Journal of Symbolic Computation 65 (2014) 15–28

Contents lists available at ScienceDirect

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

Computing the degree of a lattice ideal of dimension one ☆

Hiram H. López, 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

A R T I C L E   I N F O

Article history:
Received 9 September 2013
Accepted 23 December 2013
Available online 28 January 2014

Keywords:
Lattice ideals
Degree
Index of regularity
Smith normal form
Vanishing ideals
Hilbert functions
Torsion subgroup

A B S T R A C T

We show that the degree of a graded lattice ideal of dimension 1 is the order of the torsion subgroup of the quotient group of the lattice. This gives an efficient method to compute the degree of this type of lattice ideals.

1. Introduction

Let $S=K[t_1,\dots,t_s]$ be a graded polynomial ring over a field K, where each t_i is homogeneous of degree one, and let S_d denote the set of homogeneous polynomials of total degree d in S, together with the zero polynomial. The set S_d is a K-vector space of dimension $\binom{d+s-1}{s-1}$. If $I\subset S$ is a graded ideal, i.e., I is generated by homogeneous polynomials, we let

$$I_d=I\cap S_d$$

denote the set of homogeneous polynomials in I of total degree d, together with the zero polynomial. Note that I_d is a vector subspace of S_d. Then the *Hilbert function* of the quotient ring S/I, denoted by $H_I(d)$, is defined by

$$H_I(d)=\dim_K(S_d/I_d).$$

☆ The first author was partially supported by CONACyT. The second author was partially supported by SNI.
E-mail address: vila@math.cinvestav.mx (R.H. Villarreal).

0747-7171/$ – see front matter
http://dx.doi.org/10.1016/j.jsc.2014.01.002

According to a classical result of Hilbert (Bruns and Herzog, 1997, Theorem 4.1.3), there is a unique polynomial

$$h_I(t) = c_k t^k + (\text{terms of lower degree})$$

of degree k, with rational coefficients, such that $h_I(d) = H_I(d)$ for $d \gg 0$. By convention the zero polynomial has degree -1, that is, $h_I(t) = 0$ if and only if $k = -1$. The integer $k+1$ is the *Krull dimension* of S/I and $h_I(t)$ is the *Hilbert polynomial* of S/I. If $k \geqslant 0$, the positive integer $c_k(k!)$ is called the *degree* of S/I. The *degree* of S/I is defined as $\dim_K(S/I)$ if $k = -1$. The *index of regularity* of S/I, denoted by $\mathrm{reg}(S/I)$, is the least integer $r \geqslant 0$ such that $h_I(d) = H_I(d)$ for $d \geqslant r$. The degree and the Krull dimension are denoted by $\deg(S/I)$ and $\dim(S/I)$, respectively. As usual, by the *dimension* of I we mean the Krull dimension of S/I.

The notion of *degree* plays an important role in algebraic geometry (Cox et al., 1992, 2011; Harris, 1992) and commutative algebra (Bruns and Herzog, 1997; Eisenbud, 1995). Consider a projective space $\mathbb{P}^{s-1}$ over the field K. The *degree* and the *dimension* of a projective variety $X \subset \mathbb{P}^{s-1}$ can be read off from the Hilbert polynomial $h_I(t)$, where $I = I(X)$ is the *vanishing ideal* of X generated by the homogeneous polynomials of S that vanish at all points of X. For the geometric interpretation of the degree of $S/I(X)$ see the references above. If X is a finite set of points, the Hilbert polynomial of $S/I(X)$ is a non-zero constant, the degree of $S/I(X)$ is equal to $|X|$ (the number of points in X), and the dimension of $S/I(X)$ is equal to 1 (Harris, 1992, p. 164). In view of its applications to coding theory, we are interested in the case when K is a finite field and X is parameterized by monomials (see Section 5).

