International Journal of Pure and Applied Mathematics
Volume 74 No. 3 2012, 405-411
ISSN: 1311-8080 (printed version)
url: http://www.ijpam.eu

ijpam.eu

GOPPA CODES ON CURVES ON A HIRZEBRUCH SURFACE

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

Abstract: Here we study Goppa codes on smooth curves contained in a Hirzebruch surface.

AMS Subject Classification: 14G15, 14H99
Key Words: Goppa code, Hirzebruch surface

1. Introduction

We work over a finite field K. We consider curves on a Hirzebruch surface and some of the Goppa codes constructed using them (in particular the minimum distance and a description of all the codewords with minimum weight). Let C be a smooth and geometrically connected curve defined over K. For any line bundle $\mathcal{A}$ on C defined over K and any $B \subseteq C(K)$ let $\mathcal{C}(B, \mathcal{A})$ denote the code obtained evaluating $H^0(C, \mathcal{A})$ at the points of B; if $\mathcal{A} \cong \mathcal{O}_C(D)$ with D an effective divisor of C defined over K and whose support contains no point of B, then $\mathcal{C}(B, \mathcal{A}) \setminus \{0\}$ is the set of all rational functions $f \in K(C)$ defined over K and with $(f) + D \geq 0$, ([2], Ch. 2, [3]) (it is the geometric Goppa code $C_{\mathcal{L}}(B, D)$ defined in [2], II.2.1). The dual code $\mathcal{C}(B, \mathcal{O}_C(D))^{\perp}$ may be described in the same way ([2], Theorem II.2.8). For any $\mathbf{w} \in \mathcal{C}(B, \mathcal{A})^{\perp} \setminus \{0\}$ let Supp($\mathbf{w}$) $\subseteq B$ denote the support of $\mathbf{w}$. Hence the Hamming weight of $\mathbf{w}$ is the integer $\sharp$(Supp($\mathbf{w}$).

Received: December 10, 2011

For any integer $e > 0$ let $X_e := \mathbb{P}(\mathcal{O}_{\mathbb{P}^1} \oplus \mathcal{O}_{\mathbb{P}^1}(e))$ denote the Hirzebruch surface, i.e. the only ruled surface of $\mathbb{P}^1$ with a section with self-intersection $-e$ ([1], §V.2). X_e is a smooth and geometrically connected projective surface defined over K. Let $\pi : X_e \to \mathbb{P}^1$ be the ruling of X_e. We call $f = \pi^{-1}(P)$, $P \in \mathbb{P}^1(K)$, the class in $\mathrm{Pic}(X_e)(K)$ of a fiber of π and as h both the class of a section of π with self-intersection $-e$ and the corresponding curve curve $h \subset X_e$ with $h \cong \mathbb{P}^1$. Since we assumed $e > 0$, the curve h is unique and it is defined over K. We have $f \cong \mathbb{P}^1$ and $h \cong \mathbb{P}^1$ and $\mathrm{Pic}(X_e)(\overline{K}) \cong \mathrm{Pic}(X_e)$. We have $h^2 = -2$, $h \cdot f = 0$ and $f^2 = 0$ (intersection numbers in $\mathrm{Pic}(X_e)$).

Theorem 1. *Fix integers e, a, b, x, y such that $e > 0$, $b \geq ea > 0$, a smooth curve $C \in |\mathcal{O}_{X_e}(ah+bf)|$ defined over K and a zero-dimensional scheme $E \subset C$. Fix integers $x \geq ey > 0$ and a set $B \subset C(K) \setminus E_{reg}$ such that $\sharp(B) + \deg(E) > ax + by - eay$. Assume either $y = a - 1$ or $y \geq a$ and $x - b \geq e(y - a) - 1$. Set $\mathcal{C}(B, \mathcal{O}_C(yh + xf)(-E))$, $m := \deg(E \cap h)$ and $m' := \sharp(B \cap h)$. Let s be the maximal integer $\deg(D \cap E)$ with $D \in |\mathcal{O}_{X_e}(f)|(\overline{K})$ and σ the set of all $D \in |\mathcal{O}_{X_e}(f)|(K)$ such that $\deg(D \cap S) = s$. Let σ' be the set of all $D \in \sigma$ such that $D \cap E = \emptyset$. Then $\mathcal{C}^\perp$ has minimum distance $\geq \min\{y + 2 - s, x - ey + 2 - m\}$. Let $\mathcal{A}$ be the set of all $S \subseteq B$ such that $S \subset D$ for some $D \in \sigma$ and $\sharp(S) = y + 2 - s$. Let $\mathcal{S}$ be the set of all $S \subseteq h \cap B$ such that $\sharp(S) = x - ey + 2 - m$ ($\mathcal{S} = \emptyset$ if and only if $m' \leq x - ey + 1 - m$).*

