Some bounds for the relative generalized Hamming weights of some evaluation codes

Manuel González Sarabia

Abstract

In this paper we find some bounds for the relative generalized Hamming weights of some codes parameterized by a set of monomials of the same degree. Also we compare the relative generalized Hamming weights of the codes $C_X(d)$ and $C_{X'}(d)$ when X' is embedded in X. We use these results to obtain some lower bounds for the relative generalized Hamming weights of the codes parameterized by the edges of any connected bipartite graph with bipartition (V_1, V_2) and where $|V_1| = n_1$, $|V_2| = n_2$, in terms of the relative generalized Hamming weights of the codes associated to the projective tori $\mathbb{T}_{n_1-1}$ and $\mathbb{T}_{n_2-1}$.

1 Introduction

The relative generalized Hamming weights (RGHW from now on) are introduced in [12]. They are a natural generalization of the generalized Hamming weights introduced by Wei in [18]. The study of the RGHW is motivated because of their usefulness to protect messages from an adversary in the wire–tap channel of type II with illegitimate parties. Some properties of the RGHW of q–ary codes are described in [10] and they are computed in the cases of almost all 4–dimensional linear codes and their subcodes. Moreover some equivalences, inequalities and bounds are given in [20]. Recently the behavior of the RGHW of one point algebraic geometric codes is analyzed in [1]. In the case of Hermitian codes, the RGHW are often much larger than the corresponding

generalized Hamming weights. In this paper we consider the case of some evaluation codes, known as parameterized codes, which are defined in [15]. Parameterized codes have been studied in several cases (see [2], [3], [4], [5], [6], [11], [13], [14], [16], [17]). In fact in [7] there are some bounds for the generalized Hamming weights of some parameterized codes. We generalize these results to the RGHW of this kind of codes. The contents of this paper are as follows.

In Section 2 we introduce some basic definitions in order to understand the main results of this work.

In Section 3 we establish some lower bounds for the RGHW of the codes $C_X(d)$ which are parameterized by some monomials of the same degree α. These bounds depend on the RGHW of codes associated to the projective torus and the length of the codes $C_X(d)$ (see Theorem 3.2).

In Section 4 we describe the relationships among the RGHW of the codes $C_X(d)$ and the RGHW of the codes $C_{X'}(d)$ when X' is embedded in X (see Theorem 4.2). These inequalities are useful because they work when we consider codes parameterized by the edges of a simple graph $\mathcal{G}$ and the corresponding codes parameterized by the edges of any subgraph $\mathcal{G}'$. Finally we study the case of codes parameterized by the edges of any connected bipartite graph.

2 Preliminaries

Let $K = \mathbb{F}_q$ be a finite field with q elements and from now on we denote the cardinality of any set X as $|X|$. Also let $L = K[Z_1, \ldots, Z_n] = \oplus_{d \geq 0} L_d$ be a polynomial ring with n variables and the natural grading. Consider a set of m monomials of the form

$$\mathbf{Z}^{a_1}, \ldots, \mathbf{Z}^{a_m}, \tag{1}$$

where $\mathbf{Z}^{a_i} = Z_1^{a_{i1}} \cdots Z_n^{a_{in}}$ and a_{ij} is a non–negative integer for all $i = 1, \ldots, m$, $j = 1, \ldots, n$. The set X given by

$$X = \{[(\mathbf{t}^{a_1}, \ldots, \mathbf{t}^{a_m})] \in \mathbb{P}^{m-1} : t_i \in K^*\}, \tag{2}$$

where $\mathbf{t}^{a_i} = t_1^{a_{i1}} \cdots t_n^{a_{in}}$ for all $i = 1, \ldots, m$ and $K^* := K \setminus \{0\}$, is a toric set parameterized by the monomials (1). Moreover let $S = K[X_1, \ldots, X_m] = \oplus_{d \geq 0} S_d$ be another polynomial ring also with the natural grading. Let $X = \{P_1, \ldots, P_{|X|}\}$ be the toric set given in (2) and consider the evaluation map

$$\mathrm{ev}_d : S_d \longrightarrow K^{|X|},$$

$$f \mapsto \left(\frac{f(P_1)}{X_1^d(P_1)}, \ldots, \frac{f(P_{|X|})}{X_1^d(P_{|X|})} \right).$$

