International Journal of Pure and Applied Mathematics
Volume 85 No. 5 2013, 891-906
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
doi: http://dx.doi.org/10.12732/ijpam.v85i5.8

ijpam.eu

LOW WEIGHT CODEWORDS OF CODES COMING FROM SMOOTH CURVES IN THE HERMITIAN SURFACE

E. Ballico

Department of Mathematics
University of Trento
38 123 Povo (Trento) - Via Sommarive, 14, ITALY

Abstract: Here we describe all codewords with low weight on certain Goppa codes of curves contained in a Hermitian surface $\mathcal{H}$ over $\mathbb{F}_{q^2}$. We also show how to construct curves $C \subset \mathcal{H}$ with good cohomological properties (arithmetically Cohen-Macaulay curves).

AMS Subject Classification: 11G20, 14H50, 14N05, 14Q05
Key Words: Hermitian surface, dual code, low weight codeword, evaluation code, algebraic-geometric code, arithmetically Cohen-Macaulay curve

1. Introduction

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 $(f) + D \geq 0$ at the points of B ([20], [21]). 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 $supp(w)$. In many cases

Received: March 10, 2013

the vector space $H^0(C,\mathcal{L})$ embeds B into a projective space $\mathbb{P}^{k-1}$ and in that case we may look at the code $\mathcal{C}(B,\mathcal{L})$ as an evaluation code ([15], [16]). In many cases one uses both approaches, i.e. take C as a curve inside a projective space $\mathbb{P}^r$ and then uses this embedding to construct $\mathcal{L}$ (see e.g. [17] for a higher dimensional case). In the case in which $\mathcal{L}$ is of the restriction of some line bundle $\mathcal{O}_{\mathbb{P}^r}(x))$, $x>0$, and C is a complete intersection inside $\mathbb{P}^r$, then one can use this approach to guess where to find low weight codewords of $\mathcal{C}(B,\mathcal{L})^\perp$ and often get lower bounds for the minimum distance of $\mathcal{C}(B,\mathcal{L})^\perp$. It is interesting to extend this approach to more general line bundles $\mathcal{L}$ and to many curves C with large $\sharp(C(K))$. Maximal curves always are contained in a Hermitian variety ([10], [14], §10.3, and references therein) and high genus maximal curves are contained in a low dimensional Hermitian variety ([14], Corollary 10.25). Here we look at curves inside the Hermitian surface (all curves, not only the one which are maximal). For the osculating properties of these curves, see

We take $K=\mathbb{F}_{q^2}$. Take homogeneous coordinates x_0,x_1,x_2,x_3 of $\mathbb{P}^3$. Set $\mathcal{H}=\{x_0^{q+1}+x_1^{q+1}+x_2^{q+1}+x_3^{q+1}=0\}$. $\mathcal{H}$ is a geometrically integral and smooth surface. The set $\mathcal{H}(\mathbb{F}_{q^2})$ is so important that it deserved a name: it is the Hermitian surface ([12], Ch. 19, [13], Ch. 23) or the non-singular Hermitian surface of $PG(3,q^2)$. Some maximal curves with large genus are conThe evaluation codes obtained from $\mathcal{H}(\mathbb{F}_{q^2})$ deserved a detailed analysis in the literature ([4], [5], [6], [9] and references therein), but only if $\mathcal{L}=\mathcal{O}_{\mathcal{H}}(t)$ for some $t\in\mathbb{N}$. See [9] for maximal curves contained in $\mathcal{H}$. The surface $\mathcal{H}$ has a rich geometry and many line bundles defined over $\mathbb{F}_{q^2}$, but not isomorphic to some $\mathcal{O}_{\mathcal{H}}(t)$, $t\in\mathbb{Z}$. Let Φ be the set of all lines contained in $\mathcal{H}$ and defined over $\mathbb{F}_{q^2}$. We have $\sharp(\Phi)=(q+1)(q^3+1)$ ([12], Theorem 19.1.5). To get nice line bundles on $\mathcal{H}$ we use the geometry of lines contained in $\mathcal{H}$. A curve $C\subset\mathbb{P}^r$ is said to be arithmetically Cohen-Macaulay if $h^1(\mathbb{P}^r,\mathcal{I}_C(t))=0$ for all $t\geq 0$ (e.g. a complete intersection curve is arithmetically Cohen-Macaulay). By definition for these curves the condition $h^1(\mathbb{P}^3,\mathcal{I}_C(x))=0$ in the statements of Theorem 1 and 2 below is satisfied. See section 4 for a construction of arithmetically Cohen-Macaulay curves on $\mathcal{H}$.

For curves we prove the following results.

Theorem 1. *Let $C\subset\mathcal{H}$ be a geometrically integral smooth curve defined over $\mathbb{F}_{q^2}$. Fix an integer x such that $q\leq x\leq q^2-1$, $h^1(\mathbb{P}^3,\mathcal{I}_C(x))=0$ and a zero-dimensional scheme $E\subset C$ defined over $\mathbb{F}_{q^2}$. Assume $\deg(E)\leq x+1$. Fix $B\subseteq C(\mathbb{F}_{q^2})$ such that $B\cap E_{red}=\emptyset$. For any $L\in\Phi$ set $e_L(E):=\deg(E\cap L)$ and $f_L(B):=\sharp(B\cap L)$. Set $\mathcal{C}:=\mathcal{C}(B,\mathcal{O}_C(x)(-E))$. Assume $\sharp(B)+\deg(E)>x\cdot\deg(C)$. Let Φ_0 be the set of all $L\in\Phi$ such that $e_L(E)+f_L(B)\geq x+2$*

(a) If $\Phi_0 = \emptyset$, then the dual code $\mathcal{C}^{\perp}$ has minimum distance $\geq 2x+2-\deg(E)$.

(b) Assume $\Phi_0 \neq \emptyset$ Let w be a non-zero codeword of $\mathcal{C}$ with weight $\leq 2x+1-\deg(E)$. Then the support, S, of w is a set $S \subset L \cap B$ for some $L \in \Psi_0$ and $x+2-e_L(E) \leq \sharp(S) \leq f_L(E)$.

(c) Assume $\Phi_0 \neq \emptyset$ and take any $L \in \Phi_0$ and any $S \subseteq L \cap B$ such that $x+2-e_L(E) \leq \sharp(S) \leq f_L(E)$. Then S is the support of a codeword of $\mathcal{C}^{\perp}$.

Remark 1. By [3], Theorem at page 492, every geometrically integral curve $C \subset \mathbb{P}^r$, $r \geq 3$, satisfies $h^1(\mathbb{P}^r, \mathcal{I}_C(t)) = 0$ if either $t \geq \deg(C) - r + 1$ or $t = \deg(C) - r$ and C is not isomorphic to $\mathbb{P}^1$. Hence in the statement of Theorem 1 we may drop the condition " $h^1(\mathbb{P}^3, \mathcal{I}_C(x)) = 0$ " if $x \geq \deg(C) - 2$ and (except trivial cases) even if $x = \deg(C) - 2$. If in the statement of Theorem 1 we drop the assumption " $h^1(\mathbb{P}^r, \mathcal{I}_C(t)) = 0$ ", then parts (a) and (b) are still true. This part for arbitrary C may be used to get a quick test if a curve $C \subset \mathcal{H}$ with large $\sharp(C(\mathbb{F}_{q^2}))$ is suitable to get a code (we recall that for any line $L \subset \mathcal{H}$ and any curve $C \subset \mathcal{H}$ not containing L the integer $\deg(D \cap L)$ is the same for all $D \in |\mathcal{O}_{\mathcal{H}}(C)|$).

Set $n := \sharp(B)$ and $k := h^0(C, \mathcal{O}_C(x)) - \deg(E)$. The code $\mathcal{C}$ is an $[n, k]$-code (see Lemma 1).

In the case $E = \emptyset$ an easy modification of the proofs of [2], Theorem 3.5 and 3.8, gives the following result.