(i) If $y - s \leq x - ey - m$, then $\mathcal{C}^\perp$ has minimum distance $y + 2 - s$ if and only if $\mathcal{A} \neq \emptyset$. If $\mathcal{A} \neq \emptyset$, then $\mathcal{C}^\perp$ has $(\sharp(K) - 1)\sharp(\mathcal{A})$ minimum weight codewords (each codeword is uniquely determined, up to a non-zero constant, by its support and the supports are exactly the elements of $\mathcal{A}$).

(ii) f $y - s > x - ey - m$, then $\mathcal{C}^\perp$ has minimum distance $x - ey + 2 - m$ if any only if $\mathcal{S} \neq \emptyset$. If $\mathcal{S} \neq \emptyset$, then $\mathcal{C}^\perp$ has $(\sharp(K) - 1)\sharp(\mathcal{S})$ minimum weight codewords (each codeword is uniquely determined, up to a non-zero constant, by its support and the supports are exactly the elements of $\mathcal{S}$).

(iii) If $y - s = x - ey - m$, then $\mathcal{C}^\perp$ has minimum distance $y + 2 - s$ if and only if $\mathcal{A} \cup \mathcal{S} \neq \emptyset$, $\mathcal{C}^\perp$ has $(\sharp(K) - 1)\sharp(\mathcal{S} \cup \mathcal{A})$ minimum weight codewords and these codewords are described as in (i) and (ii).

For the other parameters of the code $\mathcal{C}$, see Remark 3.

Remark 1. Take the set-up of Theorem 1, but drop the assumption that either $y = a-1$ or $y \geq a$ and $x-b \geq e(y-a)-1$. Then $\mathcal{C}^\perp$ has minimum distance at least the one described in Theorem 1 and if equality holds, then the minimum weight codewords are described at in Theorem 1. Let $V \subset H^0(C, \mathcal{O}_C(yh+xf))$ be the image of the restriction map $H^0(C, \mathcal{O}_{X_e}(yh + xf)) \to H^0(C, \mathcal{O}_C(yh +$

$xf)$). The statement of Theorem 1 applies to the code obtained evaluating V at the points of B.

2. The Proof

Let $\overline{K}$ denote the algebraic closure of K. Let X be any variety or scheme defined over K and $\mathcal{F}$ any coherent sheaf on X. Let $X_{\overline{K}}$ and $\mathcal{F}_{\overline{K}}$ denote the objects obtained extending the field of coefficients from K to $\overline{K}$. For each $i \in \mathbb{N}$ we have $\dim_K(H^i(X,\mathcal{F})) = \dim_{\overline{K}} H^i(X_{\overline{K}},\mathcal{F}_{\overline{K}})$ ([1], Proposition III.9.3). Set $h^i(X,\mathcal{F}) := \dim_K H^i(X,\mathcal{F})$. This observation allows us to freely use un the next two remarks many results from [1], §V.2, only stated over $\overline{K}$.

