

CARTESIAN SQUARE-FREE CODES

CÍCERO CARVALHO, HIRAM H. LÓPEZ, AND RODRIGO SAN-JOSÉ

Festschrift on the occasion of the 80th anniversary of the Mexican Mathematical Society

ABSTRACT. The generalized Hamming weights (GHWs) of a linear code C extend the concept of minimum distance, which is the minimum cardinality of the support of all one-dimensional subspaces of C , to the minimum cardinality of the support of all r -dimensional subspaces of the code. In this work, we introduce Cartesian square-free codes, which are linear codes generated by evaluating square-free monomials over a Cartesian set. We use commutative algebraic tools, specifically the footprint bound, to provide explicit formulas for some of the GHWs of this family of codes, and we show how we can translate these results to evaluation codes over the projective space.

1. INTRODUCTION

An $[n, k, d]$ linear code C over a finite field with q elements $\mathbb{F}_q$ is a k -dimensional subspace of $\mathbb{F}_q^n$ with minimum distance $d := \min\{d(\mathbf{c}, \mathbf{c}') : \mathbf{c}, \mathbf{c}' \in C, \mathbf{c} \neq \mathbf{c}'\}$, where $d(\mathbf{c}, \mathbf{c}') := \min |\{i : c_i \neq c'_i\}|$ denotes the Hamming distance. Linear codes, extensively studied for more than seventy-five years since the seminal paper by Shannon in 1948 [25], were originally introduced to reliably and efficiently communicate information from a source to a receiver through a noisy channel. Throughout the years, linear codes have found a series of applications such as satellite communication, cell phones, distributed computation, and cryptography, among many others. In 1991, Wei introduced generalized Hamming weights (GHWs) for linear codes to measure the performance of a type-II wiretap channel [31]. The GHWs extend the minimum distance of a code, which is the minimum cardinality of the support of all one-dimensional subspaces of C , to the minimum cardinality of the support of all r -dimensional subspaces of C . Specifically, the r^{th} -generalized Hamming weight of a code $C \subseteq \mathbb{F}_q^n$ is given by

$$d_r(C) := \min \{|\text{supp}(C')| : C' \text{ is a subcode of } C \text{ of dimension } r\},$$

2010 *Mathematics Subject Classification.* 94B05; 81P70; 11T71; 14G50.

Key words and phrases. Square-free codes, Cartesian codes, footprint bound, generalized Hamming weights.

Cícero Carvalho was partially supported by Fapemig - grant APQ-01430-24, and CNPq grant PQ 308708/2023-7. Hiram H. López was partially supported by the NSF Grants DMS-2401558 and DMS-2502705. Rodrigo San-José was partially supported by Grant PID2022-138906NB-C21 funded by MICIU/AEI/10.13039/501100011033 and by ERDF/EU, and FPU20/01311 funded by the Spanish Ministry of Universities.

where $1 \leq r \leq k$ and $\text{supp}(C) := \{i : \exists c \in C \text{ with } c_i \neq 0\} = \bigcup_{c \in C} \text{supp}(c)$. The weight hierarchy of C is defined to be the set of integers $\{d_r(C) : 1 \leq r \leq k\}$. In the same work [31], Wei computed the weight hierarchy for several families of linear codes, including Reed–Muller, Hamming, and extended Hamming, simplex (dual of a Hamming), Reed–Solomon, and all maximum-distance-separable (MDS) codes.

Since 1991, the weight hierarchy has been extensively studied in the literature. Helleseth, Kløve, and Ytrehus focused on the GHMs of binary linear codes in [14]. They gave bounds for these weights, provided a generalized Griesmer bound, determined the weight hierarchies for $k \leq 3$, and the optimal values of d_r for $r \geq k - 3$. In 1992, Feng, Tzeng, and Wei provided the GHWs for certain families of cyclic codes in [10]. Janwa and Lal also studied the GHWs of cyclic codes in [15]. Other examples of families of codes for which the GHWs were studied are product codes [30], trace codes [26], Hermitian codes [1, 13], and more generally, decreasing norm-trace codes [8], q -ary Reed–Muller codes [13], projective Reed–Muller codes [3, 5, 21] and their variants [11, 17], Melas codes and dual Melas codes [27], BCH codes [28], convolutional codes [12, 20] and matrix-product codes [22].

Evaluation codes form an important family of linear codes defined by evaluating functions on certain points. Some examples are Reed–Solomon codes, which are given by evaluating polynomials in one variable up to a certain degree over a subset of points A of $\mathbb{F}_q$. When we move from one to several variables, and from A to $\mathbb{F}_q^m$, we obtain the Reed–Muller codes. In this work, we focus on the GHWs of the evaluation codes generated by the evaluation of square-free monomials over a Cartesian set. These are called Cartesian square-free codes, which include as particular cases all the previous families of square-free codes, such as binary Reed–Muller codes, or square-free codes over the torus $(\mathbb{F}_q^*)^m$ [16, 19].

The content of this paper is as follows. In Section 2, we introduce notation and elementary results about GHWs. In Section 3, we describe the footprint bound, an essential tool from commutative algebra that we use to compute the GHWs of Cartesian square-free codes. In Section 4, we use the results from Section 3 to give explicit formulas that provide the weight hierarchies of Cartesian square-free codes. In Section 5, we show that some of the results about the GHWs can be translated to evaluation codes over the projective space.

