_{\mathbb{X}}$, is the regularity index minus 1.

Let $A_1, \ldots, A_{s-1}$ be subsets of $K = \mathbb{F}_q$ and let $\mathbb{X} := [A_1 \times \cdots \times A_{s-1} \times \{1\}] \subset \mathbb{P}^{s-1}$ be a projective cartesian set, where $d_i = |A_i|$ for all $i = 1, \ldots, s-1$ and $2 \leq d_1 \leq \cdots \leq d_{s-1}$. The Reed–Muller-type code $C_{\mathbb{X}}(d)$ is called an *affine cartesian code* [17].

There is a recent expression for the r-th generalized Hamming weight of an affine cartesian code [1, Theorem 5.4], which depends on the r-th monomial in ascending lexicographic order of a certain family of monomials (see [1] and the proof of Theorem 2.1). Using this result in Section 2 we give an easy to evaluate formula to compute the r-th generalized Hamming weight for a family of affine cartesian codes (Theorem 2.1). Other formulas for the second generalized Hamming weight of an affine cartesian code are given in [7, Theorems 9.3 and 9.5].

Let $k \geq 1$ be an integer and let $M_1, \ldots, M_N$ be the set of all monomials in S of degree k, where $N = \binom{k+s-1}{s-1}$. The map

$$\rho_k \colon \mathbb{P}^{s-1} \to \mathbb{P}^{N-1}, \quad [x] \mapsto [(M_1(x), \ldots, M_N(x))],$$

is called the k-th *Veronese embedding*. Given $\mathbb{X} \subset \mathbb{P}^{s-1}$, the k-th *Veronese type code* of degree d is $C_{\rho_k(\mathbb{X})}(d)$, the Reed–Muller-type code of degree d on $\rho_k(\mathbb{X})$.

In Section 3 we are able to show that the Reed–Muller-type code $C_{\mathbb{X}}(kd)$ over the set $\mathbb{X}$ has the same basic parameters and the same generalized Hamming weights as the Veronese type code $C_{\rho_k(\mathbb{X})}(d)$ over the set $\mathbb{X}$ for $k \geq 1$ and $d \geq 1$ (Theorem 3.2). As a consequence making $\mathbb{X} = \mathbb{P}^{s-1}$ we recover a result of Rentería and Tapia-Recillas [23, Proposition 1]. Also we show that the dual codes of $C_{\mathbb{X}}(kd)$ and $C_{\rho_k(\mathbb{X})}(d)$ are equivalent (Theorem 3.5).

For all unexplained terminology and additional information we refer to [3, 28] (for the theory of Gröbner bases), and [18, 27] (for the theory of error-correcting codes and linear codes).

2 Generalized Hamming weights of some affine cartesian codes

In this section we present our main result on Hamming weights of certain cartesian codes. To avoid repetitions, we continue to employ the notations and definitions used in Section 1.

Let $\prec$ be a monomial order on S and let $(0) \neq I \subset S$ be an ideal. If f is a non-zero polynomial in S, the *leading monomial* of f is denoted by $\mathrm{in}_\prec(f)$. The *initial ideal* of I, denoted by $\mathrm{in}_\prec(I)$, is the monomial ideal given by

$$\mathrm{in}_\prec(I) = (\{\mathrm{in}_\prec(f) |\, f \in I\}).$$

A monomial t^a is called a *standard monomial* of S/I, with respect to $\prec$, if t^a is not in the ideal $\mathrm{in}_\prec(I)$. The set of standard monomials, denoted $\Delta_\prec(I)$, is called the *footprint* of S/I. The footprint of S/I is also called the *Gröbner éscalier* of I. The image of the standard polynomials of degree d, under the canonical map $S \mapsto S/I$, $x \mapsto \overline{x}$, is equal to S_d/I_d, and the image of $\Delta_\prec(I)$ is a basis of S/I as a K-vector space. This is a classical result of Macaulay [3, Chapter 5].

We come to our main result.

