Evaluation Codes Over a Particular Complete Intersection

Manuel González Sarabia
Unidad Profesional Interdisciplinaria en Ingeniería y Tecnologías Avanzadas
Instituto Politécnico Nacional
07340 México, D.F., MEXICO
mgonzalezsa@ipn.mx

Carlos Rentería Márquez
Escuela Superior de Física y Matemáticas
Instituto Politécnico Nacional
07300 México, D.F., MEXICO
renteri@esfm.ipn.mx

Antonio J. Sánchez Hernández
Escuela Superior de Física y Matemáticas
Instituto Politécnico Nacional
07300 México, D.F., MEXICO
fosi_ipn@msn.com

Abstract

In this paper we work with some evaluation codes arising from a subset of the projective space. We will prove that this subset is a complete intersection and it will allow us to compute the $a-$invariant of the corresponding vanishing ideal, the length and the dimension of these codes.

Mathematics Subject Classification: 94B27, 94B60

Keywords: Complete Intersection, Projective space, Evaluation code, $a-$invariant

---

1Partially supported by COFFA-IPN and SNI-SEP, México.
2Partially supported by COFFA-IPN and SNI-SEP, México.
1 Introduction

In this paper we will work with some linear codes which are called evaluation codes over a particular complete intersection $Y_m$ (a subset of the projective space $\mathbb{P}^m$ over a finite field $K$). A few years ago these codes were known as Reed-Muller type codes. The main parameters of these linear spaces have been computed in several particular cases: the affine space, the projective space, the Segre variety, the Veronese variety, toric varieties arising from some graphs, toric varieties arising from some subsets of the projective space, etc. Our main goal is to determine the main parameters of these codes when the set $Y_m$ becomes a particular complete intersection. In the following sections we will introduce the concepts that we need to develop these topics.

2 Evaluation Codes

Let $K$ be a finite field with $q$ elements, let $\mathbb{P}^m$ be the $m-$projective space over $K$ and $Y_m = \{P_1, \ldots, P_s\}$ be a subset of $\mathbb{P}^m$. We always use the standard representation for the points in $\mathbb{P}^m$, i.e., $P = (0, 0, \ldots, 0, 1, a_1, \ldots, a_m)$. Let $\mathcal{L}$ be a finite dimensional $K-$linear space of functions which are defined on the set $Y_m$ and take values on $K$. Thus the evaluation map

$$ev : \mathcal{L} \rightarrow K^s,$$

$$ev(f) = (f(P_1), \ldots, f(P_s))$$

defines a $K-$linear code: $C_{Y_m} = ev(\mathcal{L})$.

Let $S_m = K[X_0, \ldots, X_m] = \bigoplus_{d \geq 0} S_m(d)$ be the polynomial ring over the finite field $K$ with the natural graduation. If $\mathcal{L} = S_m(d)$ is the $d-$graded homogeneous component of the polynomial ring $S_m$, the corresponding linear code $C_{Y_m}(d) := ev(S_m(d))$ will be called the evaluation linear code of order $d$ arising from $Y_m$, which is isomorphic to $S_m(d)/I_{Y_m}(d)$, where $I_{Y_m} = \bigoplus_{d \geq 0} I_{Y_m}(d)$ is the graded vanishing ideal of $Y_m$. The dimension of these codes is given by the Hilbert function of $S_m/I_{Y_m}$, i.e., $\dim_K C_{Y_m}(d) = H_{Y_m}(d)$.

This kind of codes has been studied in many particular cases (cf. [1], [2], [3],[4], [6], [7], [8], [9], [10], [11], [12], [13], [14], [15], [16]) and their main parameters have been computed. Especific examples have been given with the help of Macaulay 2 (cf. [5]). In fact, a generating matrix of these codes can be obtained by finding a Gröbner basis for the ideal $I_{Y_m}$, and then the cosets module $I_{Y_m}(d)$ of monomials of degree $d$ not belonging to the leading terms ideal $LT(I_{Y_m})$ of $I_{Y_m}$, forms a $K-$basis for $S_m(d)/I_{Y_m}(d)$. If $B \subseteq S_m(d)$ is this set of monomials then $(ev(h))_{h \in B}$ is a generating matrix for $C_{Y_m}(d)$. 
3 \(a\)-Invariant

Let \(I_{Y_m} = \bigoplus_{d=\gamma}^\infty I_{Y_m}(d)\) with \(I_{Y_m}(\gamma) \neq 0\), so that \(\gamma\) is the lowest degree of a nontrivial homogeneous component of the ideal \(I_{Y_m}\). There is an integer \(a_{Y_m}\) called the \(a\)-invariant of \(S_m/I_{Y_m}\) (or the \(a\)-invariant of the ideal \(I_{Y_m}\) or even the \(a\)-invariant of \(Y_m\)) such that

1. \(H_{Y_m}(d) = \dim_K S_m(d) = \binom{d+m}{m}\) if and only if \(d < \gamma\);
2. \(H_{Y_m}(d) < H_{Y_m}(d+1) < s\) for \(0 \leq d < a_{Y_m}\);
3. \(H_{Y_m}(d) = s\) for \(d > a_{Y_m}\).

