ISIT'2013 1569716935

On the Dimension of Graph Codes with Reed–Solomon Component Codes

Peter Beelen, Tom Høholdt and Fernando Piñero
Department of Applied Mathematics and Computer Science
Technical University of Denmark
Email: {p.beelen, t.hoeholdt, f.pinero}@mat.dtu.dk

Jørn Justesen
Email: jorn@justesen.info

***Abstract*—We study a class of graph based codes with Reed–Solomon component codes as affine variety codes. We give a formulation of the exact dimension of graph codes in general. We give an algebraic description of these codes which makes the exact computation of the dimension of the graph codes easier.**

I. Introduction

In 1981 Tanner [1] introduced a construction of error-correcting codes based on bipartite graphs. Since then results on their dimension, minimum distance and decoding have been obtained. In this paper we consider some specific bipartite expander graphs based on finite geometries and codes constructed from these graphs. This class of graph codes was introduced in [2] by some of the authors. We use techniques from algebra to compute the dimension when this class of graph codes has Reed–Solomon component codes.

In this paper q denotes a prime power, $\mathbb{F}_q$ the field with q elements and a code C is a linear subspace of $\mathbb{F}_q^n$ for some n. The parameter n is the length of the code. We are particularly interested in graph codes, whose definition we now give.

Definition 1 ([3]): Let G be an n-regular bipartite graph with vertex set $V = V_1 \cup V_2$ and edge set E of cardinality $\#E = N$. For $v \in V$, we assume an ordering on the set $E(v)$, of the edges incident with v, given by ϕ_v, where ϕ_v is a bijection from $\{1, 2, \ldots, n\}$ to $E(v)$. Furthermore we define $(c)_{E(v)} := (c_{\phi_v(1)}, c_{\phi_v(2)}, \ldots, c_{\phi_v(n)}) \in \mathbb{F}_q^n$.

Let C_1 and C_2 be codes of length n over $\mathbb{F}_q$. We define the graph code

$$(G, C_1 : C_2) :=$$
$$\{(c_e) \in \mathbb{F}_q^N | \forall v \in V_1 : \ (c)_{E(v)} \in C_1, \forall v \in V_2 : \ (c)_{E(v)} \in C_2\}.$$

Observe that

$$(G, C_1 : C_2) = (G, C_1 : \mathbb{F}_q^n) \cap (G, \mathbb{F}_q^n : C_2). \tag{1}$$

The labeling functions ϕ_v are important, since, in general, the parameters of the graph codes depend on them.

Theorem 1 ([4]): Let G be a n-regular bipartite graph. Let C_1, C_2 be codes of length n over $\mathbb{F}_q$ of rates r_1 and r_2 respectively. Then the rate of $(G, C_1 : C_2)$ is at least $r_1 + r_2 - 1$.

Theorem 2: Let G be an n-regular bipartite graph with N edges. Let C_1, C_2 be codes of length n over $\mathbb{F}_q$ of dimensions k_1 and k_2 respectively. Then

$$\dim\ (G, C_1 : C_2) = \frac{N}{n}(k_1 + k_2 - n) + \dim\ (G, C_1^\perp : C_2^\perp)$$

Proof: For each vertex $v \in V_1$ we get k_1 independent parity check equations for $C_1^\perp$ involving the edges in $E(v)$ only. The resulting Nk_1/n parity check equations of a code of the form $(G, C_1^\perp : \mathbb{F}_q^n)$ are independent because the edge sets $E(v)$ and $E(u)$ are disjoint for $u \neq v$. Therefore the dimension of the code $(G, C_1^\perp : \mathbb{F}_q^n)$ is $N(n-k_1)/n$. The code $(G, \mathbb{F}_q^n : C_2^\perp)$ gives $N(n-k_2)/n$ parity check equations. The parity check equations which are not independent are those corresponding to $(G, C_1^\perp : \mathbb{F}_q^n) \cap (G, \mathbb{F}_q^n : C_2^\perp)$ which is the same code as $(G, C_1^\perp : C_2^\perp)$. ■

We will study graph codes over the following graph.

Definition 2: We define the bipartite graph $\Gamma := (V_1 \cup V_2, E)$ by:

$$V_1 := \{(x, y) \mid x, y \in \mathbb{F}_q\},\ V_2 := \{(a, b) \mid a, b \in \mathbb{F}_q\}$$

and

$$E := \{((x, y), (a, b)) \mid (x, y) \in V_1, (a, b) \in V_2, ax + b - y = 0\}.$$

Note that Γ is the point line incidence graph of the affine plane over $\mathbb{F}_q$ without the vertical lines and that Γ is q-regular.

II. Affine Variety Codes

We start this section with a short review of material in [5]. Let $\mathbb{F}_q[X_1, X_2, \ldots, X_m]$ be the polynomial ring in m variables over $\mathbb{F}_q$ and $\mathcal{P} = \{P_1, P_2, \ldots, P_N\} \subseteq \mathbb{F}_q^m$ be a set of N points in $\mathbb{F}_q^m$. Denote by $I(\mathcal{P})$ the ideal in $\mathbb{F}_q[X_1, X_2, \ldots, X_m]$ consisting of the polynomials which vanish at all points of $\mathcal{P}$. We define $R := \mathbb{F}_q[X_1, X_2, \ldots, X_m]/I(\mathcal{P})$ and the evaluation map,

$$\begin{array}{rccc} Ev_{\mathcal{P}} : & R & \rightarrow & \mathbb{F}_q^N \\ & f & \mapsto & (f(P_1), f(P_2), \ldots, f(P_N)). \end{array}$$

The map $Ev_{\mathcal{P}}$ is an isomorphism of vector spaces.