This evaluation map is a linear map between the K–vector spaces S_d and $K^{|X|}$. The parameterized code of order d associated to the toric set X, or the code of order d parameterized by the monomials (1), is the image of the evaluation map ev_d, and it is denoted by $C_X(d)$. Therefore

$$C_X(d) = \left\{ \left(\frac{f(P_1)}{X_1^d(P_1)}, \ldots, \frac{f(P_{|X|})}{X_1^d(P_{|X|})} \right) : f \in S_d \right\}. \qquad (3)$$

It is a well known fact that the dimension of the code $C_X(d)$ is given by the Hilbert function $H_X(d)$ (see [15]) and, by definition, its length is $|X|$. A projective torus in $\mathbb{P}^{n-1}$ is a toric set parameterized by the monomials $Z_1, \ldots, Z_n$, that is

$$\mathbb{T}_{n-1} = \{[(t_1, \ldots, t_n)] \in \mathbb{P}^{n-1} : t_i \in K^* \text{ for all } i\}, \qquad (4)$$

and the parameterized code of order d associated to this projective torus is the subspace of $K^{|\mathbb{T}_{n-1}|}$ given by

$$C_{\mathbb{T}_{n-1}}(d) = \left\{ \left(\frac{g(R_1)}{Z_1^d(R_1)}, \ldots, \frac{g(R_{|\mathbb{T}_{n-1}|})}{Z_1^d(R_{|\mathbb{T}_{n-1}|})} \right) : g \in L_d \right\}, \qquad (5)$$

where $\mathbb{T}_{n-1} = \{R_1, \ldots, R_{|\mathbb{T}_{n-1}|}\}$ and $|\mathbb{T}_{n-1}| = (q-1)^{n-1}$.

Furthermore let C be an $[s, k]$ linear code (it means that C is a subspace of K^s and its dimension is k). Let $\mathcal{B}$ be a subset of K^s. The support of this set is

$$\mathrm{supp}\,(\mathcal{B}) = \{i : \text{there exists } (b_1, \ldots, b_s) \in \mathcal{B} \text{ such that } b_i \neq 0\}.$$

Moreover if C_1 is a subspace of C with $\dim C_1 = k_1$, the jth relative generalized Hamming weight of C and C_1 is given by

$$M_j(C, C_1) = \min\{\, |\mathrm{supp}\,(D)| : D \text{ is a subspace of } C,$$
$$\dim(D) = j,\, D \cap C_1 = \{\vec{0}\}\}. \qquad (6)$$

for all $j = 1, \ldots, k - k_1$. In the case that $C_1 = \{\vec{0}\}$, we obtain the jth generalized Hamming weight of C,

$$d_j(C) = \min\{\, |\mathrm{supp}\,(D)| : D \text{ is a subspace of } C,\, \dim(D) = j\}.$$

That is, $d_j(C) = M_j(C, \{\vec{0}\})$ for all $j = 1, \ldots, k$. It is worth recalling that $d_1(C)$ is the minimum distance of the linear code C.

On the other hand let $\mathcal{G}$ be a connected bipartite graph with a bipartition of its vertex set given by (V_1, V_2), where $|V_1| = n_1$ and $|V_2| = n_2$. If every vertex in V_1 is joined to every vertex in V_2, then $\mathcal{G}$ is called a complete bipartite graph and it is denoted by $\mathcal{K}_{n_1, n_2}$. A spanning subgraph of a graph $\mathcal{G}$ is a subgraph containing all the vertices of $\mathcal{G}$.