The number \(a_{Y_m} + 1\) is called the regularity index of \(S_m/I_{Y_m}\). Moreover, the vanishing ideal \(I_{Y_m}\) is given by

\[I_{Y_m} = \langle I_{Y_m}(\gamma), I_{Y_m}(\gamma+1), \ldots, I_{Y_m}(a_{Y_m}+2) \rangle\]

4 Complete Intersections

We recall (cf. [7]) that a set of points \(Y_m \subseteq \mathbb{P}^m\) is called a (zero-dimensional ideal-theoretic) complete intersection if the vanishing ideal \(I_{Y_m}\) is generated by a regular sequence of \(m\) elements, i.e., there exists a set of \(m\) generators \(f_1, \ldots, f_m\) of the ideal \(I_{Y_m}\) such that \(f_i\) is not a zero divisor of \(S_m/\langle f_1, \ldots, f_{i-1} \rangle\), for \(i = 1, \ldots, m - 1\). If \(I_{Y_m} = \langle f_1, \ldots, f_m \rangle\) and each \(f_i\) is a form of degree \(d_i\), we say that \(Y_m\) is a complete intersection of multidegree \(d = (d_1, \ldots, d_m)\). The following theorem computes de main characteristics of the evaluation code of order \(d\) arising from the complete intersection \(Y_m, C_{Y_m}(d)\):

**Theorem 4.1** The main characteristics of the evaluation code of order \(d\) on a complete intersection \(Y_m, C_{Y_m}(d)\), are given by

- **Length:** \(s = |Y_m| = d_1d_2\cdots d_m\)
- **a-Invariant of \(I_{Y_m}\):** \(a_{Y_m} = (d_1 + \cdots + d_m) - (m + 1)\)
- **Dimension:**

\[H_{Y_m}(d) = \binom{m+d}{d} - \sum_{i<j} \binom{m+d-(d_i+d_j)}{d-(d_i+d_j)} + \sum_{i<j<k} \binom{m+d-(d_i+d_j+d_k)}{d-(d_i+d_j+d_k)} + \cdots + (-1)^m \binom{m+d-(d_1+\cdots+d_m)}{d-(d_1+\cdots+d_m)}\]

**Proof.** cf. [7].

In the next section we will prove that the specific set of points that we will define is a complete intersection and the last theorem will help us to find the main parameters of the corresponding evaluation codes of order \(d\) associated to that set of points.
5 Main Results

From now on we will work with the following subset of the projective space:

\[ Y_m = \{(1, t_1^{n_1}, t_2^{n_2}, \ldots, t_m^{n_m}) : t_i \in K^* \forall i = 1, \ldots, m \} \subseteq \mathbb{P}^m \]

In this case the evaluation map defined before becomes

\[ ev_d : S_m(d) \to K^s, \]

\[ ev_d(f) = (f(P_1), \ldots, f(P_s)) \]

And the linear code \( C_{Y_m}(d) \), which is the image of the last evaluation map, will be called the evaluation code of order \( d \) arising from \( Y_m \).

In the following theorem we will prove that the set \( Y_m \) is a complete intersection and therefore we will describe the main parameters of the evaluation code \( C_{Y_m}(d) \).

**Theorem 5.1** The set \( Y_m \subseteq \mathbb{P}^m \) is a complete intersection, in fact,

\[ I_{Y_m} = \langle f_i : i = 1, \ldots, m \rangle \]

where \( s_i = \frac{q-1}{(q-1,n_i)} \), \( f_i = X_i^{s_i} - X_0^{s_1} \) for all \( i = 1, \ldots, m \). Of course, \( (q-1,n_i) \) means the greatest common divisor of \( q-1 \) and \( n_i \).

**Proof.** We will use the lexicographic ordering \( X_m > X_{m-1} > \cdots > X_0 \). The proof will be carried out by induction on \( m \). If \( m = 1 \), let \( f \in I_{Y_1} \). We can write \( f(X_0, X_1) = X_0^r \cdot g(X_0, X_1) \) in such a way that \( X_0 \) is not a divisor of \( g(X_0, X_1) \). Therefore \( 0 = f(1, t^{n_1}) = g(1, t^{n_1}) \) for all \( t \in K^* \). Moreover, \( g(1, X_1) \in K[X_1] \) and if we take \( U = \{t^{n_1} : t \in K^* \} \), where obviously \( \#U = s_1 \), then \( g(1, X_1) = f_1(X_1) \cdot \prod_{a \in U} (X_1 - a) = f_1(X_1)(X_1^{s_1} - 1) \). Homogenizing on \( X_0 \):

\[ g(X_0, X_1) = f_1^h(X_0, X_1)(X_1^{s_1} - X_0^{s_1}) \]

therefore

\[ f(X_0, X_1) = X_0^r f_1^h(X_0, X_1)(X_1^{s_1} - X_0^{s_1}) \]

Hence \( I_{Y_1} = \langle f_1 \rangle \).