Definition 3: Let L be an $\mathbb{F}_q$-linear subspace of R. We define the *affine variety code* $C(I(\mathcal{P}), L) := Ev_{\mathcal{P}}(L)$.

Since L is an $\mathbb{F}_q$-linear subspace of R and $Ev_{\mathcal{P}}$ is an isomorphism, we have that

$$\dim C(I(\mathcal{P}), L) = \dim L. \tag{2}$$

Lemma 1: Let $\mathcal{P} \subset \mathbb{F}_q^m$, $R = \mathbb{F}_q[X_1, \ldots, X_m]/I(\mathcal{P})$ as before. Suppose that L and M are two $\mathbb{F}_q$-linear subspaces of R. Then

$$C(I(\mathcal{P}), L) \cap C(I(\mathcal{P}), M) = C(I(\mathcal{P}), L \cap M).$$

Proof: If $c \in C(I(\mathcal{P}), L) \cap C(I(\mathcal{P}), M)$, then $f \in L$ and $g \in M$ exist such that $Ev_{\mathcal{P}}(f) = c = Ev_{\mathcal{P}}(g)$. Since $Ev_{\mathcal{P}}$ is injective, this implies that $f = g$ and therefore that $f \in L \cap M$. Therefore $c \in C(I(\mathcal{P}), L \cap M)$. The inclusion $C(I(\mathcal{P}), L) \cap C(I(\mathcal{P}), M) \supseteq C(I(\mathcal{P}), L \cap M)$ is clear. ∎

Reed–Solomon codes are an example of affine variety codes with $m = 1$ and $\mathcal{P} = \{\alpha_1, \alpha_2, \ldots, \alpha_q\} = \mathbb{F}_q$. Then $I(\mathcal{P}) = \langle X_1^q - X_1 \rangle$. For $L(k) := \{f \in \mathbb{F}_q[X_1] \mid \deg\ f < k\}$, where k is an integer between 0 and q, we obtain the affine variety code $C(I(\mathcal{P}), L(k))$ which is a Reed–Solomon code denoted by $RS(k)$. The i-th coordinate of $Ev_{\mathcal{P}}(f)$ is $f(\alpha_i)$. Note that $RS(k)^{\perp} = RS(q-k)$.

We will look at our graph codes as affine variety codes. In order to do this we need to state the labeling functions and construct two auxilliary graph codes as affine variety codes. The two auxilliary codes and equation (1) will give the description of our graph codes as affine variety codes. Now for the set of evaluation points of the affine variety codes, we identify E, the set of edges of Γ, with $\{(x, y, a, b) \in \mathbb{F}_q^4 \mid ax + b - y = 0\}$.

Theorem 3: We define $I(\Gamma) := \langle AX + B - Y, X^q - X, Y^q - Y, A^q - A, B^q - B \rangle$. The ideal $I(\Gamma)$ equal to the ideal of polynomials which vanish on E, $I(E)$.

Proof: The elements of $I(\Gamma)$ vanish at all the points of E. Therefore $I(\Gamma) \subseteq I(E)$. This implies that

$$\begin{aligned} \dim \mathbb{F}_q[X, Y, A, B]/I(\Gamma) &\geq \dim \mathbb{F}_q[X, Y, A, B]/I(E) \\ &= \#E = q^3. \end{aligned}$$

Now let $f(X, Y, A, B) \in \mathbb{F}_q[X, Y, A, B]$. Since $Y - AX - B \in I(\Gamma)$, we have that $f(X, Y, A, B) + I(\Gamma) = g(X, Y, A) + I(\Gamma)$ for a certain g. Using that $X^q - X, Y^q - Y, A^q - A \in I(\Gamma)$, we write $g(X, Y, A)$ as an $\mathbb{F}_q$-linear combination of monomials in $\{X^i Y^j A^l \mid 0 \leq i, j, l \leq q - 1\}$. Therefore $\dim \mathbb{F}_q[X, Y, A, B]/I(\Gamma) \leq q^3$. This implies that

$$\dim \mathbb{F}_q[X, Y, A, B]/I(\Gamma) = \dim \mathbb{F}_q[X, Y, A, B]/I(E)$$

and therefore $I(\Gamma) = I(E)$. ∎

To construct graph codes over Γ we use the following labeling functions:

$$\phi_{(x,y)}(i) := (x, y, \alpha_i, y - x\alpha_i), \quad (x, y) \in V_1,$$

$$\phi_{(a,b)}(i) := (\alpha_i, a\alpha_i + b, a, b), \quad (a, b) \in V_2.$$

We describe the codes $(\Gamma, RS(k) : \mathbb{F}_q^q)$ and $(\Gamma, \mathbb{F}_q^q : RS(k))$ as affine variety codes.

