Available online at http://scik.org
J. Math. Comput. Sci. 2 (2012), No. 1, 37-53
ISSN: 1927-5307

DUAL GOPPA CODES OF CURVES CONTAINED IN A QUADRIC SURFACE

E. BALLICO*

[1]Department of Mathematics, University of Trento, 38123 Trento (TN), Italy

Abstract. Here we study the minimum distance of (duals of) Goppa codes on smooth curves $C \subset T$, where $T \subset \mathbb{P}^3$ is a geometrically irreducible quadric surface defined over a finite field.

Keywords: Goppa code; quadric surface; quadric cone; elliptic quadric surface.

2010 AMS Subject Classification: 94B27; 14G15; 14H99.

1. Introduction

We work over a finite field K. 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 $(f) + D \geq 0$, ([8], Ch. 2, [10]) (it is the geometric Goppa code $C_{\mathcal{L}}(B, D)$ defined in [8], II.2.1). The dual code $\mathcal{C}(B, \mathcal{O}_C(D))^{\perp}$ may be described in the same way ([8], Theorem II.2.8).

*Corresponding author

E-mail address: ballico@science.unitn.it

Received December 6, 2011

We first prove the following results concerning Goppa codes constructed using curves contained in a hyperbolic quadric surface Q.

Theorem 1.1. *Fix positive integers a, b, x, y such that $x \ge y$, $x \le a-2$ and $y \le b-2$. Let $Q \subset \mathbb{P}^3$ be a hyperbolic quadric surface defined over a finite field K and $Y \in |\mathcal{O}_Q(a,b)|$ a geometrically integral curve defined over K with only ordinary nodes or ordinary cusps as singularities. Let $u : C \to Y$ be the normalization. Fix a a zero-dimensional scheme $E \subset C \setminus u^{-1}(Sing(Y))$ and a set $B \subset C(K) \setminus (u^{-1}(Sing(Y)) \cup E_{red})$. Set $n := \sharp(B)$ and $k := (x+1)(y+1) - \deg(E)$. Assume $\sharp(Sing(Y)) + \deg(E) \le y-1$ and $n + \deg(E) > ay + bx$. Set $\mathcal{C} := \mathcal{C}(B, \mathcal{O}_C(x,y)(-E))$. Then $\mathcal{C}$ is an $[n,k]$-code and its dual $\mathcal{C}^\perp$ has minimum distance $\ge y + 2 - \deg(E)$.*

Theorem 1.2. *Fix positive integers a, b, x, y such that $x \ge y$, $x \le a-2$ and $y \le b-2$. Let Q be a hyperbolic quadric surface defined over a finite field K and $C \in |\mathcal{O}_Q(a,b)|$ a smooth curve defined over K. Fix a a zero-dimensional scheme $E \subset C$ defined over K and a set $B \subset C(K) \setminus E_{red}$. Set $n := \sharp(B)$ and $k := (x+1)(y+1) - \deg(E)$. Assume $\deg(E) \le y-1$ and $n + \deg(E) > ay + bx$. Set $\mathcal{C} := \mathcal{C}(B, \mathcal{O}_C(x,y)(-E))$. Then $\mathcal{C}$ is an $[n,k]$-code and its dual $\mathcal{C}^\perp$ has minimum distance $\ge y + 2 - \deg(E)$.*

(a) There is a codeword of $\mathcal{C}^\perp$ with weight $y + 2 - \deg(E)$ if and only if either there is $D \in |\mathcal{O}_Q(1,0)|$ with $E \subset D$ and $\sharp(B \cap D) \ge y + 2 - \deg(E)$ or $x = y$ and there is $D' \in |\mathcal{O}_Q(0,1)|$ with $E \subset D'$ and $\sharp(B \cap D') \ge y + 2 - \deg(E)$.

(b) Take D (resp. D' if $x = y$) and any $S \subseteq D \cap B$ (resp. $S \subseteq D' \cap B$) such that $\sharp(S) = y + 2 - \deg(E)$. There is a unique (up to a scalar) codeword of $\mathcal{C}^\perp$ with S as its support.