Theorem 2. *Let $C \subset \mathcal{H}$ be a geometrically integral smooth curve defined over $\mathbb{F}_{q^2}$. Fix an integer x such that $q \leq x \leq q^2-1$, $h^1(\mathbb{P}^3, \mathcal{I}_C(x)) = 0$ and a set $B \subseteq C(\mathbb{F}_{q^2})$. For any $L \in \Phi$ set $f_L(B) := \sharp(B \cap L)$. Set $\mathcal{C} := \mathcal{C}(B, \mathcal{O}_C(x)(-E))$. Assume $\sharp(B) > x \cdot \deg(C)$. For any integer t let $\Phi(t, B)$ be the set of all $L \in \Phi$ such that $f_L(B) \geq t$. Let $\Phi(=, B, x+1)$ denote the set of all reducible conics $L \cup R$ with $L, R \in \Phi$, $f_L(B) \geq x+1$, $f_R(B) \geq x+1$ and $\sharp((L \cap R) \cap B)) \geq 2x+2$.*

(a) If $\Phi(x+2, B) = \emptyset =$ and $\Phi(=, x+1, B) = \emptyset$, then the dual code $\mathcal{C}^{\perp}$ has minimum distance $\geq 3x$.

(b) Every codeword of $\mathcal{C}^{\perp}$ with weight at most $3x-1$ has either support contained in an element of $\Phi(x+2, B)$ or the disjoint union of two elements of $\Phi(x+2, B)$ or an element of $\Phi(=, x+1, B)$.

(c) Fix a set $S \subset B$ such that $\sharp(B) \leq 3x-1$. S is the support of a codeword of $\mathcal{C}^{\perp}$ if and only if one of the following cases occur:

(i) $\sharp(S) \geq x+2$ and there is $L \in \Phi(B, x+2)$ such that $S \subset L$;

(ii) $\sharp(S) \geq 2x+4$; *and there are* $L, R \in \Phi(B, x+2)$ *such that* $S \subset L \cup R$, $\sharp(S \cap L) \geq x+2$ *and* $\sharp(S \cap R) \geq x+2$;

(iii) $\sharp(S) \geq 2x+2$ *and there is* $L \cup R \in \Phi(=, B, x+1)$ *such that* $S \subset L \cup R$, $\sharp(S \cap L) \geq x+1$ *and* $\sharp(S \cap L) \geq x+1$.

Obviously, in (ii) (resp. (iii)) we need $x \geq 5$ (resp. $x \geq 3$), because we assumed $\sharp(S) \leq 3x-1$

2. Preliminary Lemmas

The following lemma is a straightforward extension of [2], Lemma 3.3.

Lemma 1. *Fix an integer* $x > 0$ *and a smooth and geometrically connected curve* $C \subset \mathbb{P}^r$ *over a finite field* K *such that* $h^1(\mathbb{P}^r, \mathcal{I}_C(x)) = 0$. *Let* $E \subset C$ *be a zero-dimensional scheme defined over* K *and* $B \subset C(K) \setminus E_{red}$ *such that either* $\sharp(B) + \deg(E) > x \cdot \deg(C)$ *or* $h^0(C, \mathcal{O}_C(x)(-E-B)) = 0$. *Set* $\mathcal{C} := \mathcal{C}(B, \mathcal{O}_C(x)(-E))$. *The code* $\mathcal{C}$ *is an* $[n,k]$*-code over* K *with* $n := \sharp(B)$ *and* $k := h^0(C, \mathcal{O}_C(x)(-E))$. *A set* $A \subseteq B$ *contains (resp. is) the support of a codeword of* $\mathcal{C}^\perp$ *if and only if* $h^1(\mathbb{P}^r, \mathcal{I}_{E\cup A}(x)) > h^1(\mathcal{I}_E(x))$ *(resp.* $h^1(\mathbb{P}^r, \mathcal{I}_{E\cup A}(x)) > h^1(\mathcal{I}_{E\cup A'}(x))$ *for all* $A' \subsetneq A$*). The set of all codewords of* $\mathcal{C}^\perp$ *whose support is contained in* A *is a* K*-vector space of dimension* $h^1(\mathbb{P}^r, \mathcal{I}_{E\cup A}(x)) - h^1(\mathcal{I}_E(x))$.

Proof. Since $B \cap E = \emptyset$, we have $h^0(C, \mathcal{O}_C(x)(-E-B)) = 0$ if and only if the evaluation map $H^0(C, \mathcal{O}_C(x)(-E)) \to H^0(B, \mathcal{O}_C(x)(-E)|B)$ is injective, i.e. if and only if $\mathcal{C}$ is an $[n,k]$-code. If $\sharp(B) + \deg(E) > x \cdot \deg(C)$, then $\deg(\mathcal{O}_C(x)(-E-B)) < 0$ and hence $h^0(C, \mathcal{O}_C(x)(-E-B)) = 0$. A set $A \subseteq B$, $A \neq \emptyset$, contains the support of a codeword w of $\mathcal{C}$ if and only if the evaluations associated to the point of A are not linearly independent, i.e. if and only if $h^0(C, \mathcal{O}_C(x)(-E-A)) > h^0(C, \mathcal{O}_C(x))(-E) - \sharp(A)$. Since we assumed $h^1(\mathbb{P}^r, \mathcal{I}_C(x)) = 0$, $E \subset C$ and $E \cap A = \emptyset$, then the restriction map $H^0(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(x)) \to H^0(C, \mathcal{O}_C(x))$ is surjective. Hence $h^0(\mathbb{P}^r, \mathcal{I}_{E\cup A}(x)) > h^0(\mathbb{P}^r, \mathcal{I}_E(x)) - \sharp(A)$. Since

$$h^1(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(x)) = 0,$$

$$h^0(\mathbb{P}^r, \mathcal{I}_{E\cup A}(x)) > h^0(\mathbb{P}^r, \mathcal{I}_E(x)) - \sharp(A)$$

if and only if $h^1(\mathbb{P}^r, \mathcal{I}_{E\cup A}(x)) > h^1(\mathcal{I}_E(x))$. □

With the terminology of [2], §2, the finite set A is said to be minimally x-linked if $h^1(\mathbb{P}^r, \mathcal{I}_A(x)) > h^1(\mathbb{P}^r, \mathcal{I}_{A'}(x))$ for all $A' \subsetneq A$ (it is sufficient to test the sets $A' \subset A$ such that $\sharp(A') = \sharp(A) - 1$. Theorem 1 and 2 are easily translated in the classifications of certain minimally $\mathcal{I}_E(x)$-linked sets (see Lemmas 7 and 8) for the results quoted later.

Remark 2. 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 $h^1(W, \mathcal{I}_W \otimes L) > 0$, then $h^1(W, \mathcal{I}_Z \otimes L) > 0$.

Remark 3. For any hypersurface $T \subset \mathbb{P}^r$ and any zero-dimensional subscheme $Z \subset \mathbb{P}^r$ let $\mathrm{Res}_T(Z)$ denote the residual scheme of Z with respect to T, i.e. the closed subscheme of $\mathbb{P}^r$ with $\mathcal{I}_Z : \mathcal{I}_T$ has its ideal sheaf. We have $\deg(Z) = \deg(Z \cap T) + \deg(\mathrm{Res}_T(Z))$. If $Z = Z_1 \sqcup Z_2$, then $\mathrm{Res}_T(Z) = \mathrm{Res}_T(Z_1) \sqcup \mathrm{Res}_T(Z_2)$. If Z is reduced (i.e. if Z is a finite set), then $\mathrm{Res}_T(Z) = Z \setminus Z \cap T$. For each $d \in \mathbb{Z}$ we have an exact sequence

$$0 \to \mathcal{I}_{\mathrm{Res}_T(Z)}(d-k) \to \mathcal{I}_Z(d) \to \mathcal{I}_{Z\cap T,T}(d) \to 0 \tag{1}$$

where $k := \deg(T)$. Hence for each integer $i \geq 0$ we have

$$h^i(\mathbb{P}^2, \mathcal{I}_Z(d)) \leq h^i(\mathbb{P}^2, \mathcal{I}_{\mathrm{Res}_T(Z)}(d-k)) + h^i(T, \mathcal{I}_{Z\cap T,T}(d)) \tag{2}$$

The following 6 lemmas are an easy modification of the proofs of [2], Theorem 3.5 and 3.8.