3 Comparison with the projective torus

We use the notation introduced in [7]. Let $X = \{P_1, \ldots, P_{|X|}\}$ be the toric set parameterized by the monomials (1), but in this section we consider the case where all the monomials are of the same degree α. The following two maps were introduced in [7] and they will be useful in this paper:

$$\mu : \mathbb{T}_{n-1} \longrightarrow X,$$
$$[(t_1, \ldots, t_n)] \mapsto [(\mathbf{t}^{a_1}, \ldots, \mathbf{t}^{a_m})], \tag{7}$$

and

$$\tau : S_d \longrightarrow L_{\alpha d},$$
$$f(X_1, \ldots, X_m) \mapsto f(\mathbf{Z}^{a_1}, \ldots, \mathbf{Z}^{a_m}). \tag{8}$$

We notice that μ is an epimorphism of multiplicative groups and that $|\ker \mu| = \frac{(q-1)^{n-1}}{|X|}$. Also τ is a linear map between the linear spaces S_d and $L_{\alpha d}$. With the help of these maps we define the following function:

$$\theta : C_X(d) \longrightarrow C_{\mathbb{T}_{n-1}}(\alpha d),$$
$$\Lambda_f \mapsto \Omega_f, \tag{9}$$

where

$$\Lambda_f := \left(\frac{f(P_1)}{X_1^d(P_1)}, \ldots, \frac{f(P_{|X|})}{X_1^d(P_{|X|})} \right), \quad \Omega_f := \left(\frac{\tau(f)(R_1)}{Z_1^{\alpha d}(R_1)}, \ldots, \frac{\tau(f)(R_{|\mathbb{T}_{n-1}|})}{Z_1^{\alpha d}(R_{|\mathbb{T}_{n-1}|})} \right),$$

and $f \in S_d$.

Lemma 3.1. *Let θ be the map given in (9). θ is an injective linear map and if $\mathcal{B}$ is a subset of $C_X(d)$ then*

$$|\operatorname{supp}(\theta(\mathcal{B}))| = |\ker \mu| \cdot |\operatorname{supp}(\mathcal{B})|.$$

Proof. This is an immediate consequence of [7, Lemma 3.3]. □

Theorem 3.2. *Let X be a toric set parameterized by a set of monomials of the same degree α. Let C_1 be a linear subspace of $C_X(d)$ with $\dim C_1 = k_1$. Then the jth relative generalized Hamming weight of $C_X(d)$ and C_1 is bounded by*

$$M_j(C_X(d), C_1) \geq \left\lceil \frac{|X| \cdot M_j(C_{\mathbb{T}_{n-1}}(\alpha d), \theta(C_1))}{(q-1)^{n-1}} \right\rceil,$$

for all $j = 1, \ldots, H_X(d) - k_1$.

Proof. Let D be a subspace of $C_X(d)$ with $\dim D = j$, $D \cap C_1 = \{\vec{0}\}$ and such that

$$M_j(C_X(d), C_1) = |\operatorname{supp}(D)|.$$

Let $D_1 = \theta(D)$. D_1 is a subspace of $C_{\mathbb{T}_{n-1}}(\alpha d)$ and $\dim D_1 = \dim D = j$. Moreover

$$D_1 \cap \theta(C_1) = \theta(D) \cap \theta(C_1) = \theta(D \cap C_1) = \theta(\{\vec{0}\}) = \{\vec{0}\}.$$

By using Lemma 3.1 we obtain that

$$|\operatorname{supp}(D_1)| = |\operatorname{supp}(\theta(D))| = |\ker \mu| \cdot |\operatorname{supp}(D)|.$$

Therefore

$$M_j(C_{\mathbb{T}_{n-1}}(\alpha d), \theta(C_1)) \leq |\operatorname{supp}(D_1)| = |\ker \mu| \cdot |\operatorname{supp}(D)|,$$

and due to the fact that $|\ker \mu| = \frac{(q-1)^{n-1}}{|X|}$ then

$$M_j(C_X(d), C_1) = |\operatorname{supp}(D)| \geq \frac{|X| \cdot M_j(C_{\mathbb{T}_{n-1}}(\alpha d), \theta(C_1))}{(q-1)^{n-1}},$$

and the claim follows. $\qquad\square$

4   Comparison between embedded sets

Let $X \subseteq \mathbb{P}^{m-1}$ and $X' \subseteq \mathbb{P}^{s-1}$, with $s < m$, be two toric sets parameterized by some monomials in such a way that X' is embedded in X and $|X| = \eta \cdot |X'|$. We know that $\eta = \ker \pi$ where π is the map

$$\pi : X \longrightarrow X',$$
$$[(\mathbf{t}^{a_1}, \ldots, \mathbf{t}^{a_m})] \mapsto [(\mathbf{t}^{a_1}, \ldots, \mathbf{t}^{a_s})].$$