(c) Each codeword with weight $\le 3y - 2 - \deg(E)$ (if any) has as support a set S such that either there is $D \in |\mathcal{O}_Q(1,0)|$ with $\deg((S \cup E) \cap D) \ge y + 2$ or there is $D' \in |\mathcal{O}_Q(0,1)|$ such that $\deg((E \cup S) \cap D') \ge x + 2$ or there is $A \in |\mathcal{O}_Q(1,1)|$ such that $\deg((E \cup S) \cap A) \ge x + y + 2$.

See Propositions 3.8 and 3.9 for a description of the minimum weight codewords of $\mathcal{C}^\perp$ and a shortening of $\mathcal{C}^\perp$ with better parameters (when Y is smooth). For smooth curves on a elliptic quadric surface U we prove the following result.

Theorem 1.3. *Let $U \subset \mathbb{P}^3$ be an elliptic quadric surface defined over K. Let $C \subset U$ be a smooth curve of degree $2a$ defined over K, E a zero-dimensional subscheme of C defined over K and $B \subseteq C(K) \setminus E_{red}$ a finite set. Fix a positive integer $x \geq \deg(E) - 1$. Assume $n := \sharp(B) > ax - \deg(E)$. Set $k = (x+1)^2 - \deg(E)$ if $x < a$ and $k = (x+1)^2 - (x-a+1)^2 - \deg(E)$ if $x \geq a$. Set $\mathcal{C} := \mathcal{C}(B, \mathcal{O}_C(x)(-E))$. Then $\mathcal{C}$ is an $[n,k]$-code and its dual $\mathcal{C}^\perp$ has minimum distance $\geq 2x+2-\deg(E)$. If $\mathcal{C}^\perp$ has minimum distance $2x+2-\deg(E)$, then for each codeword $\mathbf{w}$ of $\mathcal{C}^\perp$ with minimum weight there is a smooth linear section A of U defined over K and such that $S \cup E \subset A$, where $S \subseteq B$ is the support of $\mathbf{w}$.*

Very few maximal curves are contained in a quadric surface ([7], §10.4) and, except very small fields, all of them are on a quadric cone, T, and contains the vertex O of the cone ([7], Lemma 10.39 (iv), Theorem 10.41 and Proposition 10.44). Since the quadric cone $T \subset \mathbb{P}^3$ contains many curves with a large number of K-points, it is natural to study the Goppa codes arising studying curves inside T. In section 5 we prove the following result.

Theorem 1.2. *Let $T \subset \mathbb{P}^3$ be a geometrically integral quadric cone defined over K. Let $C \subset T$ be a smooth and geometrically connected curve of degree $2a+\epsilon$, $a > 1$, $\epsilon \in \{0,1\}$, defined over K. Fix an integer $y \geq 3$ and a zero-dimensional scheme $E \subset C$ with $\deg(E) < y$. Fix a set $B \subset C(K) \setminus E_{reg}$ such that $n := \sharp(B) > y \cdot \deg(C) - \deg(E)$. Set $k := (y+1)^2 - \deg(E)$ if $y < a$, $k := (y+1)^2 - (y-a+1)^2 - \deg(E)$ if $\epsilon = 0$ and $y \geq a$, $k := (y+1)^2 - (t-a)(t-a+1) - \deg(E)$ if $y \geq a$ and $\epsilon = 1$. Set $\mathcal{C} := \mathcal{C}(B, \mathcal{O}_C(y)(-E))$.*

(i) $\mathcal{C}$ is an $[n,k]$-code and $\mathcal{C}^\perp$ has minimum distance $\geq y+2-\deg(E)$.