Lemma 2. *Fix a line $L \subset \mathbb{P}^2$ and a set $S \subset L$. If $\sharp(S) - \sharp(L \cap S) + \deg(E) - \deg(E \cap L) \leq d$, then $h^1(\mathbb{P}^2, \mathcal{I}_{E\cup S}(d)) = h^1(L, \mathcal{I}_{(E\cup S)\cap L,L}(d)) = \max\{0, \deg(E \cap L) + \sharp(L \cap S) - d - 1\}$.*

Proof. Since $E \cap S = \emptyset$, we have $\deg(E\cup S) = \deg(E) + \deg(S)$, $\deg(\mathrm{Res}_L(E \cup S)) = \deg(\mathrm{Res}_L(E)) + \sharp(S) - \sharp(S \cap L)$ and $\deg(L \cap (E \cup S)) = \deg(E \cap L) + \sharp(S \cap L)$. The latter equality gives $h^1(L, \mathcal{I}_{(E\cup S)\cap L,L}(d)) = \max\{0, \deg(E \cap L) + \sharp(L \cap S) - d - 1\}$, because $L \cong \mathbb{P}^1$. Since $\deg(\mathrm{Res}_L(E \cup S)) \leq d$, we have $h^1(\mathbb{P}^2, \mathcal{I}_{\mathrm{Res}_L(E\cup L)}(d-1)) = 0$ ([1], Lemma 34, or [8], Remarque (i) at p. 116). Hence (2) gives $h^1(\mathbb{P}^2, \mathcal{I}_{E\cup S}(d)) \leq h^1(L, \mathcal{I}_{(E\cup S)\cap L,L}(d))$. Since $(E\cup S)\cap L \subseteq E \cup S$, Remark 2 gives $h^1(\mathbb{P}^2, \mathcal{I}_{E\cup S}(d)) \geq h^1(L, \mathcal{I}_{(E\cup S)\cap L,L}(d))$. □

Lemma 3. *Fix an integer $x > 0$ and lines $L, R \in \mathbb{P}^r$, $r \geq 2$, such that $L \neq R$ and $L \cap R \neq \emptyset$. Set $\{O\} := L \cap R$. Fix a finite set $S \subset L \cup R$ such that $\sharp(S \cap L) \geq \sharp(S \cap R)$ and $S \neq \emptyset$.*

(a) We have $h^1(\mathbb{P}^r, \mathcal{I}_S(x)) > 0$ if and only if either $\sharp(S \cap L) \geq x + 2$ or $\sharp(S) \geq 2x + 2$.

(b) We have $h^1(\mathbb{P}^r, \mathcal{I}_S(x)) > h^1(\mathbb{P}^r, \mathcal{I}_{S'}(x))$ *for all* $S' \subsetneq S$ *if and only if either* $S \subset L$ *and* $\sharp(S) \geq x+2$ *or* $\sharp(S \cap L) \geq x+2$ *and* $\sharp(S \cap R) \geq x+1$ *or* $\sharp(S \cap L) = \sharp(S \cap R) = x+1$ *and* $O \notin S$.

Proof. Since $\sharp(S \cap L) \geq \sharp(S \cap R)$, we have $\sharp(S \cap L) \leq x+1$ and $\sharp(S) \geq 2x+2$ if and only if $\sharp(S \cap L) = \sharp(S \cap R) = x+1$ and $O \notin S$. Fix a finite set $A \subset L \cup R$ such that $\sharp(A \cap L) \geq \sharp(A \cap R)$. Since the restriction map $H^0(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(x)) \to H^0(L \cup R, \mathcal{O}_{L \cup R}(x))$ is surjective, we have $h^1(\mathbb{P}^r, \mathcal{I}_S(x)) = h^1(L \cup R, \mathcal{I}_{A, L \cup R}(x))$. Since $h^0(L \cup R, \mathcal{O}_{L \cup R}(x)) = \binom{x+2}{2} - \binom{x}{2} = 2x+1$, we have $h^1(L \cup R, \mathcal{I}_{A, L \cup R}(x)) \geq \max\{0, \sharp(S) - 2x - 1\}$. Since $h^1(L \cup R, \mathcal{O}_A L \cup R(x)) = 0$, we also have $h^1(L \cup R, \mathcal{I}_{A, L \cup R}(x)) - h^0(L \cup R, \mathcal{I}_{A, L \cup R}(x)) = \sharp(A) - 2x - 1$. Since $L \cong R \cong \mathbb{P}^1$, we have $h^1(L, \mathcal{I}_{F,L}(x)) = \max\{0, \sharp(F) - x - 1\}$ and $h^0(R, \mathcal{I}_{F,L}(x)) = \max\{0, x+1-\sharp(F)\}$ for all finite sets $F \subset L$ and similarly for any finite subset of R. Consider the Mayer-Vietoris exact sequence

$$0 \to \mathcal{O}_{L \cup R}(x) \to \mathcal{O}_L(x) \oplus \mathcal{O}_R(x) \to \mathcal{O}_{\{O\}} \to 0 \tag{3}$$

Set $A' := A \setminus A \cap L$. Notice that $A' = A \cap R$ if $O \notin A$ and $A' = A \cap L \setminus \{O\}$ if $O \in A$. First assume $\sharp(A \cap L) \geq x+1$. Hence $h^0(L, \mathcal{I}_{A \cap L, L}(x)) = 0$. From (3) we get $h^0(L \cup R, \mathcal{I}_{A, L \cup R}(x)) = h^0(R, \mathcal{I}_{A'}(x)) = \max\{0, x - \sharp(A)\}$. Hence $h^1(\mathbb{P}^r, \mathcal{I}_A(x)) = (\sharp(A \cap L) - x - 1) + \max\{0, \sharp(A') - x\}$. Now assume $\sharp(A \cap L) \leq x$. Since $\sharp(S \cap R) \leq \sharp(S \cap L)$, from (3) we get $h^0(L \cup R, \mathcal{I}_{A, L \cup R}(x)) = (x+1) - \sharp(A \cap L) + x - \sharp(A') = 2x + 1 - \sharp(A)$ and hence $h^1(\mathbb{P}^r, \mathcal{I}_A(x)) = 0$. Applying these relations to S and its subsets we get part (b). Part (a) follows from part (b). $\square$

Lemma 4. *Fix an integer* $x > 0$ *and lines* $L, R \in \mathbb{P}^r$, $r \geq 3$, *such that* $L \cap R = \emptyset$. *Fix* $S \subset L \cup R$ *such that* $\sharp(S \cap L) \geq \sharp(S \cap R)$ *and* $1 \leq \sharp(S) \leq 3x - 1$.

(a) We have $h^1(\mathbb{P}^r, \mathcal{I}_S(x)) > 0$ *if and only if* $\sharp(S \cap L) \geq x+2$.

(b) We have $h^1(\mathbb{P}^r, \mathcal{I}_S(x)) > h^1(\mathbb{P}^r, \mathcal{I}_{S'}(x))$ *for all* $S' \subsetneq S$ *if and only if either* $S \subset L$ *and* $\sharp(S) \geq x+2$ *or* $\sharp(S \cap R) \geq x+2$.

Proof. Fix a finite set $A \subset L \cup R$. We have $\mathcal{O}_{L \cup R}(x) \cong \mathcal{O}_L(x) \oplus \mathcal{O}_R(x)$ and hence $h^i(L \cup R, \mathcal{I}_{A, L \cup R}(x)) = h^i(L, \mathcal{I}_{A \cap L}(x)) + h^i(L, \mathcal{I}_{A \cap R}(x))$, $i = 0, 1$. Hence to extend the proof of Lemma 3 it is sufficient to prove the surjectivity of the restriction map $\rho : H^0(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(x)) \to H^0(L \cup R, \mathcal{O}_{L \cup R}(x))$. Since $L \cap R = \emptyset$, there is a smooth quadric surface $Q \subset \mathbb{P}^r$ such that $Q \supset L \cup R$. Since the restriction map $H^0(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(x)) \to H^0(Q, \mathcal{O}_Q(x))$ is surjective, it is sufficient to prove the surjectivity of the restriction map $\rho' : H^0(Q, \mathcal{O}_Q(x)) \to H^0(L \cup$

$R, \mathcal{O}_{L\cup R}(x))$. We have $Q \cong \mathbb{P}^1 \times \mathbb{P}^1$, with, say, L and R divisors of type $(1,0)$ on Q. Hence $\mathcal{O}_Q(x) \cong \mathcal{O}_Q(x,x)$ and $\mathcal{I}_{L\cup R,Q}(x) \cong \mathcal{O}_Q(x-2,x)$. The map ρ' is surjective, because $h^1(Q, \mathcal{O}_Q(t-2,t)) = 0$ for all $t > 0$ (e.g. by Künneth formula). $\square$

