International Electronic Journal of Pure and Applied Mathematics

Volume 4 No. 3 2012, 175-178

ON THE MINIMUM DISTANCE OF GOPPA CODES OF SMOOTH PLANE CURVES

E. Ballico

Department of Mathematics
University of Trento
38 123 Povo (Trento) - Via Sommarive, 14, ITALY
e-mail: ballico@science.unitn.it

Abstract: We use the numerical character for zero-dimensional schemes $Z \subset \mathbb{P}^2$ to study the minimum distance of certain Goppa codes over smooth plane curves.

AMS Subject Classification: 94B27, 14N05, 14Q05
Key Words: dual code, generalized Hamming weights, higher support weights, evaluation code, plane curve, algebraic-geometric code

1. Introduction

Take a zero-dimensional scheme $Z \subset \mathbb{P}^2$, an integer $t > 0$. Set $e := h^1(\mathbb{P}^2, \mathcal{I}_Z(t))$ and assume $e > 0$. What can be said about Z if we know that $h^1(\mathcal{I}_{Z'}(t)) < e$ for any zero-dimensional scheme $Z' \subsetneq Z$? In section 3 we link this problem to the computation of the minimum distance (case $e = 1$) or the generalized e-th Hamming weight of certain Goppa codes.

Let $\mathbb{K}$ be any algebraically closed base field and $Z \subset \mathbb{P}^2$ be a zero-dimensional scheme, $Z \neq \emptyset$. For each integer $t \geq 0$ we have and exact sequence

$$0 \to \mathcal{I}_Z(t) \to \mathcal{O}_{\mathbb{P}^2}(t) \to \mathcal{O}_Z(t) \to 0 \tag{1}$$

which induces a restriction map $\rho_{Z,t} : H^0(\mathbb{P}^2, \mathcal{O}_{\mathbb{P}^2}(t)) \to H^0(Z, \mathcal{O}_Z(t))$. Set $h_Z(t) := \dim(\mathrm{Im}(\rho_{Z,t})$. The function $t \mapsto h_Z(t)$ is called the Hilbert function of Z. The integer $h_Z(t)$ is the number of independent conditions that aZ imposes to the vector space of all degree t homogeneous polynomials in three variables. For any $t \in \mathbb{Z}$ we have $h^0(Z, \mathcal{O}_Z(t)) = \deg(Z)$ and $h^1(\mathbb{P}^2, \mathcal{O}_{\mathbb{P}^2}(t)) = 0$. Hence $\deg(Z) = h_Z(t) + h^1(\mathbb{P}^2, \mathcal{I}_Z(t))$. Hence (knowing the integer $z := \deg(Z)$) to know the Hilbert function h_Z it is equivalent to know the function $t \mapsto h^1(\mathbb{P}^2, \mathcal{I}_Z(t))$. Since $\mathbb{P}^2, \mathcal{I}_Z) = \deg(Z) - 1$

Received: December 28, 2011

International Electronic Journal of Pure and Applied Mathematics – IEJPAM, Volume 4, No. 3 (2012)

if $Z \neq \emptyset$, the latter function even determines the integer $\deg(Z)$. L. Gruson and Ch. Peskine introduced the numerical character of Z and proved that its knowledge is equivalent to the knowledge of h_Z (see [3]). This invariant (or any equivalent form of it) is the strongest available tool for the study of zero-dimensional schemes (or even finite sets) in a projective plane. See for instance [2] for an application of it. We recall it. Let $s > 0$ be the minimal degree of a plane curve containing Z (we allow the case in which the curve is reducible or even a multiple curve). For any $a \in \mathbb{Z}$ set $a_+ := \max\{0, a\}$. The numerical character $\overline{n}(Z)$:

(i) s is the minimal degree of a

(ii) $n_0 \geq \cdots \geq n_{s-1} \geq s$;

(iii) $\deg(Z) - h_Z(t) = \sum_{t=0}^{s-1}[(n_i - t - 1)_+ - (i - t - 1)_+]$

Taking $t = 0$ in (iii) we get $\deg(Z) = \sum_{i=0}^{s-1}(n_i - i) = n_0 + \cdots + n_{s-1} - s(s-1)/2$. An integer $t \in \{1, \ldots, s-1\}$ is a gap for the numerical character $(n_0, \ldots, n_{s-1})$ if $n_{t-1} \geq n_t + 2$. In [2], Ellia and Peskine proved that the existence of gaps for the numerical character of Z gives strong geometrical restrictions to Z and/or gives that a proper subscheme of Z is contained in a very low degree plane curve. When we add that Z comes from something computing the minimum distance of a certain code $\mathcal{C}(B, \mathcal{O}_C(x)(-E))^{\perp}$, then often we get that Z must be contained in a very low degree plane curves (lines for certain codes on the Hermitian curve). A numerical character is connected if it has no gaps. Here we prove the following result.