(ii) Let $\mathcal{S}$ be the set of all lines $J \subset C$ such that $\deg((E \cup B) \cap J) \geq y+2$. Let $\mathcal{S}'$ be the set of all $J \in \mathcal{S}$ such that the integer $e := \deg(E \cap J) \geq 0$ is maximal among all lines in $\mathcal{S}$. Let $\mathcal{S}'(B)$ be the set of all pairs (S,J), where $J \in \mathcal{S}'$, $S \subseteq J \cap B$ and $\sharp(S) = y+2-e$. Let $\mathcal{S}''(B)$ be the set of all $S \subset B$ with $(J,S) \in \mathcal{S}'(B)$. If $\mathcal{S} = \emptyset$, then $\mathcal{C}^\perp$ has minimum distance $\geq 2y+2-\deg(E)$. If $\mathcal{S} \neq \emptyset$, then $\mathcal{C}^\perp$ has minimum distance $y+2-e$, each codeword of $\mathcal{C}^\perp$ is supported by a unique $S \in \mathcal{S}''(B)$ and each $S \in \mathcal{S}''(B)$ is the support of a unique (up to a non-zero scalar) codeword of $\mathcal{C}^\perp$ with minimum weight.

For each codeword of $\mathcal{C}^\perp$ with weight $\le 2y+1-\deg(E)$ (say with support $S \subset B$) there is a unique $J \in \mathcal{S}$ such that $S \subset J$ and $\deg(J \cap (E \cup S)) \ge y+2$.

2. Preliminaries

Let $\overline{K}$ denote the algebraic closure of K. Every variety or scheme X arising in this paper is defined over $\overline{K}$. Let X be any projective scheme over a field L_1 and $\mathcal{F}$ a coherent sheaf on X defined over a field $L_2 \supseteq L_1$. Fix any field $L_3 \supseteq L_2$. Then X and $\mathcal{F}$ are defined over L_3; call them X_{L_3} and $\mathcal{F}_{L_3}$ as objects over L_3. Since any extension of fields is flat, the integers $\dim_{L_3}(H^i(X_{L_3}, \mathcal{F}_{L_3}))$, $i \in \mathbb{N}$, does not depend from the choice of L_3 ([4], Proposition III.9.3). Set $h^i(X, \mathcal{F}) := \dim_{L_3}(H^i(X_{L_3}, \mathcal{F}_{L_3})$ for any field L_3 on which both X and $\mathcal{F}$ are defined. Hence to compute each cohomology group it is sufficient to quote references which state the corresponding result over an algebraically closed base field.

Lemma 2.1. *Fix an integer $x > 0$, a smooth curve $C \subset \mathbb{P}^r$ such that $h^1(\mathbb{P}^r, \mathcal{I}_C(x)) = 0$, a zero-dimensional scheme $E \subset C$ such that $\deg(E) \le x+1$ and a finite subset $B \subset C$ such that $B \cap E_{red} = \emptyset$. Let $\mathcal{C} := \mathcal{C}(\mathcal{O}_C(x)(-E))$ the code on C obtained evaluating the complete linear system $|\mathcal{O}_C(x)(-E)|$ at the points of B. Set $c := \deg(C)$. Assume $\sharp(B) + \deg(E) > xc$. Set $n := \sharp(B)$, and $k := h^0(C, \mathcal{O}_C(x)) - \deg(E)$. Then $\mathcal{C}$ is an $[n,k]$-code and the minimum distance of $\mathcal{C}^\perp$ is the minimal cardinality, s, of a subset of B such that $h^1(\mathbb{P}^2, \mathcal{I}_{S\cup E}(x)) > 0$ (or, equivalently, $h^1(C, \mathcal{O}_C(-E-S)) > h^1(C, \mathcal{O}_C(-E))$. A codeword of $\mathcal{C}^\perp$ has weight s if and only if it is supported by $S \subseteq B$ such that $\sharp(B) = s$ and $h^1(\mathbb{P}^r, \mathcal{I}_{E\cup S}(x)) > h^1(\mathbb{P}^r, \mathcal{I}_E(x))$.*