Definition 4: Let $k \leq q$ and $R = \mathbb{F}_q[X, Y, A, B]/I(\Gamma)$.

$$L_1(k) := \langle \{X^{i_1} Y^{i_2} A^{j_1} B^{j_2} \mid 0 \leq j_1 + j_2 \leq k - 1\} \rangle_{\mathbb{F}_q} \subseteq R,$$

$$L_2(k) := \langle \{X^{i_1} Y^{i_2} A^{j_1} B^{j_2} \mid 0 \leq i_1 + i_2 \leq k - 1\} \rangle_{\mathbb{F}_q} \subseteq R.$$

We emphasize that the elements of $L_1(k)$ and $L_2(k)$ are elements of the quotient ring R. In particular the monomials $X^{i_1} Y^{i_2} A^{j_1} B^{j_2}$ occurring in the above definition are not necessarily linearly independent when viewed as elements of R, because we are working modulo the ideal $I(\Gamma)$. We can use $L_1(k)$ and $L_2(k)$ to describe the graph code $(\Gamma, RS(k) : RS(k))$ as an affine variety code. By equation (1) we have the equality

$$(\Gamma, RS(k) : RS(k)) = (\Gamma, RS(k) : \mathbb{F}_q^q) \cap (\Gamma, \mathbb{F}_q^q : RS(k)).$$

Theorem 4: We have $C(I(\Gamma), L_1(k)) = (\Gamma, RS(k) : \mathbb{F}_q^q)$ and $C(I(\Gamma), L_2(k)) = (\Gamma, \mathbb{F}_q^q : RS(k))$. Moreover

$$(\Gamma, RS(k) : RS(k)) = C(I(\Gamma), L_1(k) \cap L_2(k)).$$

Proof: Let $f(X, Y, A, B) \in L_1(k)$. We define $c = (f(x, y, a, b))_{(x,y,a,b) \in E}$. For $(x, y, a, b) \in E$ we have $f(x, y, a, b) = f(x, y, a, y - ax)$. For $(x, y) \in V_1$, the univariate polynomial $p(A) := f(x, y, A, y - Ax)$ has degree at most $k - 1$ in A. Therefore the codeword $(p(\alpha_1), p(\alpha_2), \ldots, p(\alpha_q))$ is a codeword in $RS(k)$. On the other hand $(c)_{E((x,y))} = (f(x, y, \alpha_1, y - \alpha_1 x), \ldots, f(x, y, \alpha_q, y - \alpha_q x))$. We see that the value of the polynomial $p(A)$ at $A = \alpha_i$ is equal to the i-th coordinate of $(c)_{E((x,y))}$. Therefore $c \in (\Gamma, RS(k) : \mathbb{F}_q^q)$ implying $C(I(\Gamma), L_1(k)) \subseteq (\Gamma, RS(k) : \mathbb{F}_q^q)$.

By a similar reasoning as in the proof of Corollary 2, one obtains that $\dim(\Gamma, RS(k) : \mathbb{F}_q^q) = q^2 k$. Therefore, using equation (2), the equality $C(I(\Gamma), L_1(k)) = (\Gamma, RS(k) : \mathbb{F}_q^q)$ follows once we show that $\dim L_1(k) \geq q^2 k$. Now let (i_1, i_2, j_1) be a triple of integers satisfying the constraints $0 \leq i_1 < q$, $0 \leq i_2 < q$ and $0 \leq j_1 < q$. Clearly there are q^3 possibilities for the triple. It is well known from the theory of Gröbner basis ([6] Chapter 5, Sec. 2) that the q^3 codewords $Ev_{\mathbb{F}_q^3}(X^{i_1} Y^{i_2} A^{j_1}) \in \mathbb{F}_q^{q^3}$ are linearly independent. Since $\{(x, y, a) \mid (x, y, a, b) \in E\} = \mathbb{F}_q^3$, this implies that the $q^2 k$ codewords $Ev_E(X^{i_1} Y^{i_2} A^{j_1}) \in C(I(\Gamma), L_1(k))$ with $0 \leq i_1 < q$, $0 \leq i_2 < q$ and $0 \leq j_1 < k$ also are linearly independent. This shows that $\dim L_1(k) \geq q^2 k$, which as mentioned above, implies that $C(I(\Gamma), L_1(k)) = (\Gamma, RS(k) : \mathbb{F}_q^q)$. Similarly one shows that $C(I(\Gamma), L_2(k)) = (\Gamma, \mathbb{F}_q^q : RS(k))$.

The final statement of the theorem is a consequence of the above and Lemma 1. ∎

We wish to emphasize the result that the graph code $(\Gamma, RS(k) : RS(k))$ is the affine variety code obtained by evaluating some polynomials in the variables X, Y, A and B at the points defined by E. The polynomials which evaluate to codewords in $(\Gamma, RS(k) : RS(k))$ are those polynomials $f(X, Y, A, B)$ such that for any $x, y \in \mathbb{F}_q$, $f(x, y, A, y - Ax)$ is a univariate polynomial of degree $< k$ and for any $a, b \in \mathbb{F}_q$, $f(X, aX + b, a, b)$ is a univariate polynomial of degree $< k$. However, as we do need to take into account the nonzero polynomials which vanish at the elements of E, it is preferable to work with the elements of R instead.