We also use the notation introduced in [7]. As in the last section, let $X = \{P_1, \ldots, P_{|X|}\}$. Also let $X' = \{Q_1, \ldots, Q_{|X'|}\}$. If f is an element of $K[X_1, \ldots, X_s]_d$ then we define $\Delta_f \in C_{X'}(d)$ as

$$\Delta_f := \left(\frac{f(Q_1)}{X_1^d(Q_1)}, \ldots, \frac{f(Q_{|X'|})}{X_1^d(Q_{|X'|})} \right).$$

Now consider the map

$$\Phi : C_{X'}(d) \longrightarrow C_X(d),$$
$$\Delta_f \mapsto \Lambda_f, \tag{10}$$

where Λ_f was defined in Section 3.

Lemma 4.1. *Let Φ be the map given by (10). Φ is an injective linear map and if $\mathcal{S}'$ is a subset of $C_{X'}(d)$ then*

$$| \, supp \, (\Phi(\mathcal{S}'))| = \eta \cdot | \, supp \, (\mathcal{S}')|.$$

Proof. The claim follows immediately from [7, Lemma 4.1]. $\qquad\square$

Theorem 4.2. *Let $X \subseteq \mathbb{P}^{m-1}$ and $X' \subseteq \mathbb{P}^{s-1}$, with $s < m$, be two toric sets parameterized by some monomials in such a way that X' is embedded in X and $|X| = \eta|X'|$. Let C' be a subspace of $C_{X'}(d)$ with $\dim C' = k'$. Therefore the jth relative generalized Hamming weight of $C_{X'}(d)$ and C' is bounded by*

$$M_j(C_{X'}(d), C') \geq \left\lceil \frac{1}{\eta} \cdot M_j(C_X(d), \Phi(C')) \right\rceil,$$

for all $j = 1, \ldots, H_{X'}(d) - k'$.

Proof. Let E be a subspace of $C_{X'}(d)$ with $\dim E = j$, $E \cap C' = \{\vec{0}\}$ and such that

$$M_j(C_{X'}(d), C') = | \operatorname{supp}(E)|.$$

Notice that $\Phi(E)$ is a subspace of $C_X(d)$, $\dim \Phi(E) = \dim E = j$ and

$$\Phi(E) \cap \Phi(C') = \Phi(E \cap C') = \Phi(\{\vec{0}\}) = \{\vec{0}\}.$$

Then, by using Lemma 4.1, we obtain that

$$M_j(C_X(d), \Phi(C')) \leq | \operatorname{supp}(\Phi(E))| = \eta \cdot | \operatorname{supp}(E)|.$$

Therefore

$$M_j(C_{X'}(d), C') = | \operatorname{supp}(E)| \geq \frac{1}{\eta} \cdot M_j(C_X(d), \Phi(C')),$$

and the claim follows. $\qquad\square$

Remark 4.3. *Theorem 3.2 recovers [7, Theorem 3.4] if we take $C_1 = \{\vec{0}\}$. Analogously when we take $C' = \{\vec{0}\}$ in Theorem 4.2, we get [7, Theorem 4.2].*

Corollary 4.4. *Let $\mathcal{G}$ be a connected bipartite graph with bipartition (V_1, V_2), where $|V_1| = n_1$ and $|V_2| = n_2$. Let X' be the toric set parameterized by its edges. If C' is a subspace of $C_{X'}(d)$ then*

$$M_j(C_{X'}(d), C') \geq M_j(C_{\mathbb{T}_{n_1-1}}(d) \otimes C_{\mathbb{T}_{n_2-1}}(d), \Phi(C')),$$

for all $j = 1, \ldots, H_{X'}(d) - k'$ and where $\otimes$ means the tensor product of linear spaces.