2. PRELIMINARIES

Let $A_1, \dots, A_m$ be a collection of non-empty subsets of $\mathbb{F}_q$, the finite field with q elements. We denote their Cartesian product by $\mathbb{X} = A_1 \times \dots \times A_m$. Let $n_i = |A_i|$, for $1 \leq i \leq m$. Without loss of generality, in what follows, we assume that $2 \leq n_1 \leq n_2 \leq \dots \leq n_m$. We denote $B_{\mathbb{X}} = \{0, \dots, n_1 - 1\} \times \dots \times \{0, \dots, n_m - 1\}$. We consider $S(m) = \{0, 1\}^m$, and we denote by $S_d(m)$ (resp., $S_{\leq d}(m)$) the tuples $(\alpha_1, \dots, \alpha_m) \in S$ such that $\sum_{i=1}^m \alpha_i = d$ (resp., $\sum_{i=1}^m \alpha_i \leq d$). We may omit the reference to m if it is obvious from context, and denote these sets by S_d and $S_{\leq d}$. We consider the codes

$$C_d^{\mathbb{X}, S} := \langle \text{ev}_{\mathbb{X}}(x^\alpha) : \alpha \in S_d \rangle, \quad C_{\leq d}^{\mathbb{X}, S} := \langle \text{ev}_{\mathbb{X}}(x^\alpha) : \alpha \in S_{\leq d} \rangle.$$

Note that $C_d^{\mathbb{X},S}$ is the evaluation code generated by evaluating the square-free monomials of total degree d in m variables over the Cartesian set $\mathbb{X}$. Since we only evaluate square-free monomials, these are called Cartesian square-free codes. Their length is $n = \prod_{i=1}^m n_i$. For the codes $C_d^{\mathbb{X},S}$, we have that $\dim C_d^{\mathbb{X},S} = \binom{m}{d}$, the number of square-free monomials of degree d . By adding over all possible degrees $0 \leq d' \leq d$, we also obtain $\dim C_{\leq d}^{\mathbb{X},S} = \sum_{i=0}^d \binom{m}{i}$. Note that, for $d > m$, we have $S_d = \emptyset$ and $S_{\leq d} = V_{\leq m}^S$. Thus, we only consider these codes for $1 \leq d \leq m$.

We are mainly interested in the generalized Hamming weights of these Cartesian square-free codes. Given a tuple or a vector $\alpha = (\alpha_1, \dots, \alpha_n)$, define

$$\text{supp}(\alpha) = \{i : \alpha_i \neq 0\}.$$

Similarly, the support of a code $C \subset \mathbb{F}_q^n$ is

$$\text{supp}(C) := \{i : \exists c \in C \text{ with } c_i \neq 0\} = \bigcup_{c \in C} \text{supp}(c).$$

Definition 2.1. The r^{th} -generalized Hamming weight of an $[n, k, d]$ code C is

$$d_r(C) := \min \{|\text{supp}(C')| : C' \text{ is a subcode of } C \text{ of dimension } r\},$$

where $1 \leq r \leq k$.

The first generalized Hamming weight $d_1(C)$ is just the minimum distance of C . Wei obtained the following general properties of the generalized Hamming weights in [31].

Theorem 2.2 (Monotonicity). *For an $[n, k]$ linear code C with $k > 0$, we have*

$$1 \leq d_1(C) < d_2(C) < \dots < d_k(C) \leq n.$$

Definition 2.3. The dual of a code $C \subset \mathbb{F}_q^n$ is defined by

$$C^\perp := \{\mathbf{w} \in \mathbb{F}_q^n : \mathbf{w} \cdot \mathbf{c} = 0 \text{ for all } \mathbf{c} \in C\},$$

where $\mathbf{w} \cdot \mathbf{c}$ represents the Euclidean inner product.

The following theorem relates the GHWs of a code and its dual.

Theorem 2.4 (Duality). *Let C be an $[n, k]$ code. Then*

$$\{d_r(C) : 1 \leq r \leq k\} = \{1, 2, \dots, n\} \setminus \{n + 1 - d_r(C^\perp) : 1 \leq r \leq n - k\}.$$

3. FOOTPRINT BOUND

In this section, we introduce the footprint bound, which is the main tool we use to study the GHWs of square-free codes. For the tools we use from commutative algebra, we recommend the references [9, 29]. Fix a monomial order $\prec$ such that $x_1 \prec x_2 \prec \dots \prec x_m$, and let $\mathbb{M}^m$ be the set of monomials of $\mathbb{F}_q[x_1, \dots, x_m]$. For an ideal $I \subset \mathbb{F}_q[x_1, \dots, x_m]$, we denote

$$\Delta(I) := \{M \in \mathbb{M}^m : M \notin \text{in}(I)\} = \{M \in \mathbb{M}^m : \text{in}(g) \nmid M \ \forall g \in \mathcal{G}\},$$

where $\mathcal{G}$ is a Grobner basis for I . The footprint bound states that

$$|V(I)| \leq |\Delta(I)| = |\Delta(\text{in}(I))|,$$

with equality if I is radical (see [9, Thm. 6 and Prop. 7, Chapter 5 §3]). We denote by $\mathbb{M}_d^m$ (resp., $\mathbb{M}_{\leq d}^m$) the set $\{x^\alpha \in \mathbb{M}^m : |\alpha| = d\}$ (resp., $\{x^\alpha \in \mathbb{M}^m : |\alpha| \leq d\}$). Similarly, we denote $\mathbb{M}_d^S$ (resp., $\mathbb{M}_{\leq d}^S$) the set $\{x^\alpha \in \mathbb{M}^m : \alpha \in S_d\}$ (resp., $\{x^\alpha \in \mathbb{M}^m : \alpha \in S_{\leq d}\}$). Let $\mathcal{N}_{r,d} := \{N = \{x^{\alpha_1}, \dots, x^{\alpha_r}\} \subset \mathbb{M}_d^S : \alpha_i \neq \alpha_j \text{ for } i \neq j\}$ and $\mathcal{N}_{r,\leq d} := \{N = \{x^{\alpha_1}, \dots, x^{\alpha_r}\} \subset \mathbb{M}_{\leq d}^S : \alpha_i \neq \alpha_j \text{ for } i \neq j\}$. In terms of codes, the footprint bound gives the following:

$$(3.1) \quad \begin{aligned} d_r(C_d^{\mathbb{X},S}) &\geq n_1 \cdots n_m - \max\{|\Delta_{\mathbb{X}}(N)|, N \in \mathcal{N}_{r,d}\} = \min\{|\nabla_{\mathbb{X}}(N)|, N \in \mathcal{N}_{r,d}\}, \\ d_r(C_{\leq d}^{\mathbb{X},S}) &\geq n_1 \cdots n_m - \max\{|\Delta_{\mathbb{X}}(N)|, N \in \mathcal{N}_{r,\leq d}\} = \min\{|\nabla_{\mathbb{X}}(N)|, N \in \mathcal{N}_{r,\leq d}\}, \end{aligned}$$

where $\Delta_{\mathbb{X}}(N) := \Delta(\text{in}(I(\mathbb{X})) + (x^\alpha \in N))$ and $\nabla_{\mathbb{X}}(N) := \Delta(I(\mathbb{X})) \setminus \Delta_{\mathbb{X}}(N)$. The set $\nabla_{\mathbb{X}}(N)$ is called the shadow of N . We show now that this bound is sharp for the GHWs of the codes $C_d^{\mathbb{X},S}$ and $C_{\leq d}^{\mathbb{X},S}$. First, we recall that the footprint bound is sharp for monomial decreasing Cartesian codes (in the sense of [2,6]). This follows from the proof of [7, Thm. 5.1], which works for any decreasing Cartesian code. This leads to the following result.

Theorem 3.1. *Let $\mathbb{X} = A_1 \times \cdots \times A_m$ be a Cartesian set, let $0 \leq d \leq m$, let $1 \leq r \leq \binom{m}{d}$, and let $M = \{x^{\alpha_1}, \dots, x^{\alpha_r}\} \subset \mathbb{M}_{\leq d}^S$. Then there exists a set $F = \{f_1, \dots, f_r\} \subset \mathcal{L}(\mathbb{M}_{\leq d}^S)$ such that $\text{in}(f_i) = x^{\alpha_i}$, $1 \leq i \leq r$, and*

$$|V_{\mathbb{X}}(F)| = |\Delta_{\mathbb{X}}(M)|.$$

As a consequence,

$$d_r(C_{\leq d}^{\mathbb{X},S}) = n_1 \cdots n_m - \max\{|\Delta_{\mathbb{X}}(N)|, N \in \mathcal{N}_{r,\leq d}\} = \min\{|\nabla_{\mathbb{X}}(N)|, N \in \mathcal{N}_{r,\leq d}\}.$$

The previous theorem shows that we can compute the footprint bound instead of directly computing the GHWs and obtain the same result. This gives a significant computational advantage and transforms the problem of computing the GHWs into a combinatorial problem in which we have to find a set of r monomials that minimizes the cardinality of the shadow. We can obtain similar results for the homogeneous case under additional hypotheses.

Theorem 3.2. *Let $\mathbb{X} = A_1 \times \cdots \times A_m$ be a Cartesian set such that $0 \in A_i$, $1 \leq i \leq m$. Let $1 \leq d \leq m$, let $1 \leq r \leq \binom{m}{d}$, and let $M = \{x^{\alpha_1}, \dots, x^{\alpha_r}\} \subset \mathbb{M}_d^S$. Then there exists a set $F = \{f_1, \dots, f_r\} \subset \mathcal{L}(\mathbb{M}_d^S)$ such that $\text{in}(f_i) = x^{\alpha_i}$, $1 \leq i \leq r$, and*

$$|V_{\mathbb{X}}(F)| = |\Delta_{\mathbb{X}}(M)|.$$

As a consequence,

$$d_r(C_d^{\mathbb{X},S}) = n_1 \cdots n_m - \max\{|\Delta_{\mathbb{X}}(N)|, N \in \mathcal{N}_{r,d}\} = \min\{|\nabla_{\mathbb{X}}(N)|, N \in \mathcal{N}_{r,d}\}.$$

Proof. Let $A_i = \{a_{i0} = 0, a_{i1}, \dots, a_{i(n_i-1)}\}$, for $1 \leq i \leq m$. We consider the bijection

$$\begin{aligned} \varphi: \quad \mathbb{X} &\rightarrow \Delta(I(\mathbb{X})), \\ (a_{1,i_1}, \dots, a_{m,i_m}) &\mapsto x_1^{i_1} \cdots x_m^{i_m}. \end{aligned}$$

We will prove that φ restricts to a bijection from $V_{\mathbb{X}}(M)$ to $\Delta_{\mathbb{X}}(M)$, which gives the result. Let $P = (a_{1,i_1}, \dots, a_{m,i_m}) \in V_{\mathbb{X}}(M)$. If $x^{\alpha_\ell} \mid \varphi(P) = x_1^{i_1} \cdots x_m^{i_m}$ for some $1 \leq \ell \leq r$, then $i_j \geq 1$ for all $j \in \text{supp}(\alpha_\ell)$. This implies that $\text{supp}(\alpha_\ell) \subset \text{supp}(P)$, and $x^{\alpha_\ell}(P) = \prod_{j \in \text{supp}(\alpha_\ell)} a_{j,i_j} \neq 0$, a contradiction with the fact that $P \in V_{\mathbb{X}}(M)$.

Now let $x^\beta \in \Delta_{\mathbb{X}}(M)$. Let $1 \leq i \leq r$. There is $1 \leq j \leq m$ such that $x_j \mid x^{\alpha_i}$ but $x_j \nmid x^\beta$. This entails that $\varphi^{-1}(x^\beta)$ has a zero in position j , and thus $x^{\alpha_i}(\varphi^{-1}(x^\beta)) = 0$. Since we arrive at this conclusion for any $1 \leq i \leq r$, we obtain $\varphi^{-1}(x^\beta) \in V_{\mathbb{X}}(M)$. $\square$

Remark 3.3. The proof of Theorem 3.2 works for any set of square-free monomials, evaluating over any set X with the property that if $(P_1, \dots, P_m) \in X$, then we also have $(P_1, \dots, P_{i-1}, 0, P_{i+1}, \dots, P_m) \in X$, for any $1 \leq i \leq m$.