Lemma 5. *Fix an integer $x > 0$ and a finite set $S \subset \mathbb{P}^2$ such that $1 \le \sharp(S) \le 3x-1$. We have $h^1(\mathbb{P}^2, \mathcal{I}_S(x)) > h^1(\mathbb{P}^2, \mathcal{I}_{S'}(x))$ for all $S' \subsetneq S$ if and only if one of the following cases occurs:*

(i) $\sharp(S) \ge x+2$ and there is a line $L \subset \mathbb{P}^2$ such that $S \subset L$;

(ii) there are lines $L, R \in \mathbb{P}^2$ such that $L \ne R$, $\sharp(S\cap L) \ge x+2$ and $\sharp(S \cap R) \ge x+1$ or $\sharp(S\cap L) = \sharp(S\cap R) = x+1$ and $O \notin S$, where $\{O\} := L \cap R$;

(iii) there is a smooth conic $T_2 \subset \mathbb{P}^2$

Proof. For any line L and any finite set $A \subset L$ we have $h^1(L, \mathcal{I}_{A,L}(x)) = \max\{0, \sharp(A) - x - 1\}$. For any smooth conic T we have $h^0(T, \mathcal{O}_T(x)) = 2x+1$. Hence Lemma 3 gives the “ if ” part. Now assume $h^1(\mathbb{P}^2, \mathcal{I}_S(x)) > h^1(\mathbb{P}^2, \mathcal{I}_{S'}(x))$ for all $S' \subsetneq S$. Let τ be the maximal integer $t > 0$ such that $h^1(\mathbb{P}^2, \mathcal{I}_S(t)) > 0$. Our assumption implies $\tau \ge x$. Since $\sharp(S) < 3\tau$, we may apply the case $s = 3$ of [8], Corollaire 2, and get that either there is a line L_1 such that $\sharp(L_1 \cap S) \ge x+2$ or there is a conic L_2 such that $\sharp(S \cap L_2) \ge 2x+2$. First assume the existence of a conic L_2 such that $\sharp(S\cap L_2) \ge 2x+2$. Since $\deg(L_2) = 2$, we have an exact sequence (just (1) for $k = 2$):

$$0 \to \mathcal{I}_{S\setminus S\cap L_2}(x-2) \to \mathcal{O}_S(x) \to \mathcal{I}_{S\cap L_2, L_2}(x) \to 0 \tag{4}$$

Since $\sharp(S \setminus S\cap L_2) \le 3x-1-2x-2 \le x-1$, we have $h^1(\mathbb{P}^2, \mathcal{I}_{S\setminus S\cap L_2}(x-2)) = 0$. From (4) we get $h^1(\mathbb{P}^2, \mathcal{I}_S(x)) \le h^1(\mathbb{P}^2, \mathcal{I}_{S\cap L_2}(x))$. Hence $S \subset L_2$. If L_2 is smooth, then we are in case (iii). If L_2 is a double line, then we are in case (i) with $L := (L_2)_{red}$. Now assume $L_2 = L \cup R$ with L, R lines and $L \ne R$. Set $\{O\} := L \cap R$. Without losing generality we may assume $\sharp(S \cap L) \ge \sharp(S\cap R)$. If $\sharp(S \cap (R \setminus \{O\}) \ge x+1$, then we are in case (ii). Hence we may assume $\sharp(S \setminus S \cap L) \le x$. Since $\deg(L) = 1$, we have an exact sequence

$$0 \to \mathcal{I}_{S\setminus L\cap S}(x-1) \to \mathcal{I}_S(x) \to \mathcal{I}_{S\cap L, L}(x) \to 0 \tag{5}$$

Since $\sharp(S \setminus S\cap L) \le x$, we have $h^1(\mathbb{P}^2, \mathcal{I}_{S\setminus S\cap L}(x-1)) = 0$. From (5) we get $h^1(\mathbb{P}^2, \mathcal{I}_S(x)) \le h^1(\mathbb{P}^2, \mathcal{I}_{S\cap L}(x))$. Hence $S \subset L$. Hence we are in case (i). Now assume that $\sharp(S \cap T) \le 2x+1$ for each conic T, but that there is a line L such that $\sharp(S\cap L) \ge x+2$. If we are not in case (i), then as above we get

$h^1(\mathbb{P}^2, \mathcal{I}_{S\setminus S\cap L}(x-1)) > 0$. Since $\sharp(S\setminus S\cap L) \le 3x-1-x-2 \le 2(x-1)+1$, [1], Lemma 34, gives the existence of a line D such that $\sharp(D\cap(S\setminus S\cap L)) \ge x+1$. Hence $\sharp(S\cap(L\cup D)) \ge 2x+3$, contradicting one of our assumptions. □

Lemma 6. *Let $Q \subset \mathbb{P}^3$ be a smooth quadric surface and $L, R \subset Q$ disjoint lines. Fix a finite set $S \subset Q$ such that $1 \le \sharp(S) \le 3x+1$, $\sharp(S\cap L) \ge x+1$ and $\sharp(S\cap R) \ge x+1$. We have $h^1(\mathbb{P}^3, \mathcal{I}_S(x)) > h^1(\mathbb{P}^3, \mathcal{I}_{S'}(x))$ for all $S' \subsetneq S$ if and only if $S \subset L\cup R$, $\sharp(S\cap L) \ge x+2$ and $\sharp(S\cap R) \ge x+2$.*

Proof. Without losing generality we may assume that L and R are of type $(1,0)$ on Q. Since $L\cup R \in |\mathcal{O}_Q(2,0)|$, there is an exact sequence on Q:

$$0 \to \mathcal{I}_{S\setminus(S\cap(L\cup R))}(x-2,x) \to \mathcal{I}_S(x,x) \to \mathcal{I}_{S\cap(L\cup R),L\cup R}(x) \to 0 \qquad (6)$$

Since $\sharp(S\setminus(S\cap(L\cup R)) \le 3x+1-2x-2 = x-1$, we have $h^1(Q, \mathcal{I}_{S\setminus(S\cap(L\cup R)}(x-2,x)) = 0$. Hence (6) gives $h^1(Q, \mathcal{I}_S(x)) \ge h^1(Q, \mathcal{I}_{S\cap(L\cup R)}(x))$. Hence $S \subset L\cup R$. Lemma 4 gives $\sharp(S\cap L) \ge x+2$ and $\sharp(S\cap R) \ge x+2$. □

Lemma 7. *Fix an integer $x > 0$ and a set $S \subset \mathbb{P}^r$, $r \ge 3$, such that $1 \le \sharp(S) \le 3x-1$. We have $h^1(\mathbb{P}^r, \mathcal{I}_S(x)) > h^1(\mathbb{P}^r, \mathcal{I}_{S'}(x))$ for all $S' \subsetneq S$ if and only if one of the following cases occurs:*

(a) $\sharp(S) \ge x+2$ and there is a line $L \subset \mathbb{P}^r$ such that $S \subset L$ and $\sharp(S) \ge x+2$;

(b) there are lines $L, R \subset \mathbb{P}^r$ such that $L\cap R = \emptyset$, $\sharp(S\cap L) \ge x+2$ and $\sharp(S\cap R) \ge x+2$;

(c) there are lines $L, R \in \mathbb{P}^r$ such that $L \ne R$, $L\cap R \ne \emptyset$ (say, $\{O\} := L\cap R$), and either $\sharp(S\cap L) \ge x+2$ and $\sharp(S\cap R) \ge x+1$ or $\sharp(S\cap L) = \sharp(S\cap R) = x+1$ and $O \notin S$;

(d) $\sharp(S) \ge 2x+2$ and there is a smooth conic T_2 such that $S \subset T_2$.