III. Dimension of the graph code $(\Gamma, RS(k) : RS(k))$.

In this section we will exploit Theorem 4 to get a handle on the dimension of the graph code $(\Gamma, RS(k) : RS(k))$. In

principle we can combine equation (2) and Theorem 4 and obtain that

$$\dim\ (\Gamma, RS(k) : RS(k)) = \dim\ L_1(k) \cap L_2(k). \quad (3)$$

However, the dimension of $L_1(k) \cap L_2(k)$ is tricky to calculate. We will use the theory of Gröbner bases as a tool to facilitate this calculation. For the background material on Gröbner basis one may consult [6]. We start by computing a Gröbner basis for $I(\Gamma)$ under certain orderings.

Definition 5: Let m be a positive integer and I an ideal of $\mathbb{F}_q[X_1, X_2, \ldots, X_m]$. Further denote by δ be a monomial ordering. We define the *normal basis* (or footprint) $\Delta_\delta(I)$ of I under δ as the set of monomials which are not divisible by the leading term (under δ) of any element of I.

Footprints are important because any element of $\mathbb{F}_q[X_1, X_2, \ldots, X_m]$ can uniquely be written as an $\mathbb{F}_q$-linear combination of monomials in $\Delta_\delta(I)$ and an element from I. This means that the monomials of $\Delta_\delta(I)$ give rise to a basis of the ring $\mathbb{F}_q[X_1, X_2, \ldots, X_m]/I$. In particular in case $I = I(\Gamma)$, the footprint $\Delta_\delta(I(\Gamma))$ under a monomial ordering δ gives rise to a basis of the ring $R = \mathbb{F}_q[X, Y, A, B]/I(\Gamma)$. Since we know that R (as an $\mathbb{F}_q$-vector space) has dimension q^3, this means that $\#\Delta_\delta(I(\Gamma)) = q^3$ for any monomial ordering δ. We will consider the following two monomial orderings:

Definition 6: We denote degree graded reverse lexicographical order with $A > B > X > Y$ by δ_1 and degree graded reverse lexicographical order with $X > Y > A > B$ by δ_2.

The Gröbner basis of $I(\Gamma)$ can be computed explicitly. We will show the following polynomials are part of a Gröbner basis for $I(\Gamma)$ under δ_1 and δ_2.

Definition 7: We define the following polynomials:

$$f_i^{(1)} := X^i(Y - B)^{q-i} - A^{q-1-i}(Y - B),$$
$$f_i^{(2)} := A^i(Y - B)^{q-i} - X^{q-1-i}(Y - B).$$

For convenience Δ_1 denotes the footprint of $I(\Gamma)$ under δ_1 and Δ_2 denotes the footprint of $I(\Gamma)$ under δ_2. We first find the footprints of $I(\Gamma)$ for these two monomial orderings. To ease the description as well as for future use, we introduce the following sets of monomials:

$$\Delta_1^{(1)} := \{X^{i_1}Y^{i_2}B^{j_2} \mid i_2 < q \text{ and } i_1 + j_2 < q\}. \quad (4)$$

$$\Delta_1^{(2)} := \{Y^{i_2}A^{j_1}B^{j_2} \mid i_2 < q \text{ and } j_1 + j_2 < q\}. \quad (5)$$

$$\Delta_2^{(1)} := \{X^{i_1}Y^{i_2}B^{j_2} \mid j_2 < q \text{ and } i_1 + i_2 < q\}. \quad (6)$$

$$\Delta_2^{(2)} := \{Y^{i_2}A^{j_1}B^{j_2} \mid j_2 < q \text{ and } i_2 + j_1 < q\}. \quad (7)$$

Lemma 2: We have

$$\Delta_1 = \Delta_1^{(1)} \cup \Delta_1^{(2)} \text{ and } \Delta_2 = \Delta_2^{(1)} \cup \Delta_2^{(2)}.$$

Proof: We will only show the statement for the monomial ordering δ_1. A similar proof holds for δ_2. By definition, we know that the polynomials $X^q - X$, $Y^q - Y$, $A^q - A$, $B^q - B$ and $AX + B - Y$ are in $I(\Gamma)$. Furthermore, for any i between 1 and $q - 1$ a direct computation shows that the polynomials $f_i^{(1)}$ and $f_i^{(2)}$ vanish for any $(x, y, a, b) \in E$, therefore they are elements of $I(\Gamma)$. The leading term of $f_i^{(1)}$ is X^iB^{q-i} under δ_1. Likewise the leading term of $f_i^{(2)}$ is A^iB^{q-i} under δ_1. By the definition of a footprint, this implies that $\Delta_1 \subset \Delta_1^{(1)} \cup \Delta_1^{(2)}$. However, it is not hard to see that $\#\Delta_1^{(1)} \cup \Delta_1^{(2)} = q^3$. Note though that the sets $\Delta_1^{(1)}$ and $\Delta_1^{(2)}$ are not disjoint, but have an intersection of cardinality q^2 consisting of monomials of the form $Y^{i_2}B^{j_2}$. Since $\#\Delta_1 = q^3$, the lemma follows. ∎

Lemma 3: The polynomials $f_i^{(1)}$ and $f_i^{(2)}$, along with the field equations on X, Y, A, B and the incidence relation $Y - AX - B$ are a Gröbner basis for $I(\Gamma)$ under δ_1 and δ_2.