4. FORMULAS FOR THE GHWS

While the previous section provides an efficient method to compute the GHWs of square-free codes using the footprint bound, obtaining explicit formulas for some cases is still interesting, which is what we provide in this section. In what follows, we identify monomials and tuples via the map $x_1^{\alpha_1} \cdots x_m^{\alpha_m} \mapsto (\alpha_1, \dots, \alpha_m)$. Thus, we may say that a tuple divides another tuple, meaning that the corresponding monomial of the former divides the corresponding monomial of the latter. Similarly, we may interchangeably compute the shadow of a set of tuples or a set of monomials. We assume we are using degree lexicographic ordering when considering an ordering on the tuples. This means that, given $\alpha = (\alpha_1, \dots, \alpha_m)$, $\beta = (\beta_1, \dots, \beta_m)$, we have

$$\alpha > \beta \iff |\alpha| > |\beta| \text{ or } |\alpha| = |\beta| \text{ and } \alpha_i > \beta_i \text{ for the first index } i \text{ such that } \alpha_i \neq \beta_i.$$

For the following result, we consider the notation $[m] := \{1, \dots, m\}$.

Lemma 4.1. *Let $1 \leq d \leq m$ and $1 \leq r \leq \binom{m}{d}$ such that $1 \leq r \leq m+1-d$. Assume that*

$$(4.1) \quad \frac{n_{d+r-1}n_{d-1}}{n_i n_j} \leq \frac{n_{d+r-1} + n_{d-1} - 1}{n_i + n_j - 1},$$

for every $d \leq i < j \leq d+r-2$. Let $M \subset \mathbb{M}_d^S$ with $|M| = r$. Then

$$|\nabla_{\mathbb{X}}(M)| \geq \prod_{i=1}^{d-1} (n_i - 1) \prod_{i=d+r}^m n_i \left(\prod_{i=d}^{d+r-1} n_i - 1 \right).$$

Proof. We argue by induction on r . It is straightforward to check that the result is true for $r = 1$. Now we assume it is true for $r - 1$. Consider $M = \{a_1, \dots, a_r\}$, with $a_1 > a_2 > \dots > a_r$. Then

$$|\nabla_{\mathbb{X}}(M)| = |\nabla_{\mathbb{X}}(a_1, \dots, a_{r-1})| + |\nabla_{\mathbb{X}}(a_r) \setminus \nabla_{\mathbb{X}}(a_1, \dots, a_{r-1})|.$$

By the induction hypothesis, we have

$$(4.2) \quad |\nabla_{\mathbb{X}}(a_1, \dots, a_{r-1})| \geq \prod_{i=1}^{d-1} (n_i - 1) \prod_{i=d+r-1}^m n_i \left(\prod_{i=d}^{d+r-2} n_i - 1 \right).$$

For each $1 \leq i \leq r-1$, we choose $j_i \in \text{supp}(a_i) \setminus \text{supp}(a_r)$, and consider $J = \{j_1, \dots, j_{r-1}\}$ (note that we may have $j_i = j_\ell$ with $i \neq \ell$, so $|J| \leq r-1$). If we consider tuples whose entries corresponding to J are 0, those tuples belong to $B_{\mathbb{X}} \setminus \nabla_{\mathbb{X}}(a_1, \dots, a_{r-1})$. Then

$$(4.3) \quad |\nabla_{\mathbb{X}}(a_r) \setminus \nabla_{\mathbb{X}}(a_1, \dots, a_{r-1})| \geq \prod_{i \in \text{supp}(a_r)} (n_i - 1) \prod_{i \in [m] \setminus (\text{supp}(a_r) \cup J)} n_i.$$

We have that $|[m] \setminus (\text{supp}(a_r) \cup J)| \geq m - d - r + 1$. Let a_r be fixed, consider $\ell_1 < \dots < \ell_{r-1}$, the first $r-1$ elements in $[m] \setminus \text{supp}(a_r)$ (we can do this since $r-1 \leq m-d$), and let $u = \max\{i : i \in \text{supp}(a_r)\}$. Then we consider the following elements (recall that we treat monomials and tuples interchangeably)

$$a'_i = a_r \frac{x_{\ell_i}}{x_u}, \quad 1 \leq i \leq r-1.$$

We claim that these elements minimize (4.3), for this fixed a_r . This is equivalent to minimizing

$$\prod_{i \in [m] \setminus (\text{supp}(a_r) \cup J)} n_i.$$

Indeed, in this case we can choose $J = \{\ell_1, \dots, \ell_{r-1}\}$. Since $J \cap \text{supp}(a_r) = \emptyset$, this minimizes the number of indices considered in this product. Moreover, this also minimizes the product itself, since $n_1 \leq \dots \leq n_m$, and by construction, we are considering $\ell_1, \dots, \ell_{r-1}$ the smallest possible indices. Therefore, we have obtained

$$(4.4) \quad |\nabla_{\mathbb{X}}(a_r) \setminus \nabla_{\mathbb{X}}(a_1, \dots, a_{r-1})| \geq \prod_{i \in \text{supp}(a_r)} (n_i - 1) \prod_{i \in [m] \setminus (\text{supp}(a_r) \cup \{\ell_1, \dots, \ell_{r-1}\})} n_i.$$

Note that, since $a'_1, \dots, a'_{r-1}$ minimize the bound, then the bound obtained for $a'_1, \dots, a'_{r-1}$ also holds for $a_1, \dots, a_{r-1}$. Now we claim that

$$(4.5) \quad \prod_{i \in \text{supp}(a_r)} (n_i - 1) \prod_{i \in [m] \setminus (\text{supp}(a_r) \cup \{\ell_1, \dots, \ell_{r-1}\})} n_i \geq \prod_{i=1}^{d-1} (n_i - 1) \prod_{i=d+r}^m n_i (n_{d+r-1} - 1).$$