Proof. If $\mathcal{G}$ is a connected bipartite graph with bipartition (V_1, V_2), and where $|V_1| = n_1$, $|V_2| = n_2$ then it is a spanning subgraph of the complete bipartite graph $\mathcal{K}_{n_1, n_2}$ (see [9]). If X is the toric set parameterized by the edges of $\mathcal{K}_{n_1, n_2}$ then X' is embedded in X and (see [15, Corollary 3.8]) $|X| = |X'|$. Moreover it is known that (see [2])

$$C_X(d) = C_{\mathbb{T}_{n_1-1}} \otimes C_{\mathbb{T}_{n_2-1}}.$$

The claim follows immediately from Theorem 4.2. $\square$

Remark 4.5. *If we take C' as the zero subspace and $j = 1$ in Corollary 4.4, we recover the lower bound for the minimum distance given in [17, Theorem 3.6]: Let $\mathcal{G}$ be a connected bipartite graph with bipartition (V_1, V_2), where $|V_1| = n_1$ and $|V_2| = n_2$. Let X' be the toric set parameterized by its edges. Then*

$$d_1(C_{X'}(d)) \geq d_1(C_{\mathbb{T}_{n_1-1}}(d)) \cdot d_1(C_{\mathbb{T}_{n_2-1}}(d)),$$

and the minimum distances of the right side can be computed by using [16, Theorem 3.5]. If we take C' as the zero subspace, $j = 2$ in Corollary 4.4, and the formula for the second generalized Hamming weight of product codes (see [19, Theorem 3]) we obtain the following lower bound: Let $\mathcal{G}$ be a connected bipartite graph with bipartition (V_1, V_2), where $|V_1| = n_1$ and $|V_2| = n_2$. Let X' be the toric set parameterized by its edges. Then

$$d_2(C_{X'}(d)) \geq \min\{d_1(C_{\mathbb{T}_{n_1-1}}(d)) \cdot d_2(C_{\mathbb{T}_{n_2-1}}(d)),$$
$$d_2(C_{\mathbb{T}_{n_1-1}}(d)) \cdot d_1(C_{\mathbb{T}_{n_2-1}}(d))\}.$$

Example 4.6. Consider the cycle C_6, which is a connected bipartite graph. It can be seen as a spanning subgraph of the complete bipartite graph $\mathcal{K}_{3,3}$ (see Figure 1). Let $K = \mathbb{F}_q$ a finite field with q elements and let X be the toric set associated to the edges of the complete bipartite graph $\mathcal{K}_{3,3}$. Then

$$X = \{[(t_1t_2, t_2t_3, t_3t_4, t_4t_5, t_5t_6, t_6t_1, t_1t_4, t_3t_6, t_5t_2)] \in \mathbb{P}^8 : t_i \in K^*\}.$$

Moreover if X' is the toric set associated to the edges of the cycle C_6 then

$$X' = \{[(t_1t_2, t_2t_3, t_3t_4, t_4t_5, t_5t_6, t_6t_1)] \in \mathbb{P}^5 : t_i \in K^*\}.$$

Therefore X' is embedded in X and $|X| = |X'| = (q-1)^4$ (because C_6 and $\mathcal{K}_{3,3}$ are connected bipartite graphs and by using [15, Corollary 3.8]).

If we use Remark 4.5 we obtain that

$$d_1(C_{X'}(d)) \geq (d_1(C_{\mathbb{T}_2}(d)))^2.$$

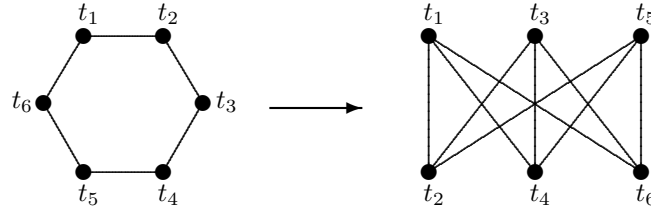With the help of Macaulay2 (see [8]) we compute the following results.

Figure 1: C_6 as a spanning subgraph of the complete bipartite graph $\mathcal{K}_{3,3}$.

- If $q = 3$, $d_1(C_{X'}(1)) \geq 4$. The exact value of the minimum distance is 6.

- If $q = 5$, $d_1(C_{X'}(1)) \geq 144$. The exact value of the minimum distance is 186.

- If $q = 5$, $d_1(C_{X'}(2)) \geq 64$.