Theorem 2.1. *Let $\mathbb{X} := [A_1 \times \cdots \times A_{s-1} \times \{1\}]$ be a subset of $\mathbb{P}^{s-1}$, where $A_i \subset \mathbb{F}_q$ and $d_i = |A_i|$ for $i = 1, \ldots, s-1$. If $2 \leq d_1 \leq \cdots \leq d_{s-1}$ and $d \geq 1$, then*

$$\delta_r(C_\mathbb{X}(d)) = \begin{cases} d_{k+r+1} \cdots d_{s-1}[(d_{k+1} - \ell + 1)d_{k+2} \cdots d_{k+r} - 1] & \text{if} \quad 1 \leq r < s-k-1, \\ (d_{k+1} - \ell + 1)d_{k+2} \cdots d_{s-1} - 1 & \text{if} \quad 1 \leq r = s-k-1, \end{cases}$$

where we set $d_i \cdots d_j = 1$ if $i > j$ or $i < 1$, and $k \geq 0$, ℓ are the unique integers such that $d = \sum_{i=1}^{k}(d_i - 1) + \ell$ and $1 \leq \ell \leq d_{k+1} - 1$.

Proof. Setting $n = s-1$, $R = K[t_1, \ldots, t_n]$ a polynomial ring with coefficients in $K = \mathbb{F}_q$, and $L = (t_1^{d_1}, \ldots, t_n^{d_n})$, we order the set $M_{\leq d} := \Delta_\prec(L) \cap R_{\leq d}$ of all standard monomials of R/L of degree at most d with the lexicographic order (lex order for short), that is, $t^a \succ t^b$ if and only if the first non-zero entry of $a - b$ is positive. For $r > 1$, $0 \leq k \leq n-r$, the r-th monomial $t_1^{b_{r,1}} \cdots t_n^{b_{r,n}}$ of $M_{\leq d}$ in decreasing lex order is

$$t_1^{d_1-1} \cdots t_k^{d_k-1} t_{k+1}^{\ell-1} t_{k+r}$$

and the r-th monomial $t_1^{a_{r,1}} \cdots t_n^{a_{r,n}}$ of $M_{\geq c_0 - d} := \Delta_\prec(L) \cap R_{\geq c_0 - d}$ in ascending lex order, where $c_0 = \sum_{i=1}^{n}(d_i - 1)$, is

$$t_{k+1}^{d_{k+1}-\ell} t_{k+2}^{d_{k+2}-1} \cdots t_{k+r-1}^{d_{k+r-1}-1} t_{k+r}^{d_{k+r}-2} t_{k+r+1}^{d_{k+r+1}-1} \cdots t_n^{d_n-1}.$$

Case (I): $0 \leq k < n-r$. The case $r = 1$ was proved in [17, Theorem 3.8]. Thus we may also assume $r \geq 2$. Therefore, applying [1, Theorem 5.4], we obtain that $\delta_r(C_{\mathbb{X}}(d))$ is given by

$$
\begin{aligned}
1+\sum_{i=1}^{n} a_{r,i} \prod_{j=i+1}^{n} d_j &= 1+(d_{k+1}-\ell)d_{k+2}\cdots d_n+\sum_{i=k+2,i\neq k+r}^{n}(d_i-1)\prod_{j=i+1}^{n} d_j \\
&+(d_{k+r}-2)d_{k+r+1}\cdots d_n \\
&=(d_{k+1}-\ell)d_{k+2}\cdots d_n+\left(1+\sum_{i=k+2}^{n}(d_i-1)\prod_{j=i+1}^{n} d_j\right)-d_{k+r+1}\cdots d_n \\
&=(d_{k+1}-\ell)d_{k+2}\cdots d_n+(d_{k+2}\cdots d_n)-d_{k+r+1}\cdots d_n \\
&=(d_{k+1}-\ell+1)d_{k+2}\cdots d_n-d_{k+r+1}\cdots d_n \\
&=d_{k+r+1}\cdots d_n[(d_{k+1}-\ell+1)d_{k+2}\cdots d_{k+r}-1].
\end{aligned}
$$

Case (II): $k = n-r$. In this case the r-th monomial $t_1^{a_{r,1}}\cdots t_n^{a_{r,n}}$ of $M_{\geq c_0-d}$ in ascending lex order is

$$t_{k+1}^{d_{k+1}-\ell}t_{k+2}^{d_{k+2}-1}\cdots t_{k+r-1}^{d_{k+r-1}-1}t_{k+r}^{d_{k+r}-2}t_{k+r+1}^{d_{k+r+1}-1}\cdots t_n^{d_n-1}.$$