Remark 2. Fix integers x, y. We have $h^0(X_e, \mathcal{O}_{X_e}(yh + xf)) = 0$ if and only if either $y < 0$ or $x < 0$. For all $y \geq -1$ we have $R^i\pi_*(\mathcal{O}_{X_e}(yh + xf)) = 0$ for all $i > 0$. For all $y \geq 0$ we have $\pi_*(\mathcal{O}_{X_e}(yh+xf)) \cong \oplus_{i=0}^{y}\mathcal{O}_{\mathbb{P}^1}(x-ie)$. Hence $h^i(X_e,\mathcal{O}_{X_e}(-h+xf)) = 0$, $i = 0,1$, $h^1(X_e,\mathcal{O}_{X_e}(yh+xf)) = 0$ if $y \geq 0$ and $x \geq -1+ey$ and $h^0(X_e,\mathcal{O}_{X_e}(yh+xf)) = \sum_{i=0}^{y}(x+1-ey) = (y+1)(x+1)-ey(y+1)/2$ if $y \geq 0$ and $x \geq -1$. The line bundle $\mathcal{O}_{X_e}(yh + xf)$ is spanned if and only if $y \geq 0$ and $x \geq ey$ (if $y > 0$ and $0 \leq x < ey$, then h appears in the base locus of $|\mathcal{O}_{X_e}(yh + xf)|$ with multiplicity $\lceil (ye - x)/e \rceil$). For all integers $y > 0$ and $x \geq ey$ there is a smooth and geometrically connected curve $C \in |\mathcal{O}_{X_e}(yh+xf)|$ defined over K (use [1], Proposition 2.20). Set $g(C) := p_a(C)$. We have $\omega_{X_e} \cong \mathcal{O}_{X_e}(-2h-(e+2)f)$ ([1], Lemma V.2.10). Hence the adjunction formula gives $\omega_C \cong \mathcal{O}_C((y-2)h + (x-e-2)f)$ ([1], Proposition II.8.20 or Proposition V.1.5). Hence $2g(C)-2 = \mathcal{O}_{X_e}((y-2)h + (x-e-2)f) \cdot \mathcal{O}_{X_e}(yh+xf) = -ey(y-2)+x(y-2)+(x-e-2)y$. Hence $g(C) = 1+xy-x-y-ey(y-1)/2$.

Remark 3. Fix integers x, y, a, b such that either $y = a-1$ or $x-b \geq e(y-a)-1$ and $b \geq ae > 0$. We have $h^1(X_e,\mathcal{O}_{X_e}((y-a)h + (x-b)f)) = 0$. Hence for each $C \in |\mathcal{O}_{X_e}(ah+bf)|$ the restriction map $H^0(C,\mathcal{O}_{X_e}(yh + xf)) \to H^0(C,\mathcal{O}_C(yh+xf))$ is surjective. Now assume $x \geq ey > 0$. We get $h^0(C,\mathcal{O}_C(yh+xf)) = h^0(X_e,\mathcal{O}_{X_e}(yh+xf)) - h^0(X_e,\mathcal{O}_{X_e}((y-a)h+(x-b)f)) = (y+1)(x+1)-ey(y+1)/2-(y+1-a)(x+1-b)-e(y-a)(y-a+1)$ (Remark 2). Let $E \subset C$ be a zero-dimensional scheme. We have $\deg(\mathcal{O}_C(yh+xf)(-E)) = ay+bx-eay-\deg(E)$. If $h^1(X_e,\mathcal{I}_E(yh+xf)) = 0$, then $k := h^0(C,\mathcal{O}_C(yh + xf)(-E)) = h^0(C,\mathcal{O}_C(yh+xf)) - \deg(E)$. If $\sharp(B) > ay+bx-eay-\deg(E)$, then $\mathcal{C}$ is an $[n,k]$-code.

Remark 4. Let W be any projective scheme and L a line bundle on it. Fix any subscheme $E \subseteq Z$. Since Z is zero-dimensional, we have $h^1(Z,\mathcal{I}_{E,Z}(x,y)) >$

0. Hence the restriction map $H^0(Z, L|Z) \to H^0(E, L|E)$ is surjective. Hence if E imposes at most $\deg(E)-1$ condition to $H^0(W, L)$, then Z imposes at most $\deg(Z)-1$ condition to $H^0(W, L)$. If $h^i(W, L) = 0$ for all $i \geq 2$, this is equivalent to say that if $h^1(W, \mathcal{I}_E \otimes L) > h^1(W, L)$, then $h^1(W, \mathcal{I}_Z \otimes L) > h^1(W, L)$. We also get $h^1(W, \mathcal{I}_Z \otimes L) \geq h^1(W, \mathcal{I}_E \otimes L)$.