On the other hand, by using again the Remark 4.5, we obtain that

$$d_2(C_{X'}(d)) \geq d_1(C_{\mathbb{T}_2}(d)) \cdot d_2(C_{\mathbb{T}_2}(d)).$$

Also with the help of Macaulay2 we notice that some lower bounds are as follows.

- If $q = 3$, $d_2(C_{X'}(1)) \geq 6$ and $d_2(C_{X'}(2)) \geq 2$.

- If $q = 5$, $d_2(C_{X'}(1)) \geq 180$ and $d_2(C_{X'}(2)) \geq 88$.

- If $q = 7$, $d_2(C_{X'}(1)) \geq 1050$ and $d_2(C_{X'}(2)) \geq 696$.

References

[1] O. Geil, S. Martin, R. Matsumoto, D. Ruano, and Y. Luo, Relative generalized Hamming weights of one–point algebraic geometric codes, *IEEE Trans. Inf. Theory* **60** (10) (2014) 5938–5949.

[2] M. González-Sarabia, C. Rentería, Evaluation Codes Associated to Complete Bipartite Graphs, *Int. J. Algebra* **2** (2008) 163-170.

[3] M. González Sarabia, J. Nava Lara, C. Rentería Márquez, and E. Sarmiento Rosales, Parameterized Codes over cycles, *An. Stiint. Univ. Ovidius Constanta Ser. Mat.* **21** (3) (2013) 241–255.

[4] M. González Sarabia, C. Rentería Márquez, and E. Sarmiento Rosales, Parameterized Codes over some Embedded Sets and their Applications to Complete Graphs, *Math. Commun.* **18** (2013) 337–391.

[5] M. González Sarabia, C. Rentería Márquez, and A. J. Sánchez Hernández, Minimum distance of some evaluation codes, *Appl. Algebra Engrg. Comm. Comput.* **24** (2013) 95–106.

[6] M. González Sarabia, C. Rentería Márquez, and E. Sarmiento Rosales, Projective parameterized linear codes, *An. Stiint. Univ. Ovidius Constanta Ser. Mat.* **23** (2) (2015).

[7] M. González Sarabia, and C. Rentería Márquez, Generalized Hamming weights and some parameterized codes. Submitted for publication (2015).

[8] D.R. Grayson, M. Stillman: *Macaulay2* (Available via anonymous ftp from math.uiuc.edu 1996).

[9] F. Harary, *Graph Theory* (Addison–Wesley, 1971).

[10] Z. Liu, W. Chen, and Y. Luo, The relative generalized Hamming weight of linear q–ary codes and their subcodes, *Des. Codes Cryptogr.* **48** (2) (2008) 111–123.

[11] H. López Hiram, C. Rentería Márquez and R.H. Villarreal, Affine cartesian codes, *Des. Codes Cryptogr.* **71** (2014) 5–19.

[12] Y. Luo, C. Mitrpant, A.J.H. Vinck, and K. Chen, Some new characters on the wire–tap channel of type II, *IEEE Trans. Inf. Theory* **51** (3) (2005) 1222–1229.

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

[14] J. Neves and M. Vaz Pinto, Vanishing ideals over complete multipartite graphs, *J. Pure Appl. Algebra* **218** (6) (2014) 1084–1094.

[15] 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) 81–104.

[16] E. Sarmiento, M. Vaz Pinto and R. H. Villarreal, The minimum distance of parameterized codes on projective tori, *Appl. Algebra Engrg. Comm. Comput.* **22** (4) (2011) 249–264.

[17] M. Vaz Pinto, and R.H. Villarreal, The degree and regularity of vanishing ideals of algebraic toric sets over finite fields, *Comm. Algebra* **41** (9) (2013) 3376–3396.

[18] V.K. Wei, Hamming weights for linear codes, *IEEE Trans. Inf. Theory* **37** (1991) 1412–1418.

[19] V.K. Wei, and K Yang, On the generalized Hamming weights of product codes, *IEEE Trans. Inf. Theory* **39** (5) (1993) 1709–1713.

[20] Z. Zhuang, Y. Luo, and B. Dai, Code constructions and existence bounds for relative generalized Hamming weight, *Des. Codes Cryptogr.* **69** (3) (2013) 275–297.

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