Therefore, applying [1, Theorem 5.4], we obtain that $\delta_r(C_{\mathbb{X}}(d))$ is given by

$$
\begin{aligned}
&1+\sum_{i=1}^{n} a_{r,i} \prod_{j=i+1}^{n} d_j \\
&=1+(d_{k+1}-\ell)d_{k+2}\cdots d_n+\sum_{i=k+2}^{n-1}(d_i-1)\prod_{j=i+1}^{n} d_j+(d_n-2) \\
&=(d_{k+1}-\ell)d_{k+2}\cdots d_n+\left(1+\sum_{i=k+2}^{n}(d_i-1)\prod_{j=i+1}^{n} d_j\right)-1 \\
&=(d_{k+1}-\ell)d_{k+2}\cdots d_n+(d_{k+2}\cdots d_n)-1=(d_{k+1}-\ell+1)d_{k+2}\cdots d_n-1.
\end{aligned}
$$

□

Definition 2.2. The set $\mathbb{T} = \{[(x_1,\ldots,x_s)] \in \mathbb{P}^{s-1} | \, x_i \in K^* \, \forall \, i\}$ is called a *projective torus*.

Corollary 2.3. *Let $\mathbb{T}$ be a projective torus in $\mathbb{P}^{s-1}$ and let $\delta_r(C_{\mathbb{T}}(d))$ be the r-th generalized Hamming weight of $C_{\mathbb{T}}(d)$. Then*

$$\delta_r(C_{\mathbb{T}}(d)) = \left[(q-1)^{r-1}(q-\ell)-1\right](q-1)^{s-k-r-1}$$

for $1 \leq r \leq s-k-1$, where $d = k(q-2)+\ell$, $k \geq 0$, $1 \leq \ell \leq q-2$.

Proof. The assertion follows readily from Theorem 2.1 making $A_i = K^* = \mathbb{F}_q \setminus \{0\}$ for $i = 1, \ldots, s-1$. $\square$

This corollary generalizes the case when $\mathbb{X}$ is a projective torus in $\mathbb{P}^{s-1}$ and $r = 1$:

Theorem 2.4. [24, Theorem 3.5] *Let $\mathbb{T}$ be a projective torus in $\mathbb{P}^{s-1}$ and let $C_{\mathbb{T}}(d)$ be the Reed–Muller-type code on $\mathbb{T}$ of degree $d \geq 1$. Then its length is $(q-1)^{s-1}$, its minimum distance is given by*

$$\delta_{\mathbb{T}}(d) = \begin{cases} (q-1)^{s-(k+2)}(q-1-\ell) & \text{if} \quad d \leq (q-2)(s-1)-1, \\ 1 & \text{if} \quad d \geq (q-2)(s-1), \end{cases}$$

where k and ℓ are the unique integers such that $k \geq 0$, $1 \leq \ell \leq q-2$ and $d = k(q-2)+\ell$, and the regularity of $S/I(\mathbb{T})$ is $(q-2)(s-1)$.

The case when $\mathbb{X}$ is a projective torus in $\mathbb{P}^{s-1}$ and $r = 2$ is treated in [6, Theorem 18].

3 Veronese type codes

Let $S = K[t_1, \ldots, t_s]$ be a polynomial ring over a field K and let $\{M_1, \ldots, M_N\}$ be the set of all monomials of S of degree $k \geq 1$, where $N = \binom{k+s-1}{s-1}$. The map

$$\rho_k \colon \mathbb{P}^{s-1} \to \mathbb{P}^{N-1}, \quad [x] \mapsto [(M_1(x), \ldots, M_N(x))]$$

is called the k-th *Veronese embedding*. Given $\mathbb{X} \subset \mathbb{P}^{s-1}$, the k-th *Veronese type code* of degree d is $C_{\rho_k(\mathbb{X})}(d)$, the Reed–Muller-type code of degree d on $\rho_k(\mathbb{X})$. The next aim is to show that the Reed–Muller-type code $C_{\mathbb{X}}(kd)$ has the same basic parameters and the same generalized Hamming weights as the Veronese type code $C_{\rho_k(\mathbb{X})}(d)$ for $k \geq 1$ and $d \geq 1$.