Remark 5. Let W be any projective scheme, Z a closed subscheme of W, D an effective Cartier divisor on W and L a line bundle on W. Let $\mathrm{Res}_D(Z)$ be the closed subscheme of W with $\mathcal{I}_Z : \mathcal{I}_D$ as its ideal sheaf. We have $\mathrm{Res}_D(Z) \subseteq Z$ and an exact sequence

$$0 \to \mathcal{I}_{\mathrm{Res}_D(Z)} \otimes L(-D) \to \mathcal{I}_Z \otimes L \to \mathcal{I}_{Z\cap D, D} \otimes (L|D) \to 0 \qquad (1)$$

From (1) we get

$$h^i(W, \mathcal{I}_Z \otimes L) \leq h^i(W, \mathcal{I}_{\mathrm{Res}_D(Z)} \otimes L(-D)) + h^i(D, \mathcal{I}_{Z\cap D, D} \otimes (L|D))$$

for all $i \geq 0$. If Z is zero-dimensional, then $\deg(Z) = \deg(\mathrm{Res}_D(Z)) + \deg(Z \cap D)$.

Lemma 1. *Fix non-negative integers e, x, y such that $x \geq ey$. Fix any $T \in |\mathcal{O}_{X_e}(h)|$ and any $D \in |\mathcal{O}_{X_e}(f)|$. Set $J := T \cup D$. Let $Z \subset J$ be a zero-dimensional scheme such that either $T \cap D \notin Z_{red}$ or the connected component of Z with $T \cap D$ as its support is reduced.*

(i) We have $h^1(X_e, \mathcal{I}_Z(yh+xf)) = h^1(J, \mathcal{I}_{Z,J}(yh+xf))$ and $h^1(X_e, \mathcal{I}_Z(yh+xf)) = \deg(Z) - h^0(X_e, \mathcal{O}_{X_e}(yh+xf)) + h^0(X_e, \mathcal{I}_Z(yh+xf)$.

(ii) $h^1(X_e, \mathcal{I}_Z(yh+xf)) > 0$ if and only if either $\deg(Z \cap D) \geq y+2$ or $\deg(Z \cap h) \geq x - ey + 2$ or $\deg(Z) = x - (e-1)y + 2$.

Proof. Part (i) follows from $h^1(X_e, \mathcal{O}_{X_e}(yh+xf)) = h^0(X_e, \mathcal{O}_{X_e}((y-1)h+(x-1)f) = 0$ (Remark 4). We have $h^0(D, \mathcal{O}_D(yh+xf)) = y+1$, $h^1(D, \mathcal{O}_D((h-1)y+xf)) = 0$ and $h^0(T, \mathcal{O}_T(yh+xf) = x-ey+1$. Since the scheme-theoretic intersection $T \cap D$ is a point, a Mayer-Vietoris exact sequence gives $h^0(J, \mathcal{O}_J(yh+xf)) = x-(e-1)y+1$. Hence the " if " part of (ii) follows from Remark 4. Now assume $\deg(Z\cap T) \leq x-ey+1$, $\deg(Z\cap T) \leq y+1$. By part (ii) it is sufficient to prove that $h^1(X_e, \mathcal{I}_Z(yh+xf)) = 0$ if $\deg(Z) \neq x-(e-1)y+2$. We have $\deg(Z) = \deg(Z\cap T) + \deg(Z \cap D) - \epsilon$ with $\epsilon = 0$ if $T \cap D \in Z_{red}$ and $\epsilon = 1$ if $T \cap D \subset Z$. Hence $\deg(Z) = x - (e-1)y + 2$ if and only if $\deg(Z \cap D) = y+1$, $\deg(Z\cap T) = x-ey+1$ and $D \cap T \nsubseteq Z$. We exclude also this case. First assume $\deg(Z\cap T) = x-ey+1$. Hence $h^1(T, \mathcal{I}_{Z\cap T}(yh+xf)) = 0$, $i = 0, 1$. Hence (1) gives $h^1(X_e, \mathcal{I}_{\mathrm{Res}_T(Z)}((y-1)h+xf)) = h^1(X_e, \mathcal{I}_Z(yh+$