Proof. We imposed that B does not intersect the support of E. Since $h^1(\mathbb{P}^r, \mathcal{I}_C(x)) = 0$, the restriction map $\rho_x : H^0(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(x)) \to H^0(C, \mathcal{O}_C(x))$ is surjective. Hence $\mathcal{C}$ is obtained evaluating a family of homogeneous degree x polynomials (the ones vanishing on the scheme E) at the points of B. Since $\deg(E) \le x+1$, we have $h^1(\mathbb{P}^r, \mathcal{I}_E(x)) = 0$ ([1], Lemma 34), i.e. E imposes $\deg(E)$ independent conditions to the set of all degree x homogeneous polynomials. Hence the restriction map $\rho_{x,E} : H^0(\mathbb{P}^r, \mathcal{I}_E(x)) \to$

$H^0(C, \mathcal{O}_C(x)(-E))$ is surjective. Hence a finite subset $S \subset C \setminus E_{red}$ imposes independent condition to $H^0(C, \mathcal{O}_C(x)(-E))$ if and only if S imposes independent conditions to $H^0(\mathbb{P}^r, \mathcal{I}_E(x))$. S imposes independent conditions to $H^0(\mathbb{P}^r, \mathcal{I}_E(x))$ if and only if $h^1(\mathbb{P}^r, \mathcal{I}_{E\cup S}(x)) = h^1(\mathbb{P}^r, \mathcal{I}_E(x))$ (here we use again that $S \cap E = \emptyset$). This completes the proof.

Remark 2.2. Take the set-up of the proof of Lemma 2.1. Since the restriction maps ρ_x and $\rho_{x,E}$ are surjective, the condition " $h^1(\mathbb{P}^2, \mathcal{I}_{E\cup S}(x)) > h^1(\mathbb{P}^2, \mathcal{I}_E(x))$ " is equivalent to the condition " $h^0(C, \mathcal{O}_C(d)(-(E \cup S)) > h^0(C, \mathcal{O}_C(d)(-E)) - \sharp(S)$ or, equivalently (Riemann-Roch) $h^1(C, \mathcal{O}_C(d)(-(E \cup S)) > h^1(C, \mathcal{O}_C(d)(-E))$. In the applications we will usually have $d \le \deg(C) - 2$ and hence $h^1(C, \mathcal{O}_C(d)) > 0$.

Remark 2.3. 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 $h^1(W, \mathcal{I}_Z \otimes L) > 0$.

3. On a hyperbolic quadric surface

In this paper Q is a smooth quadric surface defined over K and hyperbolic, i.e. Q isomorphic to $\mathbb{P}^1 \times \mathbb{P}^1$ over K. See [4] and [6] for the geometry of quadric hypersurfaces over a finite field, [7] for their use for curves over a finite field and [4], §V.2, for quadric surfaces over an algebraically closed base field.

There are two rulings on Q defined over K and $\mathrm{Pic}(Q)(K)$ is freely generated by the two rulings, which we call $\mathcal{O}_Q(1, 0)$ and $\mathcal{O}_Q(0, 1)$. Hence there is a bijection $(a, b) \mapsto \mathcal{O}_Q(a, b)$ between $\mathbb{Z}^2$ and $\mathrm{Pic}(Q)(K)$.

Remark 3.1. Since $Q \cong \mathbb{P}^1 \times \mathbb{P}^1$, Künneth formula gives

$$H^0(Q, \mathcal{O}_Q(a, b)) \cong H^0(\mathbb{P}^1, \mathcal{O}_{\mathbb{P}^1}(a)) \otimes H^0(\mathbb{P}^1, \mathcal{O}_{\mathbb{P}^1}(b)),$$

$$H^0(Q, \mathcal{O}_Q(a, b)) \cong H^0(\mathbb{P}^1, \mathcal{O}_{\mathbb{P}^1}(a)) \otimes H^1(\mathbb{P}^1, \mathcal{O}_{\mathbb{P}^1}(b)) \oplus H^1(\mathbb{P}^1, \mathcal{O}_{\mathbb{P}^1}(a)) \otimes H^0(\mathbb{P}^1, \mathcal{O}_{\mathbb{P}^1}(b))$$

in which the tensor powers are over the base field and all cohomology groups H^i, $i = 0, 1$, are finite-dimensional over that field. Hence $H^0(Q, \mathcal{O}_Q(a, b)) = 0$ if either $a < 0$ or $b < 0$,

$h^0(Q, \mathcal{O}_Q(a,b)) = (a+1)(b+1)$ if $a \ge -1$ and $b \ge -1$ and $H^1(Q, \mathcal{O}_Q(a,b)) = 0$ if $a \ge -1$ and $b \ge -1$.