Proof: The polynomials $f_i^{(1)}$ and $f_i^{(2)}$, along with the field equations on X, Y, A, B and the incidence relation $Y - AX - B$ are a basis for $I(\Gamma)$. Since there are q^3 monomials not divisible by a leading term of this basis under δ_1, then the basis is a Gröbner basis under δ_1. A similar argument holds for δ_2. ∎

Now that we have found a Gröbner basis for $I(\Gamma)$ under δ_1 and δ_2, we will find subsets of the footprints Δ_1 and Δ_2 such that the monomials of these subsets evaluate to the codes $C(I(\Gamma), L_1(k))$ and $C(I(\Gamma), L_1(k))$. These monomial basis will give us a lower bound on the dimension of $(\Gamma, RS(k) : RS(k))$.

Definition 8: We define

$$M_1(k) := \{X^{i_1}Y^{i_2}A^{j_1}B^{j_2} \in \Delta_1 \mid j_1 + j_2 < k\} \text{ and}$$
$$M_2(k) := \{X^{i_1}Y^{i_2}A^{j_1}B^{j_2} \in \Delta_2 \mid i_1 + i_2 < k\}.$$

Lemma 4: Let $0 \leq k \leq q$, then

$$\#M_1(k) = \#M_2(k) = q^2k.$$

Moreover if $k \leq q/2$, then

$$\#(M_1(k) \cap M_2(k)) = k^3.$$

Proof: This follows from a simple counting argument. ∎

Theorem 5: Let $k \leq q/2$, then we have

$$\dim(\Gamma, RS(k) : RS(k)) \geq k^3$$

and, for $q/2 < k \leq q$

$$\dim(\Gamma, RS(k) : RS(k)) \geq k^3 + k(q - k)(2k - q).$$

Proof: The second bound follows from the first one by using Theorem 2 and the observation that $RS(k)^\perp = RS(q - k)$. Since the cosets of monomials in Δ_1 are independent in R, the cosets of monomials in $M_1(k)$ evaluate to a basis of $C(I(\Gamma), L_1(k))$. Likewise the cosets of monomials in $M_2(k)$ evaluate to a basis of $C(I(\Gamma), L_2(k))$. Since $k \leq q/2$, there are k^3 monomials in $M_1(k) \cap M_2(k)$. The cosets of the k^3 monomials in $M_1(k) \cap M_2(k)$ are k^3 linearly independent elements in $L_1(k) \cap L_2(k)$. Therefore $\dim L_1(k) \cap L_2(k) \geq k^3$. By equation (3) the theorem follows. ∎

Theorem 5 offers a significant improvement on the dimension of the graph codes $(\Gamma, RS(k) : RS(k))$ over the standard rate bound. If $1 \leq k \leq \frac{q}{2}$ the standard rate bound is 0.

Otherwise, the rate bound $r_1 + r_2 - 1$ gives the lower bound $q^2(2k-q)$. Our bound surpasses it by $(q-k)^3$.

To find the dimension of the graph codes $(\Gamma, RS(k) : RS(k))$, we must find the dimension of the space $\langle L_1(k) + L_2(k)\rangle$ as a linear subspace of R. As we have found monomial sets $M_1(k)$ and $M_2(k)$ which evaluate to the same codes as $L_1(k)$ and $L_2(k)$ it suffices to compute the dimension of the space generated by the cosets of $M_1(k)$ and $M_2(k)$. Since $M_1(k)$ and $M_2(k)$ are subsets of footprints of $I(\Gamma)$ it suffices to find $\#(M_1(k) \cup M_2(k))$ and the dimension of the space $I(\Gamma) \cap \langle M_1(k) \cup M_2(k)\rangle_{\mathbb{F}_q}$.

We first define a set of elements of $I(\Gamma)$ which turn out to generate the $\mathbb{F}_q$-linear space $I(\Gamma) \cap \langle \Delta_1 \cup \Delta_2\rangle_{\mathbb{F}_q}$. Then we partition the elements of $I(\Gamma)$ into subspaces, such that the ideal elements in different spaces have disjoint support. We then prove that if an ideal element is in $I(\Gamma) \cap \langle M_1(k) \cup M_2(k)\rangle_{\mathbb{F}_q}$, then it is a linear combination of some disjoint subspaces. We then prove that if a polynomial in this subclass is in $I(\Gamma) \cap \langle M_1(k) \cup M_2(k)\rangle_{\mathbb{F}_q}$, then certain matrices of binomial coefficients must have a nonzero element in its right kernel. Finally we prove that these binomial matrices have full rank, which implies that $I(\Gamma) \cap \langle M_1(k) \cup M_2(k)\rangle_{\mathbb{F}_q} = \{0\}$.

Definition 9: Let $M \in \Delta_1$. We define

$$f_M := M - r_M,$$

where r_M is the remainder of M under multivariate polynomial division by the Gröbner basis of $I(\Gamma)$ under δ_2.

Lemma 5: $I(\Gamma) \cap \langle \Delta_1 \cup \Delta_2\rangle_{\mathbb{F}_q} = \langle f_M | M \in \Delta_1 \setminus \Delta_2\rangle_{\mathbb{F}_q}$.