Proof. Obviously in case (b) we need $x \ge 5$. Since the cases $x = 1, 2$ are obvious, we assume $x \ge 3$. For any line L and any finite set $A \subset L$ we have $h^1(L, \mathcal{I}_{A,L}(x)) = \max\{0, \sharp(A)-x-1\}$. Hence Lemmas 3 and 4 give the " if " part. Now we prove the " only if " part. Fix a finite set $S \subset \mathbb{P}^r$ such that $1 \le \sharp(S) \le 3x-1$ and $h^1(\mathbb{P}^r, \mathcal{I}_S(x)) > h^1(\mathbb{P}^r, \mathcal{I}_{S'}(x))$ for all $S' \subsetneq S$. Set $s_0 := \sharp(S)$. Let $H_1 \subset \mathbb{P}^3$ be a hyperplane such that $a_1 := \sharp(S\cap H_1)$ is maximal. Set $S_1 := S_0 \setminus S_0\cap H_1$ and $s_1 := \sharp(S_1)$. The sequence $\{a_i\}$ is non-decreasing and $S_{i+1} \subseteq S_i$ for all i. Since any r points of $\mathbb{P}^r$ are coplanar, the maximality of the integer s_i gives that if $a_i \le r-1$, then $a_{i+1} = 0$. Hence $S_i = \emptyset$ for all $i \ge x+1$. For any integer $i \in \{1, \dots, x+1\}$ we have an exact sequence

$$0 \to \mathcal{I}_{S_i}(x-i) \to \mathcal{I}_{S_{i-1}}(x-i+1) \to \mathcal{I}_{S_{i-1}\cap H_i, H_i}(x-i+1) \to 0 \qquad (7)$$

Since $h^1(\mathbb{P}^r, \mathcal{I}_{S_0}(x)) = 0$, (7) implies the existence of an integer $i \in \{1, \dots, x\}$ such that $h^1(H_i, \mathcal{I}_{S_{i-1}\cap H_i, H_i}(x-i+1)) > 0$. Call c the minimal such an integer. Since $h^1(H_c, \mathcal{I}_{S_{c-1}\cap H_c, H_c}(x-c+1)) > 0$, we have $a_c \ge x-c+3$ and equality holds only if $S_{c-1}\cap H_c$ is contained in a line ([1], Lemma 34). Since the sequence $\{a_i\}$ is non-decreasing, we get $\sharp(S) \ge c(x-c+3)$. The function $t \mapsto t(x+3-t)$ is non-decreasing if $t \le (x+3)/2$ and non-increasing if $t \ge (x+3)/2$. Since $\sharp(S) < 3x$ and $x(x+3-x) = 3x$, we get $c \in \{1, 2\}$.

(a) First assume $r = 3$.

(a1) Here we assume $c = 1$. First assume $a_1 \ge 2x+2$. Since $\sharp(S_1) = s_0 - a_1 \le x$, we have $h^1(\mathbb{P}^r, \mathcal{I}_{S_1}(x-1)) = 0$. Hence from (7) we get $h^1(\mathbb{P}^r, \mathcal{I}_{S_1}(x)) \le h^1(\mathbb{P}^r, \mathcal{I}_{S_1}(x))$. Since $h^1(\mathbb{P}^r, \mathcal{I}_S(x)) > h^1(\mathbb{P}^r, \mathcal{I}_{S'}(x))$ for all $S' \subsetneq S$, we get $S_1 = S$. Lemma 5 gives that we are either in case (a) or in case (c). Similarly, we conclude if $S_1 = \emptyset$. Hence we may assume $S_1 \ne \emptyset$ and $a_1 \le 2x+1$. There is a line $L \subset \mathbb{P}^r$ such that $\sharp(S\cap L) \ge x+2$. Since $S_1 \ne \emptyset$, we have $h^1(\mathbb{P}^r, \mathcal{I}_S(x)) > h^1(\mathbb{P}^r, \mathcal{I}_{S\cap H_1}(x))$. Hence the case $i = 1$ of (7) gives $h^1(\mathbb{P}^r, \mathcal{I}_{S_1}(x-1)) > 0$. Since $\sharp(S_1) \le 2(x-1)+1$, there is a line $R \subset H_1$ such that $\sharp(S_1 \cap R) \ge x+1$ ([1], Lemma 34). First assume $L \cap R \ne \emptyset$. Let N be the plane spanned by $L \cup R$. Since $\sharp(S \cap (L \cup R)) \ge 2x+3$, we have $a_1 \ge 2x+3$. Hence $a_2 \le x-4$, absurd. Now assume $L \cap R = \emptyset$. There is a smooth quadric surface $Q \supset L \cup R$. Since $\deg(Q) = 2$, we have an exact sequence on $\mathbb{P}^3$:

$$0 \to \mathcal{I}_{S\setminus S\cap Q}(x-2) \to \mathcal{O}_S(x) \to \mathcal{I}_{S\cap Q, Q}(x) \to 0 \qquad (8)$$

Since $\sharp(S\setminus S\cap Q) \le 3x-1-\sharp(S\cap L\cup R)) \le x-1$, we have $h^1(\mathbb{P}^3, \mathcal{I}_{S\setminus S\cap Q}(x-2)) = 0$. Hence (8) gives $h^1(\mathbb{P}^3, \mathcal{I}_S(x)) \le h^1(Q, \mathcal{I}_{S\cap Q, Q}(x)) \le h^1(\mathbb{P}^3, \mathcal{I}_{S\cap Q}(x))$. Since $h^1(\mathbb{P}^r, \mathcal{I}_S(x)) > h^1(\mathbb{P}^r, \mathcal{I}_{S'}(x))$ for all $S' \subsetneq S$, we get $S = S\cap Q$. Apply Lemma 6.

(a2) Here we assume $c = 2$. Since $a_1 \ge a_2$ and $a_1 + a_2 \le \sharp(S) < 3x$, we have $a_2 \le 2(x-1)+1$. Hence there is a line $D \subset H_1$ such that $\sharp(D\cap S) \ge x+1$. Let M be a hyperplane containing D and with maximal $b_1 := \sharp(M \cap S)$. Set $W := S \setminus S \cap M$. Since $\deg(M) = 1$ we have an exact sequence

$$0 \to \mathcal{I}_{S\setminus S\cap M}(x-1) \to \mathcal{I}_S(x) \to \mathcal{I}_{S\cap M, M}(x) \to 0 \qquad (9)$$

First assume $h^1(\mathbb{P}^3, \mathcal{I}_{S\setminus S\cap M}(x-1)) = 0$. From (9) we get $h^1(\mathbb{P}^3, \mathcal{I}_S(x)) \le h^1(\mathbb{P}^3, \mathcal{I}_{S\cap M}(x))$. Hence $S = S \cap M$. Apply Lemma 5. Now assume

$$h^1(\mathbb{P}^3, \mathcal{I}_{S\setminus S\cap M}(x-1)) > 0.$$

There is a line $T \subset \mathbb{P}^3$ such that $\sharp(T \cap (S \setminus S \cap M)) \ge x+1$. If $T \cap D \ne \emptyset$, then we are done, because $M \supset D$. Now assume $T \cap D = \emptyset$. Take a smooth quadric surface $Q' \supset D \cup T$. Since $\sharp(S \setminus S \cap Q') \le 3x - 1 - 2x - 2 \le x - 1$, as in step (a1) we get $S = S \cap Q'$. Apply Lemma 6.

(b) Now we assume $r > 3$ and that the lemma is true in $\mathbb{P}^{r-1}$. We conclude as above using the inductive assumption instead of Lemma 5 (in part (a1) we may take a hyperplane containing $L \cup R$ even if $L \cap R = \emptyset$). □

Lemma 8. *Fix an integer $x > 0$, a zero-dimensional scheme $E \subset \mathbb{P}^r$, $r \ge 2$, such that $\deg(E) \le x$ and a finite set $S \subset \mathbb{P}^r$ such that $1 \le \sharp(S) \le 2x + 1 - \deg(E)$ and $S \subset E = \emptyset$. We have $h^1(\mathbb{P}^r, \mathcal{I}_{E\cup S}(x)) > h^1(\mathbb{P}^r, \mathcal{I}_{E\cup S'}(x))$ for all $S' \subsetneq S$ if and only if there is a line $L \subset \mathbb{P}^r$ such that $S \subset L$ and $\sharp(S) + \deg(E \cap L) \ge x + 2$.*