Remark 3.2. We have $\omega_Q \cong \mathcal{O}_Q(-2,-2)$ ([4], Example II.8.20.3). Fix integers $(a,b) \in \mathbb{N}^2 \setminus \{(0,0)\}$ and any divisor $Y \in |\mathcal{O}_Q(a,b)|$ defined over a field K. For all integers x, y we have an exact sequence of coherent sheaves

$$0 \to \mathcal{O}_Q(x-a, y-b) \to \mathcal{O}_Q(x,y) \to \mathcal{O}_Y(x,y) \to 0 \tag{1}$$

The adjunction formula gives $\omega_Y \cong \mathcal{O}_Y(a-2, b-2)$ ([4], Proposition V.1.5 and Example V.1.5.2). Duality ([4], Corollary III.7.8) and Remark 3.1 gives $h^2(Q, \mathcal{O}_Q(-2,-2)) = 1$ and $h^2(Q, \mathcal{O}_Q(x,y)) = 0$ if $x \ge -2$, $y \ge -2$ and $(x,y) \ne (-2,-2)$. Hence Remark 3.1 and the case $x = a-2$, $y = a-2$ of (1), give that the restriction map $\rho_Y : H^0(Q, \mathcal{O}_Q(a-2), b-2)) \to H^0(Y, \omega_Y)$ is an isomorphism defined over K. Now assume that Y is geometrically integral and let $u : C \to Y$ be the normalization map. The map u is defined over K and C is a geometrically smooth projective curve defined over K, because any finite field is perfect. There is an ideal sheaf $\mathcal{J}$ of $\mathcal{O}_Q$ whose support is the union $\mathrm{Sing}(Y)$ of all singular points of $Y(\overline{K})$ such that there is an isomorphism $\sigma_Y : H^0(Q, \mathcal{J}(a-2, b-2)) \to H^0(C, \omega_C)$; $\mathcal{J}$ is called the conductor of u or the conductor of Y. The sheaf $\mathcal{J}$, the set $\mathrm{Sing}(Y)$ and the isomorphism σ_Y are defined over K. However, if $\sharp(\mathrm{Sing}(Y)) \ge 2$, then a single point of $\mathrm{Sing}(Y)$ may be not defined over K; we are only sure of the existence of an extension K' of K of degree $\le \sharp(\mathrm{Sing}(Y))$ such that each $P \in \mathrm{Sing}(Y)$ is defined over F'. If each singular point of Y is either an ordinary node or an ordinary cusp, then $\mathcal{J}$ is the ideal sheaf $\mathcal{I}_{\mathrm{Sing}(Y)}$ of the set $\mathrm{Sing}(Y)$. We have $\deg(\mathcal{O}_Q/\mathcal{J}) = p_a(Y) - p_a(C)$. Since σ_Y is an isomorphism, $h^0(Y, \omega_Y) = p_a(Y)$ and $h^0(C, \omega_C) = p_a(C)$, we have $H^0(Q, \mathcal{J}(a-2, b-2)) = (a-1)(b-1) - p_a(Y) + p_a(C)$ and $h^1(Q, \mathcal{J}(a-2, b-2)) = 0$. For any $(x,y) \in \mathbb{Z}^2$ set $\mathcal{O}_C(x,y)) := u^*(\mathcal{O}_C(x,y))$. Notice that $\mathcal{O}_C(x,y)$ is a line bundle of degree $ya + bx$ on C defined over K. For any zero-dimensional scheme $E \subset Y_{reg}$, u induces an isomorphism between $u^{-1}(E)$ and E. In particular for any $P \in Y_{reg}$ and any integer $e > 0$ we may identify the unique degree e zero-dimensional subscheme of Y with P as its support with the effective divisor $eu^{-1}(P)$ of the smooth curve C. Hence we may use u to study certain

Goppa codes on C with certain data on Y (for instance, for a one-point code associated to $O \in C$ we require $O \notin u^{-1}(\mathrm{Sing}(Y))$.