Theorem 1. *Let $Z \subset \mathbb{P}^2$ be a zero-dimensional scheme. Fix an integer $x > 0$ and assume $e := h^1(\mathbb{P}^2, \mathcal{I}_Z(x)) > 0$ and $h^1(\mathbb{P}^2, \mathcal{I}_{Z'}(x)) < e$ for all $Z' \subsetneq Z$. If $e \geq 2$, then assume $h^1(\mathbb{P}^2, \mathcal{I}_Z(x+1)) = 0$. Then the numerical character of Z has no gaps.*

Theorem 2. *Let $Z \subset \mathbb{P}^2$ be a zero-dimensional scheme. Fix an integer $x > 0$ and assume $e := h^1(\mathbb{P}^2, \mathcal{I}_Z(x)) > 0$. Write $Z = E \sqcup S$ with E, S zero-dimensional and $E \cap S = \emptyset$. Assume $h^1(\mathbb{P}^2, \mathcal{I}_{E \cup S'}(x)) < e$ for all $S' \subsetneq S$. If $e \geq 2$, then assume $h^1(\mathbb{P}^2, \mathcal{I}_Z(x+1)) = 0$. Assume that the numerical character $(n_0, \ldots, n_{s-1})$ has a gap and call t the first such a gap. Then there is a degree t curve $T \subset \mathbb{P}^2$ such that $S \subset T$, $T \cap Z$ has $(n_0, \ldots, n_{t-1})$ as its numerical character, $h^1(\mathbb{P}^2, \mathcal{I}_{Z \cap T}(x)) > 0$ and $\deg(Z) - \deg(Z \cap T) = \sum_{i=0}^{s-t-1}(n_{t+i} - t - i)$.*

The Hilbert functions of the scheme Z with connected numerical character is very restrictive (it is the same as the one of sets in uniform position).

2. The Proofs

For any coherent sheaf $\mathcal{F}$ on $\mathbb{P}^2$ and any integer $i \geq 0$ we write $H^i(\mathcal{F}$ and $h^i(\mathcal{F}) := \dim(H^i(\mathcal{F}))$ instead of $H^i(\mathbb{P}^2, \mathcal{F})$ and $h^i(\mathbb{P}^2, \mathcal{F})$ respectively.

International Electronic Journal of Pure and Applied Mathematics – IEJPAM, Volume 4, No. 3 (2012)

Fix a zero-dimensional scheme $Z \subset \mathbb{P}^2$ and let $(n_0, \dots, n_{s-1})$ be its numerical character. From (i) we get $h^0(\mathcal{I}_Z(s)) > 0$ and $h^0(\mathcal{I}_Z(s-1)) = 0$. Hence $h_Z(t)) = \binom{t+2}{2}$ if $0 \le t \le s-1$, while $h_Z(t)) < \binom{t+2}{2}$ if $t \ge s$. If $s = 1$, then Z is contained in a line and it is a complete intersection. Now assume $s \ge 2$ and hence $\deg(Z) \ge 3$. From (iii) we get that $n_0 - 2$ is the maximal integer t such that $h^1(\mathcal{I}_Z(t)) > 0$.

Fix any plane curve $T \subset \mathbb{P}^2$ and any zero-dimensional scheme $Z \subset \mathbb{P}^2$ let $\mathrm{Res}_T(Z)$ denote the residual scheme of Z with respect to T, i.e. the closed subscheme of $\mathbb{P}^2$ with $\mathcal{I}_Z : \mathcal{I}_T$ as its ideal sheaf. We have $\mathrm{Res}_T(Z) \subseteq Z$, $\deg(Z) = \deg(Z \cap T) + \deg(\mathrm{Res}_T(Z))$ and for any $y \in \mathbb{Z}$ we have an exact sequence

$$0 \to \mathcal{I}_{\mathrm{Res}_T(Z)}(y-t) \to \mathcal{I}_Z(y) \to \mathcal{I}_{Z\cap T,T}(y) \to 0 \tag{2}$$

where $t := \deg(T)$.

Proof of Theorem 1. Since $h^1(\mathcal{I}_Z(y+1)) < h^1(\mathcal{I}_Y(y))$ if $h^1(\mathcal{I}_Y(y)) > 0$, we have $h^1(\mathcal{I}_Z(x+1)) = 0$ even in the case $e = 1$. Assume that t is a gap of the numerical character $(n_0, \dots, n_{s-1})$ of Z. Since $(n_0, \dots, n_{s-1)})$ has a gap, we have $s \ge 2$. We also get $s \ge t+1$. Hence $x = n_0 - 2$.