Proof. Since $\deg(E) + \sharp(S) \le 2x + 1$, we have $h^1(\mathbb{P}^r, \mathcal{I}_{E\cup S}(x)) > 0$ if and only if there is a line $L \subset \mathbb{P}^r$ such that $\deg(L \cap (E \cup S)) \ge x + 2$ ([1], Lemma 34, and Remark 2). Since the scheme-theoretic intersection of two different lines has degree ≤ 1, this line L is unique. We need to prove that $h^1(\mathbb{P}^r, \mathcal{I}_{E\cup S}(x)) > h^1(\mathbb{P}^r, \mathcal{I}_{E\cup S'}(x))$ for all $S' \subsetneq S$ if and only if $S \subset L$. Assume $h^1(\mathbb{P}^r, \mathcal{I}_{E\cup S}(x)) > h^1(\mathbb{P}^r, \mathcal{I}_{E\cup S'}(x))$ for all $S' \subsetneq S$ if and only if $S \subset L$. Let H be any hyperplane containing L (hence $H = L$ if $r = 2$). We have $\deg(\mathrm{Res}_H(E \cup S)) \le 2x + 1 - x - 2 \le x$. Hence [1], Lemma 34, gives $h^1(\mathbb{P}^r, \mathcal{I}_{\mathrm{Res}_H(E\cup S)}(x-1)) = 0$. The case $k = 1$ of (1) gives $h^1(\mathbb{P}^r, \mathcal{I}_{E\cup S}(x)) \le h^1(H, \mathcal{I}_{(E\cup S)\cap H}(x))$. Since $h^1(H, \mathcal{I}_{(E\cup S)\cap H}(x)) = h^1(\mathbb{P}^r, \mathcal{I}_{(E\cup S)\cap H}(x)) \le h^1(\mathbb{P}^r, \mathcal{I}_{E\cup(S\cap H)}(x))$ (Remark 2), we get $S = S \cap H$. Since this is true for all hyperplanes containing L, we get $S \subset L$.

Now we prove the converse. Take any finite set $A \subset L \setminus (E \cap L)_{red}$ such that $\sharp(A) + \deg(E) \le 2x + 1$. First assume that either $\deg(E) \le x + 1$ or $E \cap L \ne \emptyset$. In this case we have $\deg(\mathrm{Res}_H(E \cup A)) = \deg(\mathrm{Res}_H(E)) \le x$. Hence the proof just given gives $h^1(\mathbb{P}^r, \mathcal{I}_{A\cup E}(x)) = \max\{0, \deg(E \cap L) + \sharp(A) - x - 1\}$. Now assume $\deg(E) = x + 1$ and $E \cap L = \emptyset$. Either $h^1(\mathbb{P}^r, \mathcal{I}_{A\cup E}(x)) = 0$ or there is a line $R \subset \mathbb{P}^r$ such that $\deg(R \cap (E \cup A)) \ge x + 2$. Since $A \subset L$, $E \cap L = \emptyset$ and $\sharp(A) \le x + 1$, we have $R \ne L$. Since $A \subset L$, we get $L \cap R \ne \emptyset$ and that the point $R \cap L$ is one of the point of A. Taking a hyperplane M containing R we get as above $h^1(\mathbb{P}^r, \mathcal{I}_{E\cup A}(x)) = h^1(\mathbb{P}^r, \mathcal{I}_{E\cup L\cap R}(x))$. We are in the set-up of the lemma with $S = R \cap L$ and $\sharp(S) = 1$. $\square$

3. Proofs of Theorems 1 and 2

Proofs of Theorem 1 and 2. Let $S \subset B$ be the support of a codeword of $\mathcal{C}(B, \mathcal{O}_C(x)(-E))^\perp$ (with $E = \emptyset$ for Theorem 1) and either $\sharp(S) \leq 2x + 1 - \deg(E)$ (case $E \neq \emptyset$) or $\sharp(S) < 3x$ (case $E = \emptyset$). If $E \neq \emptyset$, Lemma 8 gives the existence of a line L such that $S \subset L$ and $\deg(L \cap (E \cup S)) \geq x + 2$. Since $E \cup S \subset C \subset \mathcal{H}$ and $x + 2 > q + 1 \deg(\mathcal{H})$, Bezout theorem gives $L \subset \mathcal{H}$. If $\sharp(S) \geq 2$, then L is defined over $\mathbb{F}_{q^2}$, i.e. $L \in \Phi$. Hence $L \in \Phi_0$. Now assume $\sharp(S) \leq 1$. Since $\deg(E) \leq x + 1$ and $\deg(L \cap (E \cup S)) \geq x + 2$, we get $\deg(E) = x+1$ and $E \subset L$. Since $\deg(E) \geq 2$, the line L is uniquely determined by E. Since E is defined over $\mathbb{F}_{q^2}$, then L is defined over $\mathbb{F}_{q^2}$. Hence $L \in \Phi_0$ even in this case. From now on we assume $E = \emptyset$. By Lemma 7 we are in one of the cases (a), (b), (c) of Lemma 7. In all cases we have a reduced curve T'' such that $S \subset T''$ and for each irreducible component T' of T'' we have $\sharp(S \cap T') \geq (x + 1)\deg(T') > \deg(\mathcal{H}) \cdot \deg(T')$. Hence $T'' \subset \mathcal{H}$. We also see that each irreducible component of T'' is defined over $\mathbb{F}_{q^2}$. Hence case (a) (resp. (b), resp. (c)) of Lemma 7 corresponds to case (i) (resp. (ii), resp. (iii)) of the statement of Theorem 2.

Now we exclude cas (d) of Lemma 7, i.e. we exclude that T'' is a smooth conic. Let $D \subset \mathbb{P}^3$ be smooth conic such that $\sharp(D \cap B) \geq 5$. Any smooth conic is uniquely determined by 5 of its points. Since each point of B is defined over $\mathbb{F}_{q^2}$, D is defined over $\mathbb{F}_{q^2}$. In order to obtain a contradiction we assume $\sharp(D \cap B) \geq 2q + 3$. Bezout theorem gives $D \subset \mathcal{H}$ (not only $D(\mathbb{F}_{q^2}) \subset \mathcal{H}(\mathbb{F}_{q^2})$). Since D is defined over $\mathbb{F}_{q^2}$, the plane H spanned by D is defined over $\mathbb{F}_{q^2}$. Hence $H \cap \mathcal{H}$ is either a smooth degree $q + 1$ curve (a Hermitian curve) or a union of $q+1$ lines. Since $D \subseteq \mathcal{H} \cap H$, in both cases we get a contradiction. $\square$

4. Geometry of $\mathcal{H}$ and Arithmetically Cohen-Macaulay Curves

For each $P \in \mathcal{H}$, let $T_P\mathcal{H}$ denote the tangent plane to $\mathcal{H}$. We have $\sharp(\mathcal{H}(\mathbb{F}_{q^2})) = (q^2 + 1)q^2(q^3 + 1)$ and for each $P \in \mathcal{H}(\mathbb{F}_{q^2})$ the scheme $T_P\mathcal{H}$ is a cone formed by $q + 1$ distinct lines through P, each of them defined over $\mathbb{F}_{q^2}$ ([12], Ch. 19). Hence $\sharp(T_P\mathcal{H} \cap \mathcal{H}(\mathbb{F}_{q^2})) = 1 + (q + 1)q^2$. Varying $P \in \mathcal{H}(\mathbb{F}_{q^2})$ we get that $\mathcal{H}(\mathbb{F}_{q^2})$ is covered by $(q+1)(q^3+1)$ lines of $PG(3, q^2)$. Each plane of $PG(3, q^2)$

not tangent to $\mathcal{H}$ at a point of $PG(3,q^2)$ intersects $\mathcal{H}$ in a smooth Hermitian curve, because the intersection is a Hermitian curve with full rank ([12], Lemma 19.1.2).