$xf)$). Our assumptions imply $\mathrm{Res}_T(Z) \subset D$ and $\deg(\mathrm{Res}_T(Z)) \le y$. Hence $h^1(D, \mathcal{I}_{\mathrm{Res}_T(Z)}((y-1)h+xf)) = 0$. Since $h^1(X_e, \mathcal{O}_{X_e}((y-1)h+(x-1)f)) = 0$ (Remark 4), we get $h^1(X_e, \mathcal{I}_{\mathrm{Res}_T(Z)}((y-1)h+xf)) = 0$. Remark 5 gives $h^1(X_e, \mathcal{I}_Z(yh+xf)) = 0$. Now assume $\deg(Z \cap T) \le x - ey$. Since $\deg(D \cap Z) \le y+1$, we have $h^1(X_e, \mathcal{I}_{Z\cap D}(yh+xf)) = h^1(D, ,I_{Z\cap D}(yh+xf)) = 0$. Remark 5 gives $h^1(X_e, \mathcal{I}_Z(yh+xf)) \le h^1(X_e, \mathcal{I}_{\mathrm{Res}_D(Z)}(yh+(x-1))$. We have $\mathrm{Res}_D(Z) = Z\cap D \setminus D \cap T$ and hence $\deg(\mathrm{Res}_D(Z) \le x - ey$. Hence the game with D just done gives $h^1(X_e, \mathcal{I}_{\mathrm{Res}_D(Z)}(yh+(x-1)) = 0$. □

Lemma 2. *Fix integers $e > 0$, $x \ge ey$, $z \ge 0$ and a zero-dimensional scheme $Z \subset X_e$ such that $\deg(Z) = z$. Set $c := \deg(Z \cap h)$ and assume that each connected component of Z intersecting h is contained in h. Let η be the set of all $D \in |\mathcal{O}_{X_e}(f)|(\overline{K})$ such that $\deg(D \cap Z)$ such that $t := \deg(D\cap Z)$ is maximal. Set $\eta' := \{D \in \sigma : D \cap h \cap Z = \emptyset\}$. Assume either $z \le y+2$ or $z \le c + \min\{x, y+2\}$.*

(i) If either $c \ge x - ey + 2$ or $t \ge y+2$ or $\deg((D\cup h)\cap Z) = x-(e-1)y+2$, then $h^1(X_e, \mathcal{I}_Z(x,y)) > 0$.

(ii) Assume $c \le x - ey + 1$ and $t \le y+1$. We have $h^1(X_e, \mathcal{I}_Z(yh+xf)) > 0$ if and only if $c = x - ey + 1$, $t = y+1$ and $\eta' \ne \emptyset$; in this case we have $h^1(X_e, \mathcal{I}_Z(yh+xf)) = 1$, $\eta = \eta'$ has a unique element, D, and $Z \subset D \cup h$. If Z is defined over K, then D is defined over K.

(iii) Assume $c \le x - ey + 1$, $z - c \le y + 2$ and either $c \le x - ey$ or $\eta' = \emptyset$. We have $h^1(X_e, \mathcal{I}_Z(yh+zf)) > 0$ if and only if $t = y+2$. In this case η has a unique element, D, and $Z \subset h \cup D$. If Z is defined over K, then D is defined over K.

(iv) If $c \ge x - ey + 1$ and $z \le c + y$, then $h^1(X_e, \mathcal{I}_Z(hy+xf)) = c - x + ey - 1$.