The number of factors on both sides is $m - r + 1$. In particular, we have d factors of the form $n_i - 1$, and $m - d - r + 1$ of the form n_i . Let t be the position, in a_r , of the first nonzero entry after the first zero entry. This would not make sense only for the greatest element of S_d but we are in the case where $r \geq 2$. Let $\tilde{a}_r$ be the m -tuple whose entries coincide with a_r , except in the t -th position, where now we have a zero, and in the $(t-1)$ -th position, where now we have a 1. Note that $\tilde{a}_r > a_r$. We write $\tilde{\ell}_1, \dots, \tilde{\ell}_{r-1}$

to denote the smallest possible indices which are not in the support of $\tilde{a}_r$. We will show that

$$\begin{aligned}
& \prod_{i \in \text{supp}(a_r)} (n_i - 1) \prod_{i \in [m] \setminus (\text{supp}(a_r) \cup \{\ell_1, \dots, \ell_{r-1}\})} n_i \\
&= \left(\prod_{i \in \text{supp}(a_r) \setminus \{t\}} (n_i - 1) \right) (n_t - 1) \prod_{i \in [m] \setminus (\text{supp}(a_r) \cup \{\ell_1, \dots, \ell_{r-1}\})} n_i \\
&\geq \left(\prod_{i \in \text{supp}(a_r) \setminus \{t\}} (n_i - 1) \right) (n_{t-1} - 1) \prod_{i \in [m] \setminus (\text{supp}(\tilde{a}_r) \cup \{\tilde{\ell}_1, \dots, \tilde{\ell}_{r-1}\})} n_i
\end{aligned}$$

Let $L = \text{supp}(a_r) \cup \{\ell_1, \dots, \ell_{r-1}\}$ and $\tilde{L} = \text{supp}(\tilde{a}_r) \cup \{\tilde{\ell}_1, \dots, \tilde{\ell}_{r-1}\}$. We know that $t \in L$, $t-1 \in \tilde{L}$ and $t-1 \in L$ if and only if $t \in \tilde{L}$. In the case where t and $t-1$ both belong to L and $\tilde{L}$, the inequality is clear because $L = \tilde{L}$. In case $t-1 \notin L$ then we have a factor in

$$\prod_{i \in [m] \setminus (\text{supp}(a_r) \cup \{\ell_1, \dots, \ell_{r-1}\})} n_i$$

which is equal to n_{t-1} , and replacing this factor by n_t we get

$$\prod_{i \in [m] \setminus (\text{supp}(\tilde{a}_r) \cup \{\tilde{\ell}_1, \dots, \tilde{\ell}_{r-1}\})} n_i.$$

Thus the inequality holds because $(n_t - 1)n_{t-1} \geq (n_{t-1} - 1)n_t$. By iterating this procedure, we move the first indices in $\text{supp}(a_r)$ to $\{1, \dots, d-2\}$, as long as the resulting tuple satisfies $\tilde{a}_r \leq L_r$, where $L_r = x_1 \cdots x_{d-1} x_{d+r-1}$ is the r th monomial with $\deg(L_r) = d$ in descending lexicographic order. Then $\tilde{a}_r$, seen as a monomial, is of the form $x_1 \cdots x_{d-2} x_i x_j$, with $i < j$. If $i = d-1$, then $j \geq d+r-1$ because $a_1 > \cdots > a_r$, which implies $L_r \geq a_r$, and therefore $\text{supp}(a_r)$ contains at least two indices larger than $d-2$. In that case, we directly obtain inequality (4.5). If $i \geq d$ and $j \leq d+r-1$, then, taking into account (4.1), we have $(n_{d-1} - 1)n_i n_j (n_{d+r-1} - 1) \leq n_{d-1}(n_i - 1)(n_j - 1)n_{d+r-1}$, which gives (4.5). Note that, for $j = d+r-1$, the inequality is always true and we do not need to have that case as an extra hypothesis. We finish the proof by noting that adding (4.2) and (4.5) we get the stated bound. $\square$

Remark 4.2. Condition (4.1) does not apply when $r \leq 2$. This condition implies a moderate growth for the sizes of the sets A_i , $d-1 \leq i \leq d+r-1$. In particular, if the sizes of those sets are equal, the condition is satisfied.

Corollary 4.3. Let $1 \leq d \leq m$ and $1 \leq r \leq m+1-d$. Let $\mathbb{X} = A_1 \times \cdots \times A_m$ be a Cartesian set such that $0 \in A_i$, $1 \leq i \leq m$, and assume that

$$\frac{n_{d+r-1} n_{d-1}}{n_i n_j} \leq \frac{n_{d+r-1} + n_{d-1} - 1}{n_i + n_j - 1},$$

for every $d \leq i < j \leq d + r - 2$. Then

$$d_r(C_d^{\mathbb{X}, S}) = \prod_{i=1}^{d-1} (n_i - 1) \prod_{i=d+r}^m n_i \left(\prod_{i=d}^{d+r-1} n_i - 1 \right).$$

Proof. By Theorem 3.2 and Corollary 4.1, it is enough to find $M \subset \mathbb{M}_d^S$ achieving the stated bound. Consider

$$S_d(r) = \{x_1 \cdots x_{d-1} x_d, x_1 \cdots x_{d-1} x_{d+1}, \dots, x_1 \cdots x_{d-1} x_{m-r}\}.$$

We use the inclusion-exclusion principle to compute $|\nabla_{\mathbb{X}}(S_d(r))|$. We have that

$$|\nabla_{\mathbb{X}}(x_1 \cdots x_{d-1} x_{d+i-1})| = (n_{d+i-1} - 1) \prod_{j=1}^{d-1} (n_j - 1) \prod_{j=d, j \neq d+i-1}^m n_j.$$