Take a geometrically connected curve $C \subset \mathcal{H}$ defined over a finite extension, K, of $\mathbb{F}_{q^2}$. Here we take as $\mathcal{L}$ a hyperplane line bundle, say $\mathcal{O}_C(t)$, and fix $B \subseteq C(K)$. Look at the restriction maps $\rho_{C,t} : H^0(\mathbb{P}^3, \mathcal{O}_{\mathbb{P}^3}(t)) \to H^0(C, \mathcal{O}_C(t))$ and $\rho'_{C,t} : H^0(\mathcal{H}, \mathcal{O}_{\mathcal{H}}(t)) \to H^0(C, \mathcal{O}_C(t))$. Since the restriction map $H^0(\mathbb{P}^3, \mathcal{O}_{\mathbb{P}^3}(t)) \to H^0(\mathcal{H}, \mathcal{O}_{\mathcal{H}}(t))$ is surjective, we have $\mathrm{Im}(\rho'_{C,t}) = \mathrm{Im}(\rho_{C,t})$. Over C we have the Goppa code obtained evaluating $H^0(C, \mathcal{O}_C(t))$ ([20], II.2.1, [21]) and the " field code " obtained from $\mathrm{Im}(\rho_{C,t})$ ([19], [18], Lemma 6.5.1). The latter is easier from a computation point of view, because only involves homogeneous degree t polynomials. The former is conceptually easier and its dual code is again a Goppa code on C ([20], Theorem II.2.8). As shown in [2] the low weight codewords associated to the dual of $\mathrm{Im}(\rho)$ may be found only using elementary geometric properties of B (e.g. the maximal number of collinear points of B). A curve $C \subset \mathbb{P}^3$ is said to be arithmetically Cohen-Macaulay if $\rho_{C,t}$ is surjective for all t. Any complete intersection curve is arithmetically Cohen-Macaulay (see. e.g. [2] or [7]). In this section we construct several arithmetically Cohen-Macaulay curves $C \subset \mathcal{H}$ which are not complete intersection (see Corollary 1 and Remark 4).

Lemma 9. *Let $W \subset \mathbb{P}^3$ be any effective divisor and $T \subset \mathbb{P}^3$ any projective curve contained in W. Set $c := \deg(C)$.*

(a) For each integer t the restriction mapp

$$\rho_{W,t} : H^0(\mathbb{P}^3, \mathcal{O}_{\mathbb{P}^3}(t)) \to H^0(W, \mathcal{O}_W(t))$$

is surjective.

(c) C is arithmetically Cohen-Macaulay if and only if for every $t \in \mathbb{N}$ the restriction map $\rho_{W,C,t} : H^0(W, \mathcal{O}_W(t)) \to H^0(C, \mathcal{O}_C(t))$ is surjective.

(d) Fix $t \in \mathbb{N}$. the map $\rho_{W,C,t}$ is surjective if and only if $H^1(W, \mathcal{I}_{T,W}(t)) = 0$.

(e) If $T \in |\mathcal{O}_W(z)|$ for some $z > 0$, then T is arithmetically Cohen-Macaulay.

(f) Assume that T is a complete intersection of two surfaces, say of degree d_1, d_2 with $d_1 \leq d_2$. Then $d_1 \leq \deg(W)$. If W is geometrically integral, then either $d_1 = \deg(W)$ or $\deg(W) \geq d_2$. If $d_1 \leq \deg(W) \leq d_2$, then $\deg(W) \in \{d_1, d_2\}$ and T is the complete intersection of W and a surface of degree $\deg(T)/\deg(W)$.

Proof. For each integer t we have an exact sequence

$$0 \to \mathcal{O}_{\mathbb{P}^3}(t-c) \to \mathcal{O}_{\mathbb{P}^3}(t) \to \mathcal{O}_W(t) \to 0 \tag{10}$$

Since $H^1(\mathbb{P}^3, \mathcal{O}_{\mathbb{P}^3}(t-c)) = 0$ ([11], part (b) of Theorem III.5.1) we get (a). Part (a) implies the " if " part (b). The " only if " part of (b) is trivial, because the restriction map ${}^0(\mathbb{P}^3, \mathcal{O}_{\mathbb{P}^3}(t)) \to H^0(C, \mathcal{O}_C(t))$. Consider the exact sequence

$$0 \to \mathcal{I}_{T,W}(t) \otimes \mathcal{O}_W(t) \to \mathcal{O}_T(t) \to 0 \tag{11}$$

Since $h^i(\mathbb{P}^3, \mathcal{O}_{\mathbb{P}^3}(x)) = 0$, $i = 1, 2$ for all $x \in \mathbb{Z}$, we have $h^1(S, \mathcal{O}_W(t)) = 0$. Hence (11) shows that $H^1(S, \mathcal{O}_W(t)(-T))$ is the cokernel of $\rho_{W,C,t}$, proving part (d). Part (e) follows from part (d), because we proved that $H^1(W, \mathcal{O}_W(t-z)) = 0$ for all t. Now assume that T is the complete intersection of a surface W_1 of degree d_1 and a surface of degree $d_2 \geq d_1$. Using (12) with W_1 instead of W and d_1 instead of c we get that T is contained in no surface of degree $< d_1$. Using also (11) for (W_1, d_1) instead of (W, c) we get that every surface of degree x with $d_1 \leq x < d_2$ contains W_1 as a component. Hence we get (f). $\square$

Part (e) is useful to check that most of the arithmetically Cohen-Macaulay curves obtained in this paper are not complete intersections.

For any $P \in \mathcal{H}(\mathbb{F}_{q^2})$ let $A(P)$ denote the set of $q+1$ lines of $\mathcal{H} \cap T_P\mathcal{H}$. For any non-empty subset S of of the lines of $T_P\mathcal{H} \cap \mathcal{H}$ we call $L(P, S)$ the scheme $\cup_{L \in S} L$. Each scheme $L(P, S)$ is defined over $\mathbb{F}_{q^2}$ and it is isomorphic to over $\mathbb{F}_{q^2}$ to a degree t plane curve (where $t := \sharp(S)$), union of t distinct lines through P, each of them defined over $\mathbb{F}_{q^2}$. Since $L(P, S)$ is a plane curve, it is arithmetically Cohen-Macaulay. Hence for each integer $z > 0$ each divisor $A \in |\mathcal{O}_{\mathcal{H}}(z)(-L(P, S))|$ is arithmetically Cohen-Macaulay ([7], part (b) of Theorem 21.23).

Fix a plane $H \subset \mathbb{P}^3$ defined over $\mathbb{F}_{q^2}$ and transversal to $\mathcal{H}$. The smooth curve $D := H \cap \mathcal{H}$ is a smooth Hermitian curve ([12], Table 1) and hence $\sharp(D(\mathbb{F}_{q^2})) = q^3 + 1$. For all $P, Q \in D(\mathbb{F}_{q^2})$, with $P \neq Q$ the tangent planes $T_P\mathcal{H}$ and $T_Q\mathcal{H}$ are distinct ([12], Lemma 19.1.4 (i)). The line $\langle \{P, Q\} \rangle$ is contained in H (because $\{P, Q\} \subset H$), but not in $\mathcal{H}$, because $H \cap \mathcal{H}$ is the smooth curve D. Hence the line $T_P\mathcal{H} \cap T_Q\mathcal{H}$ is not contained in $\mathcal{H}$. Hence $T_P\mathcal{H} \cap \mathcal{H}$ and $T_Q\mathcal{H} \cap \mathcal{H}$ have no common line. Conversely, if $P, Q \in \mathcal{H}(\mathbb{F}_{q^2})$, $P \neq Q$ and the line $\langle \{P, Q\} \rangle$ is contained in $\mathcal{H}$, then $\langle \{P, Q\} \rangle = (T_P\mathcal{H} \cap \mathcal{H}) \cap (T_P\mathcal{H} \cap \mathcal{H})$.

Lemma 10. *Set $\Psi := \cup_{L \in \Phi} L$. Then $\Psi = \cup_{P \in D(\mathbb{F}_{q^2})}(T_P\mathcal{H} \cap \mathcal{H})$ and Ψ is the complete intersection of $\mathcal{H}$ with a degree (q^3+1) surface, union of q^3+1 planes, each of them defined over $\mathbb{F}_{q^2}$.*

Proof. Set $\Sigma := \cup_{P\in D(\mathbb{F}_{q^2})}(T_P\mathcal{H}\cap\mathcal{H})$. We claim that $\Psi = \Sigma$. Indeed, obviously $\Sigma \subseteq \Psi$. Fix any $L \in \Phi$. Since H meets any line of $\mathbb{P}^3$, $H\cap L \neq \emptyset$. Since $L \subset \mathcal{H}$, we have $L \nsubseteq H$ and hence $H\cap L$ is a point (call it P). Since $L \subset \mathcal{H}$, we have $P \in D$. Since L and D are defined over $\mathbb{F}_{q^2}$, we have $P \in D(\mathbb{F}_{q^2})$. Hence $L \in T_P\mathcal{H}$. Hence $L \in \Phi$. Hence $L \subset \Sigma$. Thus Ψ is the complete intersection of $\mathcal{H}$ with a degree (q^3+1) surface, union of q^3+1 planes, each of them defined over $\mathbb{F}_{q^2}$. □