Proof. Since $x \ge ey - 1$, we have $h^1(X_e, \mathcal{O}_{X_e}(yh+xf)) = 0$. Hence $h^1(X_e, \mathcal{I}_Z(yh+xf)) > 0$ if and only if $h^0(X_e, \mathcal{O}_{X_e}(yh+xf)) - \deg(Z)$. For any $D \in |\mathcal{O}_{X_e}(f)(\overline{K})|$ we have $h^0(D, \mathcal{O}_D(yh+xf)) = y+1$. Hence if $\deg(Z\cap D) \ge y+2$, then $D \cap Z$ imposes $< \deg(Z \cap D)$ conditions to $H^0(D, \mathcal{O}_{X_e}(yh+xf))$ and hence to $H^0(X_e, \mathcal{O}_{X_e}(yh+xf))$ (Remark 4). Similarly, since $h^0(h, \mathcal{O}_h(yh+xf)) = x - ey + 1$, we get that if $c \ge x - ey + 1$, then $h^1(X_e, \mathcal{I}_Z(hy+xf)) \ge c - x + ey - 1 > 0$ (Remark 4).

(a) Here we assume $\deg(Z\cap h) \le x - ey + 1$. Fix $D_1 \in |\mathcal{O}_{X_e}(f)|(\overline{K})$ such that $a_1 := \deg(Z \cap D_1)$ is maximal among all $D \in |\mathcal{O}_{X_e}(f)|(\overline{K})t$. If $a_1 \ge y+2$, then we are done. Hence we may assume $a_1 \le y+1$. Set $J := h \cup D_1$. Lemma

1 gives $h^1(J,\mathcal{I}_{J\cap Z}(yh+xf))>0$ if and only if $T\cap D_1\notin Z$, $\deg(D_1\cap Z)=y+1$ and $\deg(T\cap Z)=x-ey+1$. Hence we may assume $h^1(J,\mathcal{I}_{Z\cap J,J}(yh+xf))=0$. Set $E:=\mathrm{Res}_J(Z)$. Remark 5 gives $h^1(X_e,\mathcal{I}_Z(yh+xf))\le h^1(X_e,\mathcal{I}_E((y-1)h+(x-1)f))$. By assumption $h\cap E=\emptyset$. Set $Z_1:=E$ and $z_1:=\deg(E)$. Let $D_2\in|\mathcal{O}_{X_e}(h)|(\overline{K})$ such that $a_2:=\deg(D_1\cap E)$ is maximal and set $J_2:=T\cup D_2$ and $E_2:=\mathrm{Res}_{D_2}(E)$. We have $\deg(E_2)=z_1-a_2$ (Remark 5). For all integers $i\ge 3$ define inductively the curves $D_i|\mathcal{O}_{X_e}(h)|(\overline{K})$, the scheme $E_i\subseteq E_{i-1}$ and the integers a_i and z_i in the following way. Fix any $D_i|\mathcal{O}_{X_e}(h)|$ such that $a_i:=\deg(D_i\cap E_{i-1})$ is maximal and set $E_i:=\mathrm{Res}_{D_i}(E_{i-1})$. The maximality property of the integers a_i gives that the sequence $\{a_i\}$ is non-decreasing. Since $|\mathcal{O}_{X_e}(h)|$ has no base points, we have $E_i=\emptyset$ (and hence $a_j=0$ for all $j>0$) if $z_{i-1}\le 1$. Hence $E_i=\emptyset$ for all $i\gg 0$.

(a1) Here we assume $a_i\le y-i+1$ for all $2\le i\le y-1$. Applying Remark 5 $y-2$ times we get $h^1(X_e,\mathcal{I}_Z(hy+xf))\le h^1(X_e,\mathcal{I}_{E_{y-1}}((x-y)f))$. Since $a_y\le 1$, we get that $\pi|\mathcal{E}_{y-1}$ is an isomorphism onto a degree $\deg(E_{y-1})$ subscheme of $\mathbb{P}^1$. Since $\pi^*(H^0(\mathbb{P}^1,\mathcal{O}_{\mathbb{P}^1}(x-y)))\to H^0(X_e,\mathcal{O}_{X_e})((x-y)f)$ is an isomorphism, we get $h^1(X_e,\mathcal{I}_{E_{y-1}}((x-y)f))=0$ if $\deg(E_{y-1})\le x-y+1$. Hence $h^1(X_e,\mathcal{I}_Z(hy+xf))=0$ if $z\le c+x$ (under the assumption $a_i\le y-i+1$ for all $2\le i\le y$).