Proof: If $f \in I(\Gamma) \cap \langle \Delta_1 \cup \Delta_2\rangle_{\mathbb{F}_q}$, then $f = g - r_g$ for some $g \in \langle \Delta_1\rangle_{\mathbb{F}_q}$. If $g = \Sigma c_M\ M$, where $c_M \in \mathbb{F}_q$, then $f = \Sigma c_M\ f_M$. The reverse implication follows from the definition of f_M. ∎

Lemma 6: The $\mathbb{F}_q$-linear space $I(\Gamma) \cap \langle M_1(k) \cup M_2(k)\rangle_{\mathbb{F}_q}$ is a subspace of the space generated by the ideal elements f_M where $M \in M_1(k) \setminus \Delta_2$ and $deg_X\ M < k$.

Proof: The $\mathbb{F}_q$-linear space $I(\Gamma) \cap \langle M_1(k) \cup M_2(k)\rangle_{\mathbb{F}_q}$ is a subspace of the $\mathbb{F}_q$-linear space $I(\Gamma) \cap \langle \Delta_1 \cup \Delta_2\rangle_{\mathbb{F}_q}$. If $f \in I(\Gamma) \cap \langle M_1(k) \cup M_2(k)\rangle_{\mathbb{F}_q}$, then $f = \Sigma_{M \in \Delta_1 \setminus \Delta_2} c_M f_M$. The leading term of f under δ_1 belongs to $M_1(k) \setminus M_2(k)$ and the leading term of f under δ_2 belongs to $M_2(k) \setminus M_1(k)$. Since the leading term of f_M under δ_1 is M, if $M \in \Delta_1 \setminus M_1(k)$, then $c_M = 0$. Since the leading term of f under δ_1 is a monomial satisfying $deg_X\ M = i_1$ and $deg_Y\ M + deg_B\ M = i_2 + j_2$, the leading term of f under δ_2 must also satisfy the two equalities. Therefore $i_1 < k$. ∎

We use Lemma 6 to get a lower bound on the dimension of $C(I(\Gamma), \langle M_1(k) + M_2(k)\rangle_{\mathbb{F}_q})$, which gives an upper bound on $\dim\ (\Gamma, RS(k) : RS(k))$. However we find the true dimension of the vector space $I(\Gamma) \cap \langle M_1(k) \cup M_2(k)\rangle_{\mathbb{F}_q}$ which gives the true dimension of the graph codes. To do this, we exploit the structure of the ideal elements f_M. We can compute f_M explicitly. However, we need the following facts: if $M = X^{i_1} Y^{i_2} B^{j_2}$, then

$$f_M = X^{i_1} f_1(Y, B) + X^{i_1} f_2(Y, B) + A^{q-1-i_1} f_3(Y, B) \quad (8)$$

where f_1, f_2 and f_3 are homogeneous polynomials in Y and B of degrees $i_2 + j_2$, $i_2 + j_2 - (q-1)$ and $i_2 + j_2 + i_1 - q + 1$ respectively and f_2 is a multiple of B. Furthermore,

$$f_1(Y, B) + B^{q-i_1} f_2(Y, B) = q_{i_2, q-i_1}(Y, B)(Y - B)^{q-i_1} \quad (9)$$

Likewise if $M = A^{j_1} Y^{i_2} B^{j_2}$, then

$$g_M = A^{j_1} g_1(Y, B) + A^{j_1} g_2(Y, B) + X^{q-1-j_1} g_3(Y, B) \quad (10)$$

where g_1, g_2 and g_3 are homogeneous polynomials in Y and B of degrees $i_2 + j_2$, $i_2 + j_2 - (q-1)$ and $i_2 + j_2 + j_1 - q + 1$ respectively and g_2 is a multiple of B. Furthermore,

$$g_1(Y, B) + B^{q-1} g_2(Y, B) = q_{i_2, q-j_1}(Y, B)(Y - B)^{q-j_1} \quad (11)$$

where $q_{i,j}(Y, B)$ is a homogeneous polynomial in Y and B of degree $i - j$.

Definition 10: We partition the elements of Δ_1 using the sets defined as follows:

$$M_1(k)^{(1)}_{i,a} := \{X^i Y^{i_2} B^{j_2} \in M_1(k) \mid i_2 + j_2 = a\}$$

$$M_1(k)^{(2)}_{i,a} := \{A^i Y^{i_2} B^{j_2} \in M_1(k) \mid i_2 + j_2 = a\}$$

The sets $M_1(k)^{(1)}_{i,a}$ and $M_1(k)^{(2)}_{i,a}$ allow us to separate the elements of $I(\Gamma) \cap \langle M_1(k) \cup M_2(k)\rangle_{\mathbb{F}_q}$ into subspaces of polynomials with disjoint support. This separation will help us in finding the elements, if any, of $I(\Gamma) \cap \langle M_1(k) \cup M_2(k)\rangle_{\mathbb{F}_q}$.

Lemma 7: Let S_1, S_2 be two distinct monomial subsets of the form $M_1(k)^{(1)}_{i,a}$ or $M_1(k)^{(2)}_{i,a}$ as defined in Definition 10 where $i < k \leq q/2$. Let $f = \Sigma_{M \in S_1} c_M f_M$ and $g = \Sigma_{M \in S_2} d_M f_M$. Then f and g have disjoint support.