Similarly, we obtain that the number multiples of both $x_1 \cdots x_{d-1} x_{d+i-1}$ and $x_1 \cdots x_{d-1} x_{d+\ell-1}$ in $\Delta(I(\mathbb{X}))$ is

$$(n_{d+i-1} - 1)(n_{d+\ell-1} - 1) \prod_{j=1}^{d-1} (n_j - 1) \prod_{j=d, j \notin \{d+i-1, d+\ell-1\}}^m n_j.$$

In general, using the inclusion-exclusion principle, we get

$$\begin{aligned} |\nabla_{\mathbb{X}}(S_d(r))| &= \prod_{j=1}^{d-1} (n_j - 1) \sum_{A \subset \{d, \dots, d+r-1\}, A \neq \emptyset} (-1)^{|A|-1} \prod_{j \in A} (n_j - 1) \prod_{j=d, j \notin A}^m n_j \\ &= \prod_{j=1}^{d-1} (n_j - 1) \prod_{j=d+r}^m n_j \sum_{A \subset \{d, \dots, d+r-1\}, A \neq \emptyset} (-1)^{|A|-1} \prod_{j \in A} (n_j - 1) \prod_{j=d, j \notin A}^{d+r-1} n_j. \end{aligned}$$

The fact that

$$\sum_{A \subset \{d, \dots, d+r-1\}, A \neq \emptyset} (-1)^{|A|-1} \prod_{j \in A} (n_j - 1) \prod_{j=d, j \notin A}^{d+r-1} n_j = \prod_{j=d}^{d+r-1} n_j - 1$$

follows by expanding the product $\prod_{j=d}^{d+r-1} (n_j - (n_j - 1)) = 1$.

□

Corollary 4.4. Let $1 \leq d \leq m$ and $1 \leq r \leq m + 1 - d$. Assume that

$$\frac{n_{d+r-1} n_{d-1}}{n_i n_j} \leq \frac{n_{d+r-1} + n_{d-1} - 1}{n_i + n_j - 1},$$

for every $d \leq i < j \leq d + r - 2$. Then

$$d_r(C_{\leq d}^{\mathbb{X}, S}) = \prod_{i=1}^{d-1} (n_i - 1) \prod_{i=d+r}^m n_i \left(\prod_{i=d}^{d+r-1} n_i - 1 \right).$$

Proof. By Theorem 3.1, if we prove that, for any $M \subset \mathbb{M}_{\leq d}^S$ with $|M| = r$, we have that

$$|\nabla_{\mathbb{X}}(M)| \geq \prod_{i=1}^{d-1} (n_i - 1) \prod_{i=d+r}^m n_i \left(\prod_{i=d}^{d+r-1} n_i - 1 \right),$$

then we obtain the result by considering the same set of monomials as in Corollary 4.3. Let $M = \{a_1, \dots, a_r\}$. If $|a_j| < d$, for some $1 \leq j \leq r$, then

$$|\nabla_{\mathbb{X}}(M)| \geq |\nabla_{\mathbb{X}}(x^{a_j})| \geq \prod_{i=1}^{|a_j|} (n_i - 1) \prod_{i=|a_j|+1}^m n_i \geq \prod_{i=1}^{d-1} (n_i - 1) \prod_{i=d+r}^m n_i \left(\prod_{i=d}^{d+r-1} n_i - 1 \right).$$

Indeed, the bound for $|\nabla_{\mathbb{X}}(x^{a_j})|$ follows from Lemma 4.1. For the last inequality, factoring out the common terms, we have that the inequality holds if and only if

$$\prod_{i=|a_j|+1}^{d+r-1} n_i \geq \prod_{i=|a_j|+1}^{d-1} (n_i - 1) \left(\prod_{i=d}^{d+r-1} n_i - 1 \right),$$

which holds because $\prod_{i=|a_j|+1}^{d-1} n_i > \prod_{i=|a_j|+1}^{d-1} (n_i - 1)$ and $\prod_{i=d}^{d+r-1} n_i > \left(\prod_{i=d}^{d+r-1} n_i - 1 \right)$. $\square$

Similar results to Corollary 4.3 have been obtained for toric codes in [16, 19]. In that case, $\mathbb{X} = (\mathbb{F}_q^*)^m$, and in principle Theorem 3.2 does not apply with equality. However, it still applies as a lower bound, and it turns out to be sharp for some of the cases considered in [16, 19], where this is proven by considering appropriate families of polynomials achieving the bound. Our approach of first proving that the footprint bound is sharp and then computing the set of monomials by giving a minimal bound does not generally work for that case, as we show in the next example, where the footprint bound is not sharp.

Example 4.5. Consider $q = 3$, $m = 5$, $d = 2$, $r = 3$, and $\mathbb{X} = (\mathbb{F}_q^*)^m$. Using the package from [23, 24], we see that $d_3(C_d^{\mathbb{X}, S}) = 16$. On the other hand, one can check that $|\nabla(S_2(3))| = |\nabla(x_1x_2, x_1x_3, x_1x_4)| = 14$. Thus, the footprint bound is not sharp in this case. This fact was observed for the minimum distance when $d > m/2$ in [16].