Lemma 3.1. *ρ_k is well-defined and injective.*

Proof. If $[x] = [z]$, $x, y \in \mathbb{P}^{s-1}$, $x = (x_1, \ldots, x_s)$, $z = (z_1, \ldots, z_s)$, then $x = \lambda z$ for some $\lambda \in K^*$. Thus $M_i(x) = \lambda^k M_i(z)$ for all i, that is, $[(M_i(x))] = [(M_i(z))]$, here we are using $(M_i(x))$ as a short hand for $(M_1(x), \ldots, M_N(x))$. Thus ρ_k is well-defined. To show that ρ_k is injective assume that $\rho_k([x]) = \rho_k([z])$. Then for some $\mu \in K^*$ one has $M_i(x) = \mu M_i(z)$ for all i. Pick j such that $z_j \neq 0$ and let $\lambda = x_j/z_j$. Note that $M_i = t_j^k$ for some i. Then one has $x_j^k = \mu z_j^k$, that is, $\mu = \lambda^k$. For each $1 \leq \ell \leq s$, using the monomial $M_i = t_j^{k-1} t_\ell$, one has

$$x_j^{k-1} x_\ell = \mu z_j^{k-1} z_\ell = \lambda^k z_j^{k-1} z_\ell = \lambda(\lambda z_j)^{k-1} z_\ell = \lambda(x_j^{k-1}) z_\ell.$$

Thus $x_\ell = \lambda z_\ell$ for all ℓ, that is, $[x] = [z]$. $\square$

We come to the main result of this section.

Theorem 3.2. *If $\mathbb{X} \subset \mathbb{P}^{s-1}$, then the projective Reed–Muller-type codes $C_{\mathbb{X}}(kd)$ and $C_{\rho_k(\mathbb{X})}(d)$ have the same basic parameters and the same generalized Hamming weights for $k \geq 1$ and $d \geq 1$.*

Proof. Setting $N = \binom{k+s-1}{s-1}$, let $R = K[y_1, \ldots, y_N] = \oplus_{d=0}^{\infty} R_d$ be a polynomial ring over the field K with the standard grading. We can write $\mathbb{X} = \{[P_1,], \ldots, [P_m]\}$, where $m = |\mathbb{X}|$, $P_i \in K^s$, and the $[P_i]$'s are in standard form, i.e., the first non-zero entry of P_i is 1 for all i. By Lemma 3.1 the map ρ_k is injective. Thus $C_{\mathbb{X}}(kd)$ and $C_{\rho_k(\mathbb{X})}(d)$ have the same length. As $[P_1], \ldots, [P_m]$ are in standard form, for each i there is $g_i \in S_{kd}$ such that $g_i(P_i) = 1$. Therefore, by [19, Lemma 2.13], we may assume that the Reed–Muller-type code $C_{\mathbb{X}}(kd)$ is the image of the evaluation map

$$\mathrm{ev}_{kd}\colon S_{kd} = K[t_1, \ldots, t_s]_{kd} \to K^m, \qquad g \mapsto (g(P_1), \ldots, g(P_m))\,, \tag{1}$$

and the Veronese type code $C_{\rho_k(\mathbb{X})}(d)$ is the image of the evaluation map

$$\mathrm{ev}_d^1\colon R_d = K[y_1, \ldots, y_N]_d \to K^m, \qquad f \mapsto \left(\frac{f(Q_1)}{f_1(Q_1)}, \ldots, \frac{f(Q_m)}{f_m(Q_m)}\right), \tag{2}$$

where $Q_i = (M_1(P_i), \ldots, M_N(P_i))$ for $i = 1, \ldots, m$, and $f_1, \ldots, f_m$ are polynomials in R_d such that $f_i(Q_i) \neq 0$ for $i = 1, \ldots, m$. For any polynomial $f = f(y_1, \ldots, y_N) = \sum \lambda_a y^a$ in R_d, $\lambda_a \in K^*$, one has

$$\begin{aligned} f(M_1, \ldots, M_N)(P_i) &= \sum \lambda_a (M_1^{a_1} \cdots M_N^{a_N})(P_i) \qquad (3)\\ &= \sum \lambda_a M_1^{a_1}(P_i) \cdots M_N^{a_N}(P_i) \\ &= f(M_1(P_i), \ldots, M_N(P_i)). \end{aligned}$$