Proof: If $M \in S_1 = M_1(k)^{(1)}_{i_1,a}$, then equation (8) implies that f can be written as $X^{i_1} f_4(Y, B) + X^{i_1} f_5(Y, B) + A^{q-1-i_1} f_6(Y, B)$ where f_4, f_5 and f_6 are homogeneous polynomials in Y and B of degrees a, $a-(q-1)$ and $a+i_1-q+1$ respectively. If $S_2 = M_1(k)^{(1)}_{i_1',a'}$ and either $i_1' \neq i_1$ or $a \neq a'$ then g has no term in its support in common with f. Therefore we assume $S_2 = M_1(k)^{(2)}_{j_1,a'}$. However, equation (10) implies $q - 1 - i_1 = j_1$. The hypothesis of the lemma states $j_1 < k$. However since $j_1 + i_1 = q - 1$, $j_1 > q - 1 - k \geq q/2$. Therefore f and g have disjoint support. Similarly, the case $S_1 = M_1(k)^{(2)}_{j_1,a}$ follows. ∎

Lemma 8: Suppose $f \in \langle f_M\rangle_{\mathbb{F}_q}$, $M \in M_1(k)^{(1)}_{i_1,a}$. Furthermore suppose f is equal to $X^{i_1} f_4(Y, B) + X^{i_1} f_5(Y, B) + A^{q-1-i_1} f_6(Y, B)$ where f_4, f_5 and f_6 are homogeneous polynomials in Y and B of degrees a, $a-(q-1)$ and $a+i_1-q+1$. If $f \in \langle M_1(k) \cup M_2(k)\rangle_{\mathbb{F}_q}$, then $f_4(Y, B) + B^{q-1} f_5(Y, B)$ is a multiple of $(Y - B)^{q-i_1}$ whose terms satisfy either $deg_B \geq q$ or $deg_B < k$.

Proof: Equation (9) implies that $h(Y, B)(Y - B)^{q-i_1} = f_4(Y, B) + B^{q-1} f_5(Y, B)$ where $h(Y, B)$ is a certain homogeneous polynomial. Since $X^{i_1}(f_4(Y, B) + f_5(Y, B)) \in \langle M_1(k) \cup M_2(k)\rangle_{\mathbb{F}_q}$, the polynomial $h(Y, B)$ has the desired properties. ∎

Lemma 9: Suppose $f \in \langle f_M\rangle_{\mathbb{F}_q}$, $M \in M_1(k)^{(2)}_{j_1,a}$. Furthermore suppose f is equal $A^{j_1} g_4(Y, B) + A^{j_1} g_5(Y, B) +$

$X^{q-1-j_1}g_6(Y,B)$ where g_4, g_5 and g_6 are homogeneous polynomials in Y and B of degrees a, $a-(q-1)$ and $a+j_1-q+1$. If $f \in \langle M_1(k) \cup M_2(k) \rangle_{\mathbb{F}_q}$, then $g_4(Y,B)+B^{q-1}g_5(Y,B)$ is a multiple of $(Y-B)^{q-j_1}$ whose terms satisfy either $deg_B \geq q$ or $deg_B < k - j_1$.

Proof: The proof is the same as in lemma 8. ∎

Lemma 8 shows that a nonzero element of $I(\Gamma) \cap \langle M_1(k) \cup M_2(k) \rangle_{\mathbb{F}_q}$, gives a multiple of $(Y-B)^{q-i_1}$ which has no monomials in the middle. We will show that in the cases relevant to the graph code $(\Gamma, RS(k) : RS(k))$, we can not find a multiple of $(Y-B)^l$ such that we find a nonzero element of $I(\Gamma)$ contained in $\langle M_1(k) \cup M_2(k) \rangle_{\mathbb{F}_q}$. This will give a closed formula for the dimension in these cases.

Lemma 10: Let $h(Y,B) = \Sigma_{j=0}^{m} h_j Y^j B^{m-j}$, the polynomial $h(Y,B)(Y-B)^l$ can be written as a polynomial whose terms have either degree in B less than d_1 or degree in B greater than d_2 if and only if the vector $h = (h_m, h_{m-1}, \ldots, h_0)$ is in the left kernel of $F = (\binom{l}{d_1-v+u})_{0 \leq u \leq d_2-d_1, 0 \leq v \leq m}$

Proof: The vector hF represents the coefficients of $h(Y,B)(Y-B)^l$ which do not satisfy the degree conditions from the theorem. These terms are 0 if and only if h is in the left kernel of F. ∎

Definition 11: Let k, h, r be integers. We define

$$B(k,h,r) := \left(\binom{k}{r+h-v+u} \right)_{0 \leq u,v \leq h}$$

Lemma 11: Let $m \geq 1$, $i < 2^{m-1}$, $0 \leq h \leq i-1$, then $B(2^m - i, h, 2^{m-1} - h)$ has full rank over the binary field.

Proof: Since $i < 2^{m-1}$, Lucas' Lemma [7] implies $\binom{2^m-i}{2^{m-1}} = 1$. Therefore the entries in the main diagonal $u - v = 0$ are equal to 1. If $0 < v - u \leq h$, then $2^m - i < 2^{m-1} - (v-u) < 2^{m-1}$. Similarly the entries below the main diagonal are 0. This finishes the proof. ∎

Lemma 12: Let $q = 2^m$. Suppose $k \leq 2^{m-1}$. Then $I(\Gamma) \cap \langle M_1(k) \cup M_2(k) \rangle_{\mathbb{F}_q} = \{0\}$.