5. CODES OVER THE PROJECTIVE SPACE

In this section, we see how some of the results corresponding to the codes $C_d^{\mathbb{X}, S}$ can be translated to evaluation codes over the projective space. Consider $\mathbb{P}^m(\mathbb{F}_q)$, the rational points of the m -dimensional projective space, and fix a set of representatives, which we denote by P^m . Then we can define

$$C_d^{\mathbb{P}, S}(m) := \langle \text{ev}_{P^m}(x^\alpha) : \alpha \in S_d(m+1) \rangle.$$

A different choice of representatives P^m would lead to a monomially equivalent code. The length of the code is $|P^m| = \frac{q^{m+1}-1}{q-1}$, and the dimension is $\binom{m+1}{d}$. If we define

$\mathbb{A}_0^m = \mathbb{A}^m(\mathbb{F}_q) \setminus \{0\}$, then we can consider

$$C_d^{\mathbb{A}_0^m, S}(m) := \langle \text{ev}_{\mathbb{A}_0^m}(x^\alpha) : \alpha \in S_d(m) \rangle.$$

Let $\xi \in \mathbb{F}_q$ be a primitive element. We denote $\xi \cdot P^m := \{\xi Q : Q \in P^m\}$. Then we have (for example, see [21])

$$(5.1) \quad \mathbb{A}^{m+1}(\mathbb{F}_q) = P^m \cup \xi \cdot P^m \cup \xi^2 \cdot P^m \cup \dots \cup \xi^{q-2} \cdot P^m \cup \{(0, \dots, 0)\}.$$

In what follows, we will assume that we have fixed an ordering for the points of P^m , which also fixes an ordering for the points of $\xi^i \cdot P^m$, and we will assume we order the points of $\mathbb{A}^{m+1}(\mathbb{F}_q)$ as in (5.1). The relation between $C_d^{\mathbb{P}, S}(m)$ and $C_d^{\mathbb{A}_0^m, S}(m)$ is similar to that between homogeneous Reed-Muller codes and projective Reed-Muller codes, e.g., see [4, 18].

Lemma 5.1. *Let $1 \leq d \leq m+1$, and $\xi \in \mathbb{F}_q$ a primitive element. Then*

$$C_d^{\mathbb{A}_0^{m+1}, S}(m+1) = (1, \xi^d, \xi^{2d}, \dots, \xi^{d(q-2)}) \otimes C_d^{\mathbb{P}, S}(m).$$

As a consequence, $\dim(C_d^{\mathbb{A}_0^{m+1}, S}(m+1)) = \dim(C_d^{\mathbb{P}, S}(m))$, and, for every $1 \leq r \leq \binom{m+1}{d}$, we have $d_r(C_d^{\mathbb{A}_0^{m+1}, S}(m+1)) = (q-1)d_r(C_d^{\mathbb{P}, S}(m))$.

Proof. Let $f \in \mathbb{F}_q[x_0, \dots, x_m]_d$ be a homogeneous polynomial of degree d . Then, taking (5.1) into account, we have

$$\begin{aligned} \text{ev}_{\mathbb{A}_0^m}(f) &= (\text{ev}_{P^m}(f), \text{ev}_{\xi \cdot P^m}(f), \text{ev}_{\xi^2 \cdot P^m}(f), \dots, \text{ev}_{\xi^{q-2} \cdot P^m}(f)) \\ &= (\text{ev}_{P^m}(f), \xi^d \text{ev}_{P^m}(f), \xi^{2d} \text{ev}_{P^m}(f), \dots, \xi^{d(q-2)} \text{ev}_{P^m}(f)) \\ &= (1, \xi^d, \xi^{2d}, \dots, \xi^{d(q-2)}) \otimes \text{ev}_{P^m}(f). \end{aligned}$$

□

Remark 5.2. For $d = 1$, the codes $C_d^{\mathbb{P}, S}(m)$ are non-degenerate. But for $1 < d \leq m+1$, these codes are degenerate, since all the polynomials of $S_d(m+1)$ vanish at any point with $m+2-d$ zero entries, or, equivalently, at every point with Hamming weight lower than or equal to $d-1$. After removing these coordinates, the length of $C_d^{\mathbb{P}, S}(m)$ would be

$$\frac{q^{m+1} - 1}{q - 1} - \sum_{i=1}^{d-1} \binom{m+1}{i}.$$

From the connection given in Lemma 5.1, we can directly obtain the GHWs of the codes $C_d^{\mathbb{A}_0^m, S}(m)$ and $C_d^{\mathbb{P}, S}(m)$ for some cases.

Corollary 5.3. *Let $1 \leq d \leq m$ and $1 \leq r \leq m+1-d$. We have that*

$$d_r(C_d^{\mathbb{A}_0^m, S}(m)) = (q-1)^{d-1} q^{m-d-r+1} (q^r - 1).$$

As a consequence, for $1 \leq d \leq m+1$ and $1 \leq r \leq m+2-d$, we have

$$d_r(C_d^{\mathbb{P}, S}(m)) = (q-1)^{d-2} q^{m-d-r+2} (q^r - 1).$$

Proof. From Corollary 4.3 and Remark 4.2 we obtain that

$$d_r(C_d^{\mathbb{A}^{m+1},S}) = (q-1)^{d-1}q^{m-d-r+1}(q^r-1).$$

Now we note that $d_r(C_d^{\mathbb{A}^{m+1},S}) = d_r(C_d^{\mathbb{A}^m,S}(m))$, since all the homogeneous polynomials of degree d vanish at the point $(0, \dots, 0)$, implying that the puncturing at the corresponding coordinate preserves the support. The result for $C_d^{\mathbb{P},S}(m)$ follows from Lemma 5.1. $\square$

DECLARATIONS

Conflict of interest. The authors declare no conflict of interest.