By [2], Proposition at page 112, there is a degree t plane curve $T \subset \mathbb{P}^2$ such that the scheme $T \cap Z$ has numerical character $(n_0, \dots, n_{t-1})$ (and in particular no curve of degree $< t$ contains $T \cap Z$), while $\mathrm{Res}_T(Z)$ has numerical character $(m_0, \dots, m_{s-t-1}$ with $m_i := n_{t+i} - t$ for all i (and in particular $s - t$ is the minimal degree of a plane curve containing $\mathrm{Res}_T(Z)$. In particular $\mathrm{Res}_T(Z) \neq \emptyset$, i.e. $Z \cap T \subseteq Z$. Our assumption implies $h^1(\mathcal{I}_{Z\cap T}(x)) < h^1(\mathcal{I}_Z(x))$. From (2) with $y = x$ we get $h^1(\mathcal{I}_{\mathrm{Res}_T(Z)}(x-t)) > 0$. Hence $x - t \le m_0 - 2 = n_t - t - 2$. Since $n_t - 2 \le n_{t-1} - 4 \le n_0 - 4 < x$, we obtained a contradiction. □

Proof of Theorem 2. Take word for word the proof of Theorem 1. We only get $S \subset T$. The other statements of Theorem 2 follows from [2], Proposition at page 112. □

3. The Motivation

Let K be a finite field and $\overline{K}$ its algebraic closure. Let C be a smooth and geometrically connected projective curve defined over K. Fix any line bundle $\mathcal{L} = \mathcal{O}_C(D)$ on C defined over K and any $B \subset C(K)$, with B disjoint from the support of D. Let $\mathcal{C}(B, \mathcal{L})$ denote the Goppa code obtained evaluating the rational functions f on C with $(f) + D \ge 0$ at the points of B. Under very mild conditions $\mathcal{C}(B, \mathcal{L})$ is an $[n, k]$-code with $n = \sharp(B)$ and $k = h^0(C, \mathcal{L})$. For each $w \in \mathcal{C}(B, \mathcal{L})^{\perp}$, $w \neq 0$, the support $supp(w)$ of B is the set of all $P \in B$ at which w is non-zero. Hence the minimum distance of $\mathcal{C}(B, \mathcal{L})^{\perp}$ is the minimal integer $supp(w)$. For each linear subpace $V \subseteq \mathcal{C}(B, \mathcal{L})^{\perp}$, $V \neq 0$, set $supp(V) := \cup_{w \in V \setminus \{0\}} supp(w) \subseteq B$. Hence $supp(V)$ is the minimal set $S \subseteq B$ such that each $w \in V$ is zero at each point of $B \setminus S$. For each

International Electronic Journal of Pure and Applied Mathematics – IEJPAM, Volume 4, No. 3 (2012)

integer h such that $1 \leq h < n$, the generalized h-Hamming weight $d_h(\mathcal{C}(B,\mathcal{L})^{\perp})$ of $\mathcal{C}(B,\mathcal{L})^{\perp}$ is the minimal cardinality of the support of some h-dimensional linear subspace of $\mathcal{C}(B,\mathcal{L})^{\perp}$ (see [4], [5]). Now assume that C is embedded in $\mathbb{P}^2$ over K. If $\mathcal{L} \cong \mathcal{O}_C(x))$, then A. Covreur proved how to list all codewords of $\mathcal{C}(B,\mathcal{L})^{\perp}$ with, say, weight $\leq 3x$ (see [1]). In the set-up of Theorem 1 we take as Z a finite subset of B computing the minimum distance (or the e-th Hamming weight) of the dual code $\mathcal{C}(B,\mathcal{O}_C(x))$. Covreur's approach was extended to the case $\mathcal{L} \cong \mathcal{O}_C(x)(-E))$ with E effective divisor of C. We assume $h^1(\mathbb{P}^2,\mathcal{I}_E(x)) = 0$. The set $S \subset B$ computing the minimum distance of $\mathcal{C}(B,\mathcal{O}_C(x)(-E))^{\perp}$ is as described in the set-up of Theorem 1. We also get that if the numerical character of $E \cup S$ is not connected, then S computes the minimum distance of the dual of the larger code $\mathcal{C}(B,\mathcal{O}_C(x)(-(E \cap T))$. We may apply Theorems 1 and 2, because the cohomology groups are invariant under field extension and hence to get the plane curve T we may work over $\overline{K}$.

Acknowledgements

The author was partially supported by MIUR and GNSAGA of INdAM (Italy).

References

[1] A. Couvreur, The dual minimum distance of arbitrary dimensional algebraic-geometric codes, *ArXiv:* 0905.2345v3, *J. Algebra*, To Appear.

[2] Ph. Ellia, Ch. Peskine, Groupes de points de $\mathbf{P}^2$: Caractère et position uniforme, *Algebraic Geometry*, L'Aquila (1988), 111-116; *Lecture Notes in Math.*, **1417**, Springer, Berlin (1990).

[3] L. Gruson, Ch. Peskine, Genre des courbes de l'espace projectif, *Algebraic Geometry*, Proc. Sympos., Univ. Troms, Troms (1977), 31-59; *Lecture Notes in Math.*, **687**, Springer, Berlin (1978).

[4] G.M. Hana, T. Johnsen, Scroll codes, *Des. Codes Cryptogr.*, **45**, No. 3 (2007), 365-377.

[5] T. Johnsen, N.H. Rasmussen, Scroll codes over curves of higher genus, *Appl. Algebra Engrg. Comm. Comput.*, **21** (2010), 397-415.