(a2) Assume the existence of an integer $i\in\{2,\dots,y-1\}$ such that $a_i\ge y-i+2$ and call w the minimal such an integer. First assume $w\le e$. Set $A':=D_2+\cdot+D_{w-1}$ and $A:=A'\cup J$ (as effective divisor of X_e, not as a set, because we may have $D_i=D_j$ even if $i\ne j$). We have $h^1(X_e,\mathcal{I}_{A'\cap Z}(((y-1)h+(x-1)f))=0$ and hence $h^1(X_e,\mathcal{I}_{A\cap Z}(yh+xf))=0$ (Remark 5). Thus $h^1(X_e,\mathcal{I}_Z(yh+xf))\le h^1(X_e,\mathcal{I}_{\mathrm{Res}_A(Z)}((y-1)+(x-w)f))$. We have $\deg(A\cap Z)=c+a_1+\cdots+a_w\ge c+wa_w\ge c+w(y-w+4)$. The function $\phi:[0,y+4]\to\mathbb{R}$ defined by $\phi(t)=t(y+4-t)$ is increasing for $0\le t\le (y+4)/2$ and decreasing for $(y+4)/2\le t\le y+4$. First assume $w=3$, i.e. $a_1=a_2=y+1$. Hence $z\ge c+2y+2$, absurd. Now assume $w=y-1$. We get $\deg(Z)\ge c+5y-5$, absurd. Now assume $w>e$. We get $z\ge c+w(y+4-w)$. Since $w\le y-1$ and either $z\le y+2$ or $z\le c+y$, we get a contradiction (even in the case $w=y-1$).

(a3) Since $\overline{K}$ is a Galois extension of K, the uniqueness of D in (ii) and (iii) implies that D is defined over K.

(b) Assume $c\ge x-ey+1$ and $z\le c+y$. We have $\deg(\mathrm{Res}_h(Z))=z-c$. Our assumptions on Z gives $\mathrm{Res}_h(Z)\cap h)=\emptyset$. By step == we get $h^1(X_e,\mathcal{I}_{\mathrm{Res}_h(Z)}((y-1)h+xf))=0$. Hence (1) gives $h^1(X_e,\mathcal{I}_Z(hy+xf))=c-x+ey-1$. □

Proof of Theorem 1. By the definition of $\mathcal{C}^\perp$ the minimum distance of $\mathcal{C}^\perp$ is the minimal cardinality of a set $S \subseteq B$ such that $h^0(C, \mathcal{O}_C(yh+xf)(-E-S)) > h^0(C, \mathcal{O}_C(yh+xf)(-E)) - \sharp(S)$, i.e. such that $h^1(C, \mathcal{O}_C(yh+xf)(-E-S)) > h^1(C, \mathcal{O}_C(yh+xf)(-E))$ (Riemann-Roch) Since $m \le x - ey + 1$ and $s \le y + 1$, Lemma 2 gives $h^1(C, \mathcal{O}_C(yh + xf)(-E)) = h^1(C, \mathcal{O}_C(yh + xf))$. Hence the minimum distance of $\mathcal{C}^\perp$ is the minimal cardinality of a set $S \subseteq B$ such that $h^1(C, \mathcal{O}_C(yh + xf)(-E - S)) > h^1(\mathcal{O}_C(yh + xf))$. By Remarks 2 and 3 this is the minimal cardinality of a subset $S \subseteq B$ such that

Fix any $S \subseteq B$ supporting a codeword of $\mathcal{C}^\perp$ with minimum codeword. There is a unique, up to a non-zero scalar, codeword with S as its support. □

Acknowledgements

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

References

[1] R. Hatshorne, *Algebraic Geometry*, Springer-Verlag, Berlin (1977).

[2] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer, Berlin (1993).

[3] J.H. van Lint, G. van der Geer, *Introduction to Coding Theory and Algebraic Geometry*, DMV Seminar, **12**, Birkhäuser Verlag, Basel (1988).