Lemma 11. *Fix integer $t, a \in \{1,\dots,q+1\}$, a line $L \subset \mathbb{P}^3$ defined over $\mathbb{F}_{q^2}$ and transversal to $\mathcal{H}$ (and hence with $\sharp(\mathcal{H}(\mathbb{F}_{q^2})\cap D) = q+1$) and a set $S \subseteq \mathcal{H}(\mathbb{F}_{q^2})\cap D$ such that $\sharp(S) = t$. Fix a ponts $P_1,\dots,P_a \in \mathcal{H}(\mathbb{F}_{q^2})\setminus D$ such that $T_{P_i}\mathcal{H} \supset D$ for all i (there are $q+1$ such points). Then $W := \cup_{i=1}^a L(P_i,S)$ is the complete intersection of the degree a surface $\cup_{i=1}^a T_{P_i}\mathcal{H}$ and a surface union of t distinct planes defined over $\mathbb{F}_{q^2}$.*

Proof. Fix $A \in \mathcal{H}(\mathbb{F}_{q^2})$, We have $P \in T_A\mathcal{H}$ if and only if $\langle\{P,A\}\langle \subset \mathcal{H}$, i.e. if and only if $A \in T_P\mathcal{H}$. Since $T_P\mathcal{H}\cap T_Q\mathcal{H}\cap\mathbb{H}$ is formed by $q+1$ collinear points, we may take as a any integer $\leq q+1$.

If $a = 1$, then W is a plane curve union of t lines and hence the lemma is obvious. Now assume $a \geq 2$. For each $Q \in S$ set $H_Q := \langle\{Q,P_1,P_2\}\rangle$. H_Q is a plane, because the line $T_{P_1}\mathcal{H}\cap T_{P_2}\mathcal{H} = L$ implies $P_2 \notin T_{P_1}\mathcal{H}$, while the line $\langle\{Q,P_1\}\rangle$ is contained in $T_{P_1}\mathcal{H}$. Since $H_Q\cap\mathcal{H}$ contains two lines through Q, it is the union of $q+1$ lines defined over $\mathbb{F}_{q^2}$ and forming a singular Hermitian curve of H_Q. Among these lines there are the lines $L(P_i,Q)$, $1 \leq i \leq a$. Hence $W = \cup_{i=1}^a T_{P_i}\mathcal{H}\cap(\cup_{Q\in S}H_Q$. □

Lemma 12. *Let $W \subset \mathbb{P}^3$ be any smooth surface and $\mathcal{L}$ any line bundle on W. Fix an integer z and curves $D \in |\mathcal{L}|$ and $T \in |\mathcal{L}(z)|$. If D is arithmetically Cohen-Macaulay, then T is arithmetically Cohen-Macaulay.*

Proof. Fix $t \in \mathbb{Z}$. We need to prove the surjectivity of the restriction map $H^0(\mathbb{P}^3,\mathcal{O}_{\mathbb{P}^3}(t)) \to H^0(T,\mathcal{O}_T(t))$. Since the restriction map $H^0(\mathbb{P}^3,\mathcal{O}_{\mathbb{P}^3}(t)) \to H^0(\mathcal{H},\mathcal{O}_{\mathcal{H}}(t))$ is surjective, it is sufficient to prove the surjectivity of the restriction map $\rho_{T,t} : H^0(\mathcal{H},\mathcal{O}_{\mathcal{H}}(t)) \to H^0(T,\mathcal{O}_T(t))$. Since $\mathcal{H}$ is a surface of $\mathbb{P}^3$, we have $h^1(\mathcal{H},\mathcal{O}_{\mathcal{H}}(t)) = 0$. Hence the exact sequence

$$0 \to \mathcal{O}_{\mathcal{H}}(t)(-T) \to \mathcal{O}_{\mathcal{H}}(t) \to \mathcal{O}_T(t) \to 0 \tag{12}$$

shows that $\rho_{T,t}$ is surjective if and only if $h^1(\mathcal{H},\mathcal{O}_{\mathcal{H}}(t))(-T)) = 0$. Using D instead of T and $t-z$ instead of t in (12) and that D is arithmetically Cohen-Macaulay we get $h^1(\mathcal{H},\mathcal{O}_{\mathcal{H}}(t-z))(-D)) = 0$. Since $\mathcal{O}_{\mathcal{H}}(t-z))(-D) \cong \mathcal{L} \cong \mathcal{O}_{\mathcal{H}}(t))(-T)$, T is arithmetically Cohen-Macaulay. □

Corollary 1. *Fix sets $F \subsetneq A \subseteq \Phi$ such that $\cup_{L\in A}L$ is a complete intersection and $\cup_{L\in F}L$ is arithmetically Cohen-Macaulay. Fix any $t \in \mathbb{Z}$ and any $Y \in |\mathcal{O}_{\mathcal{H}}(\cup_{L\in A\setminus F}L)(t)|$. Then Y is arithmetically Cohen-Macaulay.*

Proof. Apply Lemma 12 and [7], part (b) of Theorem 21.23. □

Remark 4. See Lemmas 10 and 11 for the constructions of sets $G \subseteq \Phi$ such that $\cup_{L\in G}L$ is a complete intersection. Since a complete intersection is arithmetically Cohen-Macaulay, we may apply these constructions also to the set F appearing in Corollary 1. Notice that in general $\cup_{L\in A\setminus F}L$ is not a complete intersection, even if both $\cup_{L\in A}L$ and $\cup_{L\in F}L$ are complete intersections.

Acknowledgements

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

References

[1] A. Bernardi, A. Gimigliano, M. Idà, Computing symmetric rank for symmetric tensors, *J. Symbolic. Comput.*, **46**, No. 1 (2011), 34-53.

[2] A. Couvreur, The dual minimum distance of arbitrary dimensional algebraic-geometric codes, *J. of Algebra*, **350**, No. 1 (2012), 84-107.

[3] L. Gruson, R. Lazarfeld, C. Peskine, On a theorem of Castelnuovo, and the equations defining space curves, *Invent. Math.*, **72**, No. 3 (1983), 491-506.

[4] F.A.B. Edoukou, Codes defined by forms of degree 2 on Hermitian surfaces and Sørensen's conjecture, *Finite Fields Appl.*, **13**, No. 3 (2007), 616-627.

[5] F.A.B. Edoukou, The weight distribution of the functional codes defined by forms of degree 2 on Hermitian surfaces, *J. Théor. Nombres Bordeaux*, **21**, No. 1 (2009), 131-143.

[6] F.A.B. Edoukou, A. Hallez, F. Rodier, L. Storme, The small weight codewords of the functional codes associated to non-singular Hermitian varieties, *Des. Codes Cryptogr.*, **56**, No-s: 2-3 (2010), 219-233.

[7] D. Eisenbud, *Commutative Algebra*, Springer, Berlin (1995).

[8] 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).

[9] S. Fanali, M. Giulietti, On maximal curves with Frobenius dimension 3, *Des. Codes Cryptogr.*, **53** (2009), 165-174.

[10] R. Fuhrmann, F. Torres, On Weierstrass points and optimal curves, *Rend. Circ. Mat. Palermo Suppl.*, **51** (1998), 25-46.

[11] R. Hartshorne, *Algebraic Geometry*, Springer, Berlin (1977).

[12] J.W.P. Hirschfeld, *Finite Projective Spaces of Three Dimensions*, Clarendon Press, Oxford (1985).

[13] J.W.P. Hirschfeld, J.A. Thas, *General Galois Geometries*, Clarendon Press, Oxford (1991).

[14] J.W.P. Hirschfeld, G. Korchmáros, F. Torres, *Algebraic Curves over a Finite Field*, Princeton Series in Applied Mathematics, Princeton University Press, Princeton, NJ (2008).

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

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

[17] G. Lachaud, Number of points of plane sections and linear codes defined on algebraic varieties, In: *Arithmetic, Geometry, and Coding Theory*, Luminy, France, De Gruyter, Berlin (1996), 77-104.

[18] H. Niederreiter, C. Xing, *Rational Points on Curves over Finite Fields*, Cambridge University Press, Cambridge (2001).

[19] R. Pellikaan, B.-Z. Shen, G.J.M. Van Wee, Which linear codes are algebraic-geometric?, *IEEE Trans. Inform. Theory*, **37** (1991), 583-602.

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

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