Proof: By contradiction. Let $h < i_1 < k$. Let $g(Y,B)$ be a homogeneous polynomial of degree h such that no term, M, of $g(Y,B)(Y-B)^{q-i_1}$ satisfies $k \leq deg_B\ M < q$. This implies the matrix $(\binom{q-i_1}{k-v+u})_{0 \leq u \leq q-1-k, 0 \leq v \leq h}$ has a nonzero left kernel element. However, this matrix has the matrix $B(q-i, h, k-h)$ as a submatrix, therefore it has no nonzero left kernel elements. ∎

Lemma 13: Let $q = p$, p a prime. Suppose $k \leq \frac{p}{2}$. Then $I(\Gamma) \cap \langle M_1(k) \cup M_2(k) \rangle_{\mathbb{F}_q} = \{0\}$.

Proof: By contradiction. Let $h < i_1 < k$. Let $g(Y,B)$ be a homogeneous polynomial of degree h such that no term, M, of $g(Y,B)(Y-B)^{p-i_1}$ satisfies $k \leq deg_B\ M < p$. This implies the matrix $(\binom{p-i_1}{k-v+u})_{0 \leq u \leq p-1-k, 0 \leq v \leq h}$ has a nonzero left kernel element. However, this matrix has the matrix $B(p-i, h, k-h)$ as a submatrix. Corollary 5 in [8] states that this submatrix has full rank. ∎

We have proved that in certain cases there are no nonzero ideal elements in $I(\Gamma) \cap \langle M_1(k) \cup M_2(k) \rangle_{\mathbb{F}_q}$. In this way we obtain the following dimensions for the following graph codes.

Theorem 6: Let q equal a power of 2 or a prime. Let $k \leq q/2$, then we have

$$\dim(\Gamma, RS(k) : RS(k)) = k^3$$

and, for $q/2 < k \leq q$,

$$\dim(\Gamma, RS(k) : RS(k)) = k^3 + k(q-k)(2k-q).$$

Proof: Lemmas 12 and 13 imply that when q satisfies the conditions of the theorem and $k \leq q/2$, then the intersection of $L_1(k)$ and $L_2(k)$ as subspaces of R is the space generated by $M_1(k) \cap M_2(k)$. Therefore $\dim(\Gamma, RS(k) : RS(k)) = k^3$. The case $k > q/2$ follows from duality and Theorem 2. ∎

Theorem 6 does not hold in general. When q is an odd prime power, and the rate of the component codes is around $1/2$, then the dimension of the graph codes is larger. For example, in the case $q = 9$ and $k = 4$, the dimension of the graph code $(\Gamma, RS(4) : RS(4))$ is $66 > 4^3$. Looking at the polynomial $(Y-B)^6$ over $\mathbb{F}_3$, it is equal to $Y^6 + B^3Y^3 + B^6$. With this polynomial we find the ideal elements $X^3(Y-B)^6 - A^5(Y-B)$ and $A^3(Y-B)^6 - X^5(Y-B)$ are in $\langle M_1(4) \cup M_2(4) \rangle$. These ideal elements give two codewords which are not monomials in $M_1(4) \cap M_2(4)$. However, k^3 still is a useful lower bound on the dimension of $(\Gamma, RS(k) : RS(k))$.

IV. Conclusion

In the proof of Theorem 2 we described the dual of a graph code. Using this description we have extended a known lower bound on the dimension of graph codes (Theorem 1) to an exact expression. This enabled us to compute the exact dimension of the codes $(\Gamma, RS(k) : RS(k))$ in many cases (Theorem 6) and an improved lower bound in general (Theorem 5). We expect the same methods apply to a larger class of interesting graph codes.

Acknowledgment

The authors gratefully acknowledge the support from the Danish National Research Foundation and the National Science Foundation of China (Grant No.11061130539) for the Danish-Chinese Center for Applications of Algebraic Geometry in Coding Theory and Cryptography. We also thank Peng Zeng for his helpful discussions and mindful corrections.

References

[1] R. Tanner, "A recursive approach to low complexity codes," *IEEE Trans. Inf. Theory*, vol. 27, no. 5, pp. 533 – 547, sep 1981.

[2] T. Høholdt and J. Justesen, "Graph codes with reed-solomon component codes," in *Information Theory, 2006 IEEE International Symposium on*, 2006, pp. 2022–2026.

[3] R. M. Roth, *Introduction to Coding Theory*. Cambridge University Press, 2006.

[4] M. Sipser and D. Spielman, "Expander codes," *IEEE Trans. Inf. Theory*, vol. 42, no. 6, pp. 1710 –1722, nov 1996.

[5] J. Fitzgerald and R. Lax, "Decoding affine variety codes using Gröbner bases," *DCC*, vol. 13, pp. 147–158, 1998.

[6] D. Cox, J. Little, and D. O'Shea, *Ideals, Varieties and Algorithms*. Springer, 2007.

[7] E. Lucas, "Théorie des fonctions numériques simplement périodiques"." *American Journal of Mathematics*, vol. 1, 1878.

[8] S. Mattarei, "Linear recurrence relations for binomial coefficients modulo a prime," *J. Number Theor.*, vol. 128, no. 1, pp. 49 – 58, 2008.