Journal of Pure and Applied Algebra 221 (2017) 251–275

Contents lists available at ScienceDirect

Journal of Pure and Applied Algebra

www.elsevier.com/locate/jpaa

Minimum distance functions of graded ideals and Reed–Muller-type codes ☆

José Martínez-Bernal, Yuriko Pitones, Rafael H. Villarreal *

Departamento de Matemáticas, Centro de Investigación y de Estudios Avanzados del IPN, Apartado Postal 14–740, 07000 Mexico City, D.F., Mexico

ARTICLE INFO

Article history:
Received 16 December 2015
Received in revised form 7 June 2016
Available online 9 August 2016
Communicated by A.V. Geramita

MSC:
Primary: 13P25; secondary: 14G50; 94B27; 11T71

ABSTRACT

We introduce and study the *minimum distance function* of a graded ideal in a polynomial ring with coefficients in a field, and show that it generalizes the minimum distance of projective Reed–Muller-type codes over finite fields. This gives an algebraic formulation of the minimum distance of a projective Reed–Muller-type code in terms of the algebraic invariants and structure of the underlying vanishing ideal. Then we give a method, based on Gröbner bases and Hilbert functions, to find lower bounds for the minimum distance of certain Reed–Muller-type codes. Finally we show explicit upper bounds for the number of zeros of polynomials in a projective nested cartesian set and give some support to a conjecture of Carvalho, Lopez-Neumann and López.

1. Introduction

Let $S = K[t_1, \dots, t_s] = \oplus_{d=0}^{\infty} S_d$ be a polynomial ring over a field K with the standard grading and let $I \neq (0)$ be a graded ideal of S of Krull dimension k. The *Hilbert function* of S/I is:

$$H_I(d) := \dim_K(S_d/I_d), \quad d = 0, 1, 2, \dots,$$

where $I_d = I \cap S_d$. By a theorem of Hilbert, there is a unique polynomial $h_I(x) \in \mathbb{Q}[x]$ of degree $k-1$ such that $H_I(d) = h_I(d)$ for $d \gg 0$. The degree of the zero polynomial is -1.

The *degree* or *multiplicity* of S/I is the positive integer

$$\deg(S/I) := \begin{cases} (k-1)! \lim_{d\to\infty} H_I(d)/d^{k-1} & \text{if } k \geq 1, \\ \dim_K(S/I) & \text{if } k = 0. \end{cases}$$

☆ The first and third author were supported by SNI, Mexico. The second author was supported by a CONACYT scholarship from Mexico.

* Corresponding author.
E-mail addresses: jmb@math.cinvestav.mx (J. Martínez-Bernal), ypitones@math.cinvestav.mx (Y. Pitones), vila@math.cinvestav.mx (R.H. Villarreal).

http://dx.doi.org/10.1016/j.jpaa.2016.06.006

Let $\mathcal{F}_d$ be the set of all zero-divisors of S/I not in I of degree $d \geq 0$:

$$\mathcal{F}_d := \{\, f \in S_d \,|\, f \notin I,\, (I\colon f) \neq I\},$$

where $(I\colon f) = \{h \in S|\, hf \in I\}$ is a quotient ideal. Notice that $\mathcal{F}_0 = \emptyset$.

The main object of study here is the function $\delta_I\colon \mathbb{N} \to \mathbb{Z}$ given by

$$\delta_I(d) := \begin{cases} \deg(S/I) - \max\{\deg(S/(I,f))|\, f \in \mathcal{F}_d\} & \text{if } \mathcal{F}_d \neq \emptyset, \\ \deg(S/I) & \text{if } \mathcal{F}_d = \emptyset. \end{cases}$$

We call δ_I the *minimum distance function* of I. If I is a prime ideal, then $\mathcal{F}_d = \emptyset$ for all $d \geq 0$ and $\delta_I(d) = \deg(S/I)$. We show that δ_I generalizes the minimum distance function of projective Reed–Muller-type codes over finite fields (Theorem 4.7). This abstract algebraic formulation of the minimum distance gives a new tool to study these type of linear codes.