As $K[t_1, \ldots, t_s]_{kd}$ is equal to $K[M_1, \ldots, M_N]_d$, any g in $K[t_1, \ldots, t_s]_{kd}$ can be written as $g = f(M_1, \ldots, M_N)$ for some $f = f(y_1, \ldots, y_N)$ in R_d. Therefore, using Eq. (3), we get

$$\begin{aligned} C_{\mathbb{X}}(kd) &= \{(g(P_1), \ldots, g(P_m)) \,|\, g \in K[t_1, \ldots, t_s]_{kd}\} \\ &= \{(f(Q_1), \ldots, f(Q_m)) \,|\, f \in K[y_1, \ldots, y_N]_d\}. \end{aligned}$$

As a consequence, setting $\lambda_i = f_i(Q_i)$ and $\lambda = (\lambda_1, \ldots, \lambda_m)$, one has

$$C_{\mathbb{X}}(kd) = \lambda \cdot C_{\rho_k(\mathbb{X})}(d) := \{\lambda \cdot a \,|\, a \in C_{\rho_k(\mathbb{X})}(d)\}, \tag{4}$$

where $\lambda \cdot a := (\lambda_1 a_1, \ldots, \lambda_m a_m)$ for $a = (a_1, \ldots, a_m)$ in $C_{\rho_k(\mathbb{X})}(d)$. This means that the linear codes $C_{\mathbb{X}}(kd)$ and $C_{\rho_k(\mathbb{X})}(d)$ are equivalent [8, Remark 1]. Thus the dimension and minimum distance of $C_{\mathbb{X}}(kd)$ and $C_{\rho_k(\mathbb{X})}(d)$ are the same, and so are the generalized Hamming weights. □

For convenience we recall the following classical result of Sørensen [26].

Theorem 3.3. (Sørensen [26]) *Let $K = \mathbb{F}_q$ be a finite field and let $C_{\mathbb{X}}(d)$ be the classical projective Reed–Muller code of degree d on the set $\mathbb{X} = \mathbb{P}^{s-1}$. Then $|\mathbb{X}| = (q^s - 1)/(q - 1)$, the minimum distance of $C_{\mathbb{X}}(d)$ is given by*

$$\delta_{\mathbb{X}}(d) = \begin{cases} (q-\ell+1)\, q^{s-k-2} & \text{if } d \leq (s-1)(q-1), \\ 1 & \text{if } d \geq (s-1)(q-1)+1, \end{cases}$$

where $0 \leq k \leq s-2$ and ℓ are the unique integers such that $d = k(q-1)+\ell$ and $1 \leq \ell \leq q-1$, and the regularity of $S/I(\mathbb{X})$ is $(s-1)(q-1)+1$.

Veronese codes are a natural generalization of the classical projective Reed–Muller codes.

Corollary 3.4. *[23, Proposition 1] If $\mathbb{V}_k = \rho_k(\mathbb{P}^{s-1})$, then the projective Reed–Muller-type codes $C_{\mathbb{V}_k}(d)$ and $C_{\mathbb{P}^{s-1}}(kd)$ have the same basic parameters for $k \geq 1$ and $d \geq 1$.*

Proof. This follows at once from Theorem 3.2 making $\mathbb{X} = \mathbb{P}^{s-1}$. □

As a byproduct we relate the dual codes of $C_{\rho_k(\mathbb{X})}(d)$ and $C_{\mathbb{X}}(kd)$.

Theorem 3.5. *If $\mathbb{X}$ is a subset of $\mathbb{P}^{s-1}$, then $C^{\perp}_{\rho_k(\mathbb{X})}(d)$ and $C^{\perp}_{\mathbb{X}}(kd)$ are equivalent codes and*

$$C^{\perp}_{\rho_k(\mathbb{X})}(d) = \lambda \cdot C^{\perp}_{\mathbb{X}}(kd),$$

where $\lambda = (\lambda_1, \ldots, \lambda_m)$, with $\lambda_i = f_i(Q_i)$ for all $i = 1, \ldots, m$, is the vector that was given in the proof of Theorem 3.2.