REFERENCES

- [1] A. I. Barbero and C. Munuera. The weight hierarchy of hermitian codes. *SIAM Journal on Discrete Mathematics*, 13(1):79–104, 2000.
- [2] M. Bardet, V. Dragoi, A. Otmani, and J.-P. Tillich. Algebraic properties of polar codes from a new polynomial formalism. In *2016 IEEE International Symposium on Information Theory (ISIT)*, pages 230–234, 2016.
- [3] P. Beelen, M. Datta, and S. R. Ghorpade. A combinatorial approach to the number of solutions of systems of homogeneous polynomial equations over finite fields. *Mosc. Math. J.*, 22(4):565–593, 2022.
- [4] T. P. Berger. Automorphism groups of homogeneous and projective Reed-Muller codes. *IEEE Trans. Inform. Theory*, 48(5):1035–1045, 2002.
- [5] M. Boguslavsky. On the number of solutions of polynomial systems. *Finite Fields Appl.*, 3(4):287–299, 1997.
- [6] E. Camps, H. H. López, G. L. Matthews, and E. Sarmiento. Polar decreasing monomial-Cartesian codes. *IEEE Trans. Inform. Theory*, 67(6):3664–3674, 2021.
- [7] E. Camps-Moreno, I. García-Marco, H. H. López, I. Márquez-Corbella, E. Martínez-Moro, and E. Sarmiento. On the generalized Hamming weights of hyperbolic codes. *Journal of Algebra and Its Applications*, 23(07):2550062, 2024.
- [8] E. Camps-Moreno, H. H. López, G. L. Matthews, and R. San-José. The weight hierarchy of decreasing norm-trace codes. *Des. Codes Cryptogr.*, 93(7):2873–2894, July 2025.
- [9] D. A. Cox, J. Little, and D. O’Shea. *Ideals, varieties, and algorithms*. Undergraduate Texts in Mathematics. Springer, Cham, fourth edition, 2015. An introduction to computational algebraic geometry and commutative algebra.
- [10] G. Feng, K. Tzeng, and V. Wei. On the generalized hamming weights of several classes of cyclic cods. *IEEE Transactions on Information Theory*, 38(3):1125–1130, 1992.
- [11] M. González-Sarabia, D. Jaramillo, and R. H. Villarreal. On the generalized Hamming weights of certain Reed-Muller-type codes. *An. Științ. Univ. “Ovidius” Constanța Ser. Mat.*, 28(1):205–217, 2020.
- [12] E. Gorla and F. Salizzoni. Generalized weights of convolutional codes. *IEEE Transactions on Information Theory*, 69(8):4927–4943, 2023.
- [13] P. Heijnen and R. Pellikaan. Generalized hamming weights of q-ary reed-muller codes. *IEEE Transactions on Information Theory*, 44(1):181–196, 1998.
- [14] T. Helleseth, T. Klove, and O. Ytrehus. Generalized hamming weights of linear codes. *IEEE Transactions on Information Theory*, 38(3):1133–1140, 1992.

- [15] H. Janwa and A. Lal. On the generalized hamming weights of cyclic codes. *IEEE Transactions on Information Theory*, 43(1):299–308, 1997.
- [16] D. Jaramillo, M. Vaz Pinto, and R. H. Villarreal. Evaluation codes and their basic parameters. *Des. Codes Cryptogr.*, 89(2):269–300, 2021.
- [17] J. Martínez-Bernal, M. A. Valencia-Bucio, and R. H. Villarreal. Generalized Hamming weights of projective Reed-Muller-type codes over graphs. *Discrete Math.*, 343(1):111639, 9, 2020.
- [18] O. Moreno, I. M. Duursma, J.-P. Cherdieu, and A. Edouard. Cyclic subcodes of generalized Reed-Muller codes. *IEEE Trans. Inform. Theory*, 44(1):307–311, 1998.
- [19] N. Patanker and S. K. Singh. Generalized Hamming weights of toric codes over hypersimplices and squarefree affine evaluation codes. *Adv. Math. Commun.*, 17(3):626–643, 2023.
- [20] J. Rosenthal and E. York. On the generalized hamming weights of convolutional codes. *IEEE Transactions on Information Theory*, 43(1):330–335, 1997.
- [21] R. San-José. A recursive construction for projective Reed-Muller codes. *IEEE Trans. Inform. Theory*, 70(12):8511–8523, 2024.
- [22] R. San-José. About the generalized Hamming weights of matrix-product codes. *Comput. Appl. Math.*, 44(4):Paper No. 186, 2025.
- [23] R. San-José. An algorithm for computing generalized Hamming weights and the Sage package GHWs. *ACM Transactions on Mathematical Software*. <https://doi.org/10.1145/3773284>, 2025.
- [24] R. San-José. GHWs: A Sage package for computing the generalized Hamming weights of a linear code. GitHub repository. Available online: <https://github.com/RodrigoSanJose/GHWs>, 2025.
- [25] C. E. Shannon. A mathematical theory of communication. *Bell System Tech. J.*, 27:379–423, 623–656, 1948.
- [26] H. Stichtenoth and C. Voss. Generalized hamming weights of trace codes. *IEEE Transactions on Information Theory*, 40(2):554–558, 1994.
- [27] G. van der Geer and M. van der Vlugt. Generalized hamming weights of Melas codes and dual Melas codes. *SIAM Journal on Discrete Mathematics*, 7(4):554–559, 1994.
- [28] G. van der Geer and M. van der Vlugt. On generalized hamming weights of bch codes. *IEEE Transactions on Information Theory*, 40(2):543–546, 1994.
- [29] R. H. Villarreal. *Monomial algebras*. Monographs and Research Notes in Mathematics. CRC Press, Boca Raton, FL, second edition, 2015.
- [30] V. Wei and K. Yang. On the generalized hamming weights of product codes. *IEEE Transactions on Information Theory*, 39(5):1709–1713, 1993.
- [31] V. K. Wei. Generalized Hamming weights for linear codes. *IEEE Trans. Inform. Theory*, 37(5):1412–1418, 1991.

(Cicero Carvalho) DEPARTMENT OF MATHEMATICS, UNIVERSITY OF UBERLANDIA, UBERLANDIA, BRAZIL

Email address: `cicero@ufu.br`

(Hiram H. López) DEPARTMENT OF MATHEMATICS, VIRGINIA TECH, BLACKSBURG, VA USA

Email address: `hhlopez@vt.edu`

(Rodrigo San-José) DEPARTMENT OF MATHEMATICS, VIRGINIA TECH, BLACKSBURG, VA USA. *Previous address:* IMUVA-MATHEMATICS RESEARCH INSTITUTE, UNIVERSIDAD DE VALLADOLID, 47011 VALLADOLID (SPAIN)

Email address: `rsanjose@vt.edu`