Let $\mathcal{L} \subset \mathbb{Z}^s$ be a *lattice*, i.e., $\mathcal{L}$ is a subgroup of $\mathbb{Z}^s$. The *lattice ideal* of $\mathcal{L}$, denoted by $I(\mathcal{L})$, is the ideal of S generated by the set of all binomials $t^{a^+} - t^{a^-}$ such that $a \in \mathcal{L}$, where a^+ and a^- are the positive and negative parts of a (see Section 3). A first hint of the rich interaction between the group theory of $\mathcal{L}$ and the algebra of $I(\mathcal{L})$ is that the rank of $\mathcal{L}$, as a free abelian group, is equal to $s - \dim(S/I(\mathcal{L}))$ (Miller and Sturmfels, 2004, Proposition 7.5). This number is the height of the ideal $I(\mathcal{L})$ in the sense of Bruns and Herzog (1997), and is usually denoted by $\mathrm{ht}(I(\mathcal{L}))$. Another useful result is that $\mathbb{Z}^s/\mathcal{L}$ is a torsion-free group if and only if $I(\mathcal{L})$ is a prime ideal (Miller and Sturmfels, 2004, Theorem 7.4). In the same vein, for a certain family of lattice ideals, we will relate the structure of the finitely generated abelian group $\mathbb{Z}^s/\mathcal{L}$ and the degree of $S/I(\mathcal{L})$.

The set of nonnegative integers (resp. positive integers) is denoted by $\mathbb{N}$ (resp. $\mathbb{N}_+$). The structure of $\mathbb{Z}^s/\mathcal{L}$ can easily be determined, as we now explain. Let A be an integral matrix of order $m \times s$ whose rows generate $\mathcal{L}$. There are unimodular integral matrices U and V such that $UAV = D$, where $D = \mathrm{diag}(d_1, d_2, \ldots, d_r, 0, \ldots, 0)$ is a diagonal matrix, with $d_i \in \mathbb{N}_+$ and d_i divides d_j if $i \leqslant j$. The matrix D is the *Smith normal form* of A and the integers $d_1, \ldots, d_r$ are the *invariant factors* of A. Recall that the *torsion subgroup* of $\mathbb{Z}^s/\mathcal{L}$, denoted by $T(\mathbb{Z}^s/\mathcal{L})$, consists of all $\bar{a} \in \mathbb{Z}^s/\mathcal{L}$ such that $\ell\bar{a} = \bar{0}$ for some $\ell \in \mathbb{N}_+$. From the fundamental structure theorem for finitely generated abelian groups (Jacobson, 1996) one has:

$$\mathbb{Z}^s/\mathcal{L} \simeq \mathbb{Z}/(d_1) \oplus \mathbb{Z}/(d_2) \oplus \cdots \oplus \mathbb{Z}/(d_r) \oplus \mathbb{Z}^{s-r},$$
$$T\left(\mathbb{Z}^s/\mathcal{L}\right) \simeq \mathbb{Z}/(d_1) \oplus \mathbb{Z}/(d_2) \oplus \cdots \oplus \mathbb{Z}/(d_r),$$

where r is the rank of $\mathcal{L}$. In particular the order of $T(\mathbb{Z}^s/\mathcal{L})$ is $d_1 \cdots d_r$. Thus, using any algebraic system that computes Smith normal forms of integral matrices, *Maple* (Char et al., 1991) for instance, one can determine the order of $T(\mathbb{Z}^s/\mathcal{L})$.

Let $I(\mathcal{L}) \subset S$ be a graded lattice ideal of dimension one. Note that the corresponding lattice $\mathcal{L}$ is homogeneous and has rank $s-1$ (see Definition 3.5 and Remark 3.6). The aim of this paper is to give a new method, using integer linear algebra, to compute the degree of $S/I(\mathcal{L})$.

The contents of this paper are as follows. In Section 2, we present some well known results about the behavior of Hilbert functions of graded ideals. In particular, we recall a standard method, using Hilbert series, to compute the degree and the index of regularity.

In Section 3, we use linear algebra and Gröbner bases methods to describe the torsion subgroup of $\mathbb{Z}^s/\mathcal{L}$ (see Lemmas 3.8 and 3.10). Then, using standard Hilbert functions techniques, we give an upper bound for the index of regularity (see Proposition 3.12).