Proof. Let $(u_1, \ldots, u_m) \in C^{\perp}_{\mathbb{X}}(kd)$. Then

$$\langle (u_1, \ldots, u_m), (v_1, \ldots, v_m) \rangle = \sum_{i=1}^{m} u_i v_i = 0,$$

for all $(v_1, \ldots, v_m) \in C_{\mathbb{X}}(kd)$. By using Eq. (4) we conclude that

$$\langle (u_1, \ldots, u_m), (\lambda_1 v'_1, \ldots, \lambda_m v'_m) \rangle = \sum_{i=1}^{m} u_i \lambda_i v'_i = 0,$$

for all $(v'_1, \ldots, v'_m) \in C_{\rho_k(\mathbb{X})}(d)$. Therefore

$$\langle (\lambda_1 u_1, \ldots, \lambda_m u_m), (v'_1, \ldots, v'_m) \rangle = \sum_{i=1}^{m} \lambda_i u_i v'_i = 0.$$

for all $(v_1', \ldots, v_m') \in C_{\rho_k(\mathbb{X})}(d)$. Thus

$$\lambda \cdot C_{\mathbb{X}}^{\perp}(kd) \subset C_{\rho_k(\mathbb{X})}^{\perp}(d). \tag{5}$$

Furthermore one has the equalities

$$\begin{aligned} \dim_K \lambda \cdot C_{\mathbb{X}}^{\perp}(kd) &= \dim_K C_{\mathbb{X}}^{\perp}(kd) = m - \dim_K C_{\mathbb{X}}(kd) \\ &= m - \dim_K C_{\rho_k(\mathbb{X})}(d) = \dim_K C_{\rho_k(\mathbb{X})}^{\perp}(d), \end{aligned} \tag{6}$$

and the equality $C_{\rho_k(\mathbb{X})}^{\perp}(d) = \lambda \cdot C_{\mathbb{X}}^{\perp}(kd)$ follows from Eqs. (5) and (6). Thus $C_{\rho_k(\mathbb{X})}^{\perp}(d)$ and $C_{\mathbb{X}}^{\perp}(kd)$ are equivalent codes [8, Remark 1]. □

Corollary 3.6. *If $\mathbb{X} = \mathbb{P}^{s-1}$, $\mathbb{V}_k = \rho_k(\mathbb{P}^{s-1})$, and $kd \leq (q-1)(s-1)$, then the linear code $C_{\mathbb{V}_k}(d)$ is equivalent to*

$$\begin{cases} C_{\mathbb{P}^{s-1}}((q-1)(s-1) - kd) & \text{if } kd \not\equiv 0 \mod (q-1), \\ ((1, \ldots, 1), C_{\mathbb{P}^{s-1}}((q-1)(s-1) - kd)) & \text{if } kd \equiv 0 \mod (q-1), \end{cases}$$

where $((1, \ldots, 1), C_{\mathbb{P}^{s-1}}((q-1)(s-1) - kd))$ is the subspace of K^m generated by $(1, \ldots, 1)$ and $C_{\mathbb{P}^{s-1}}((q-1)(s-1) - kd)$.

Proof. This result follows at once from Theorem 3.5 and [26, Theorem 2]. □

The rest of this section is devoted to show some explicit examples.

Example 3.7. Let K be the field $\mathbb{F}_8$. If $\mathbb{X} = \mathbb{P}^2$, then by Theorem 3.3 the basic parameters of the classical projective Reed–Muller-type code $C_{\mathbb{X}}(d)$ of degree d are given by

d	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\lvert\mathbb{X}\rvert$	73	73	73	73	73	73	73	73	73	73	73	73	73	73	73
$H_{\mathbb{X}}(d)$	3	6	10	15	21	28	36	45	52	58	63	67	70	72	73
$\delta_{\mathbb{X}}(d)$	64	56	48	40	32	24	16	8	7	6	5	4	3	2	1

The dimension of $C_{\mathbb{X}}(d)$ is $H_{\mathbb{X}}(d)$. The regularity of $S/I(\mathbb{X})$ is 15 and the a-invariant is 14.