Now we will suppose that the result is correct for \( m-1 \) and let \( f \in I_{Y_m} \). By using the division algorithm we can find polynomials \( q_1, r_1 \in S_m \) such that \( (t \in K^*) \)

\[ f = (X_m - t^{n_m}X_0)q_1 + r_1 \]
and none of the monomials of \( r_1 \) is divisible by \( X_m \). Therefore \( r_1 \in S_{m-1} \). Moreover if \( P' \in Y_{m-1} \), then \( P = (P', t^{n_m}) \in Y_m \) and

\[
0 = f(P) = r_1(P'), \text{ hence } r_1 \in I_{Y_{m-1}} = \langle f_1, \ldots, f_{m-1} \rangle
\]

In fact if \( z \in K^*, z^{n_m} \neq t^{n_m} \), we can use the division algorithm again and write

\[
q_1 = (X_m - z^{n_m}X_0)q_2 + r_2 \text{ with } r_2 \in S_{m-1}
\]

In the same way if \( P_1 = (P', z^{n_m}) \in Y_m \), then

\[
0 = q_1(P_1) = r_2(P'), \text{ hence } r_2 \in I_{Y_{m-1}}
\]

Working in the same way and taking \( W = \{t^{n_m} : t \in K^*\} \) where obviously \( \#W = s_m \), we obtain that

\[
f = \left( \prod_{a \in W} (X_m - aX_0) \right)q + r = (X_m^{s_m} - X_0^{s_m})q + r = f_m q + r
\]

with \( r \in I_{Y_{m-1}} = \langle f_1, \ldots, f_{m-1} \rangle \). Therefore \( f \in \langle f_1, \ldots, f_m \rangle \), and then \( I_{Y_m} = \langle f_1, \ldots, f_m \rangle \). ■

**Corollary 5.2** The main characteristics of the evaluation codes of order \( d \) arising from the complete intersection \( Y_m \subseteq \mathbb{P}^m \), defined before, are the following:

1. **Length**: \( s = |Y_m| = \prod_{i=1}^{m} s_i \)

2. **a–Invariant of the vanishing ideal** \( I_{Y_m} \): \( a_{Y_m} = \sum_{i=1}^{m} s_i - (m + 1) \)

3. **Dimension**:

   \[
   H_{Y_m}(d) = \binom{m+d}{d} - \sum_{i<j} \binom{m+d-(s_i+s_j)}{d-(s_i+s_j)} + \sum_{i<j<k} \binom{m+d-(s_i+s_j+s_k)}{d-(s_i+s_j+s_k)} + \cdots + (-1)^m \binom{m+d-(s_1+\cdots+s_m)}{d-(s_1+\cdots+s_m)}
   \]

**Proof.** Cf. [7] and the last theorem. ■
5.1 An example

In this example we will work with a field with \( q = 37 \) elements, \( m = 3, n_1 = 4, n_2 = 6, n_3 = 27 \). Then \( S_3 = \mathbb{K}[X_0, X_1, X_2, X_3] \) and \( Y_3 = \{(1, t_1^4, t_2^6, t_3^{27}) : t_1, t_2, t_3 \in \mathbb{K}^*\} \subseteq \mathbb{P}^3 \). In fact \( s_1 = \frac{36}{(36,4)} = 9 \), \( s_2 = \frac{36}{(36,6)} = 6 \) and \( s_3 = \frac{36}{(36,27)} = 4 \). The main results about the evaluation codes \( C_{Y_3}(d) \) are the following:

- **Length:** \( s = \#Y_3 = s_1 \cdot s_2 \cdot s_3 = 216 \)
- **Vanishing ideal:** By using Macaulay 2 (cf. [5]) we get
  \[
  I_{Y_3} = \langle X_3^4 - X_0^4, X_2^6 - X_0^6, X_4^4 - X_0^4 \rangle
  \]
  and it is easy to see that \( I_{Y_3} = \langle X_1^9 - X_0^9, X_2^6 - X_0^6, X_3^4 - X_0^4 \rangle \)
- **a−Invariant:** \( a_{Y_3} = (s_1 + s_2 + s_3) - (m + 1) = 19 - 4 = 15 \).
- **Hilbert series:**
  \[
  F_{Y_3}(z) = \frac{1 - z^4 - z^6 - z^9 + z^{10} + z^{13} + z^{15} + z^{19}}{(1 - z)^3}
  \]
- **Dimension:**

\[
\begin{array}{|c|c|}
\hline
d & H_{Y_3}(d) \\
\hline
0 & 1 \\
1 & 4 \\
2 & 10 \\
3 & 20 \\
4 & 34 \\
5 & 52 \\
6 & 73 \\
7 & 96 \\
8 & 120 \\
9 & 143 \\
10 & 164 \\
11 & 182 \\
12 & 196 \\
13 & 206 \\
14 & 212 \\
15 & 215 \\
16 & 216 \\
\hline
\end{array}
\]
References


Received: February, 2011