To compute $\delta_I(d)$ is a difficult problem. For certain family of ideals we will give lower bounds for $\delta_I(d)$ which are easier to compute.

Fix a monomial order $\prec$ on S. Let $\Delta_\prec(I)$ be the *footprint* of S/I consisting of all the *standard monomials* of S/I, with respect to $\prec$, and let $\mathcal{G} = \{g_1, \ldots, g_r\}$ be a Gröbner basis of I. Then $\Delta_\prec(I)$ is the set of all monomials of S that are not a multiple of any of the leading monomials of $g_1, \ldots, g_r$ (Lemma 2.5). A polynomial f is called *standard* if $f \neq 0$ and f is a K-linear combination of standard monomials.

If $\Delta_\prec(I) \cap S_d = \{t^{a_1}, \ldots, t^{a_n}\}$ and $\mathcal{F}_{\prec,d} = \{f = \sum_i \lambda_i t^{a_i} \mid f \neq 0,\ \lambda_i \in K,\, (I\colon f) \neq I\}$, then using the division algorithm [4, Theorem 3, p. 63] we can write:

$$\begin{aligned} \delta_I(d) &= \deg(S/I) - \max\{\deg(S/(I,f))|\, f \in \mathcal{F}_d\} \\ &= \deg(S/I) - \max\{\deg(S/(I,f))|\, f \in \mathcal{F}_{\prec,d}\}. \end{aligned}$$

Notice that $\mathcal{F}_d \neq \emptyset$ if and only if $\mathcal{F}_{\prec,d} \neq \emptyset$. If $K = \mathbb{F}_q$ is a finite field, then the number of standard polynomials of degree d is $n^q - 1$, where n is the number of standard monomials of degree d. Hence, we can compute $\delta_I(d)$ for small values of n and q (Examples 7.1 and 7.2).

Upper bounds for $\delta_I(d)$ can be obtained by fixing a subset $\mathcal{F}'_{\prec,d}$ of $\mathcal{F}_{\prec,d}$ and computing

$$\delta'_I(d) = \deg(S/I) - \max\{\deg(S/(I,f))|\, f \in \mathcal{F}'_{\prec,d}\} \geq \delta_I(d).$$

Typically one uses $\mathcal{F}'_{\prec,d} = \{f = \sum_i \lambda_i t^{a_i} \mid f \neq 0,\ \lambda_i \in \{0,1\},\, (I\colon f) \neq I\}$ or a subset of it.

Lower bounds for $\delta_I(d)$ are harder to find. Thus, we seek to estimate $\delta_I(d)$ from below. So, with this in mind, we introduce the *footprint function* of I:

$$\mathrm{fp}_I(d) = \begin{cases} \deg(S/I) - \max\{\deg(S/(\mathrm{in}_\prec(I), t^a))\,|\, t^a \in \Delta_\prec(I)_d\} & \text{if } \Delta_\prec(I)_d \neq \emptyset, \\ \deg(S/I) & \text{if } \Delta_\prec(I)_d = \emptyset, \end{cases}$$

where $\mathrm{in}_\prec(I) = (\mathrm{in}_\prec(g_1), \ldots, \mathrm{in}_\prec(g_r))$ is the initial ideal of I, $\mathrm{in}_\prec(g_i)$ is the initial monomial of g_i for $i = 1, \ldots, s$, and $\Delta_\prec(I)_d = \Delta_\prec(I) \cap S_d$.

The contents of this paper are as follows. In Section 2 we present some of the results and terminology that will be needed throughout the paper.

Some of our results rely on a degree formula to compute the number of zeros that a homogeneous polynomial has in any given finite set of points in a projective space (Lemma 3.2).

In Section 4 we study δ_I and present an alternative formula for δ_I, pointed out to us by Vasconcelos, valid for unmixed graded ideals (Theorem 4.4). If $\mathcal{F}_d \neq \emptyset$ for $d \geq 1$ and I is unmixed, then, by Lemma 4.1,