Example 3.8. Let K be the field $\mathbb{F}_8$. If $k = 2$, $\mathbb{X} = \mathbb{P}^2$, and $\mathbb{V}_2 = \rho_2(\mathbb{X})$, then by Theorem 3.2 and Example 3.7 the parameters of the Veronese code $C_{\mathbb{V}_2}(d)$ of degree d are given by

d	1	2	3	4	5	6	7	8
$\lvert\mathbb{V}_2\rvert$	73	73	73	73	73	73	73	73
$H_{\mathbb{V}_2}(d)$	6	15	28	45	58	67	72	73
$\delta_{\mathbb{V}_2}(d)$	56	40	24	8	6	4	2	1

The regularity of $S/I(\mathbb{V}_2)$ is 8 and the a-invariant is 7.

Example 3.9. Let K be the field $\mathbb{F}_5$. If $k = 2$, $\mathbb{T}$ is a projective torus in $\mathbb{P}^2$, and $\rho_2(\mathbb{T})$ is the corresponding Veronese type code, then by Corollary 2.3, Theorem 2.4, [6, Theorem 18], and *Macaulay*2 [12], we obtain the following information for $C_{\mathbb{T}}(d)$:

d	1	2	3	4	5	6
$\lvert\mathbb{T}\rvert$	16	16	16	16	16	16
$H_{\mathbb{T}}(d)$	3	6	10	13	15	16
$\delta_{\mathbb{T}}(d)$	12	8	4	3	2	1
$\delta_2(C_{\mathbb{T}}(d))$	15	11	7	4	3	2
$\delta_3(C_{\mathbb{T}}(d))$	16	12	8	6	4	3

and the regularity of $S/I(\mathbb{T})$ is 6. Therefore, by Theorem 3.2, we get the following information for the Veronese type code $C_{\rho_2(\mathbb{T})}(d)$:

d	1	2	3
$\lvert\rho_2(\mathbb{T})\rvert$	16	16	16
$H_{\rho_2(\mathbb{T})}(d)$	6	13	16
$\delta_{\rho_2(\mathbb{T})}(d)$	8	3	1
$\delta_2(C_{\rho_2(\mathbb{T})}(d))$	11	4	2
$\delta_3(C_{\rho_2(\mathbb{T})}(d))$	12	6	3

and the regularity of $S/I(\rho_2(\mathbb{T}))$ is 3.

References

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

[2] C. Carvalho, On the second Hamming weight of some Reed-Muller type codes, Finite Fields Appl. **24** (2013), 88–94.

[3] D. Cox, J. Little and D. O'Shea, *Ideals, Varieties, and Algorithms*, Springer-Verlag, 1992.

[4] M. Datta and S. Ghorpade, Number of solutions of systems of homogeneous polynomial equations over finite fields, Proc. Amer. Math. Soc. **145** (2017), no. 2, 525–541.

[5] I. M. Duursma, C. Rentería and H. Tapia-Recillas, Reed-Muller codes on complete intersections, Appl. Algebra Engrg. Comm. Comput. **11** (2001), no. 6, 455–462.

[6] M. González-Sarabia, E. Camps, E. Sarmiento and R. H. Villarreal, The second generalized Hamming weight of some evaluation codes arising from a projective torus, Finite Fields Appl. **52** (2018), 370–394.

[7] M. Gonzlez-Sarabia, J. Martnez-Bernal, R.H. Villarreal, and C.E. Vivares, Generalized minimum distance functions, J. Algebraic Combin. **50** (2019), no. 3, 317–346.

[8] M. González–Sarabia and C. Rentería, The dual code of some Reed-Muller type codes, Appl. Algebra Engrg. Comm. Comput. **14** (2004), no. 5, 329–333.

[9] M. González–Sarabia and C. Rentería, Generalized Hamming weights and some parameterized codes, Discrete Math. **339** (2016), 813–821.

[10] M. González–Sarabia, C. Rentería, and E. Sarmiento, Projective parameterized linear codes, An. Stiint. Univ. Ovidius Constanta Ser. Mat. 23, 2 (2015) 223–240.

[11] M. González-Sarabia, C. Rentería and H. Tapia-Recillas, Reed-Muller-type codes over the Segre variety, Finite Fields Appl. **8** (2002), no. 4, 511–518.

[12] D. Grayson and M. Stillman, *Macaulay*2, *a software system for research in algebraic geometry*, available at `http://www.math.uiuc.edu/Macaulay2/`.

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

[14] T. Helleseth, T. Kløve and J. Mykkelveit, The weight distribution of irreducible cyclic codes with block lengths $n_1((q^l-1)/N)$, Discrete Math. **18** (1977), 179–211.

[15] T. Johnsen and H. Verdure, Generalized Hamming weights for almost affine codes, IEEE Trans. Inform. Theory **63** (2017), no. 4, 1941–1953.

[16] T. Kløve, The weight distribution of linear codes over $GF(q^l)$ having generator matrix over $GF(q)$, Discrete Math. **23** (1978), no. 2, 159–168.

[17] H. H. López, C. Rentería and R. H. Villarreal, Affine cartesian codes, Des. Codes Cryptogr. **71** (2014), no. 1, 5–19.

[18] F. J. MacWilliams and N. J. A. Sloane, The Theory of Error-correcting Codes, North-Holland, 1977.

[19] J. Martínez-Bernal, Y. Pitones and R. H. Villarreal, Minimum distance functions of graded ideals and Reed-Muller-type codes, J. Pure Appl. Algebra **221** (2017), 251–275.

[20] J. Neves, M. Vaz Pinto and R. H. Villarreal, Vanishing ideals over graphs and even cycles, Comm. Algebra 43 3 (2015) 1050–1075.

[21] W. Olaya–León and C. Granados–Pinzón, The second generalized Hamming weight of certain Castle codes, Des. Codes Cryptogr. **76** (2015), no. 1, 81–87.

[22] C. Rentería, A. Simis and R. H. Villarreal, Algebraic methods for parameterized codes and invariants of vanishing ideals over finite fields, Finite Fields Appl. **17** (2011), no. 1, 81–104.

[23] C. Rentería and H. Tapia-Recillas, Reed-Muller type codes on the Veronese variety over finite fields, *Coding theory, cryptography and related areas* (Guanajuato, 1998), 237–243, Springer, Berlin, 2000.

[24] E. Sarmiento, M. Vaz Pinto and R. H. Villarreal, The minimum distance of parameterized codes on projective tori, Appl. Algebra Engrg. Comm. Comput. **22** (2011), no. 4, 249–264.

[25] H. G. Schaathun and W. Willems, A lower bound on the weight hierarchies of product codes, Discrete Appl. Math. **128** (2003), no. 1, 251–261.

[26] A. Sørensen, Projective Reed-Muller codes, IEEE Trans. Inform. Theory **37** (1991), no. 6, 1567–1576.

[27] M. Tsfasman, S. Vladut and D. Nogin, *Algebraic geometric codes*: *basic notions*, Mathematical Surveys and Monographs **139**, American Mathematical Society, Providence, RI, 2007.

[28] R. H. Villarreal, *Monomial Algebras, Second Edition*, Monographs and Research Notes in Mathematics, Chapman and Hall/CRC, 2015.

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

[30] V. K. Wei and K. Yang, On the generalized Hamming weights of product codes, IEEE Trans. Inform. Theory **39** (1993), no. 5, 1709–1713.

[31] M. Yang, J. Lin, K. Feng and D. Lin, Generalized Hamming weights of irreducible cyclic codes, IEEE Trans. Inform. Theory **61** (2015), no. 9, 4905–4913.

Manuel GONZÁLEZ–SARABIA,
Instituto Politécnico Nacional,
UPIITA, Av. IPN No. 2580,
Col. Barrio la Laguna, Ticomán,
Gustavo A. Madero,
C.P. 07340, Ciudad de México, México.
Departamento de Ciencias Básicas.
Supported by COFAA-IPN and SNI, México.
Email: mgonzalezsa@ipn.mx

Delio JARAMILLO,
Departamento de Matemáticas,
Centro de Investigación y de Estudios Avanzados del IPN,
Apartado Postal 14–740,
07000 Mexico City, D.F.
Supported by a scholarship from CONACyT, México.
Email: djaramillo@math.cinvestav.mx

Rafael H. VILLARREAL,
Departamento de Matemáticas,
Centro de Investigación y de Estudios Avanzados del IPN,
Apartado Postal 14–740,
07000 Mexico City, D.F.
Supported by SNI, México.
Email: vila@math.cinvestav.mx