Remark 3.3. Fix integers m, m' with $(m, m') \in \mathbb{N}^2 \setminus \{(0,0)\}$ and any divisor $H \in |\mathcal{O}_Q(m, m')|$. Let $\mathrm{Res}_H(Z)$ be the residual scheme of Z with respect to H, i.e. the closed subscheme of Q with $\mathcal{I}_Z : \mathcal{I}_H$ as its ideal sheaf. We have $\deg(Z) = \deg(\mathrm{Res}_H(Z)) + \deg(H \cap Z)$ (scheme-theoretic intersection) and for all $(v, v') \in \mathbb{Z}^2$ there is an exact sequence of sheaves on Q:

$$0 \to \mathcal{I}_{\mathrm{Res}_{H(Z)}}(v-m, v'-m') \to \mathcal{I}_Z(v, v') \to \mathcal{I}_{H\cap Z, H}(v, v') \to 0 \tag{2}$$

Remark 3.4. Fix $(x, y) \in \mathbb{N}^2$, any $D \in |\mathcal{O}_Q(1,0)|$, any $D' \in |\mathcal{O}_Q(0,1)|$ and any $A \in |\mathcal{O}_Q(1,1)|$. We have $D \cong \mathbb{P}^1 \cong D'$, $\deg(\mathcal{O}_D(x,y)) = y$ and $\deg(\mathcal{O}_{D'}(x,y)) = x$. Hence $h^0(D, \mathcal{O}_D(x,y)) = y+1$ and $h^0(D', \mathcal{O}_{D'}(x,y)) = x+1$. Since $h^1(Q, \mathcal{O}_Q(x-1, x-1)) = 0$ (Remark 3.1), we have $h^0(A, \mathcal{O}_A(x,y)) = (x+1)(y+1) - xy = x+y+1$. If W is a zero-dimensional subscheme of D (resp. D', resp. A) and $\deg(W) \geq y+2$ (resp. $\deg(W) \geq x+2$, resp. $\deg(W) \geq x+y+2$), then $h^1(D, \mathcal{I}_{W,D}(x,y)) > 0$ (resp. $h^1(D', \mathcal{I}_{W,D'}(x,y)) > 0$, resp. $h^1(A, \mathcal{I}_{W,A}(x,y)) > 0$). Fix any subscheme $E \subseteq Z$. Remark 2.3 gives that if $h^1(Q, \mathcal{I}_E(x,y)) > 0$, then $h^1(Q, \mathcal{I}_Z(x,y)) > 0$. Hence if either $\deg(D \cap Z) \geq y+2$ or $\deg(D' \cap Z) \geq x+2$ or $\deg(A \cap Z) \geq x+y+2$, then $h^1(Q, \mathcal{I}_Z(x,y)) > 0$.

Lemma 3.5. *Fix positive integers x, y. Fix $D \in |\mathcal{O}_Q(1,0)|$ and $D' \in |\mathcal{O}_Q(0,1)|$ and set $A := D \cup D'$. Let $Z \subset A$ be a zero-dimensional scheme. We have $h^1(A, \mathcal{I}_Z(x,y)) > 0$ if and only if either* $\deg(Z) \geq x+y+2$ *or* $\deg(D \cap Z) \geq y+2$ *or* $\deg(D' \cap Z) \geq x+2$.

Proof. Remark 3.4 gives the " if " part. Now assume $h^1(A, \mathcal{I}_A(x,y)) > 0$. Since $h^1(Q, \mathcal{O}_Q(x-1, y-1)) = 0$ (Remark 3.1) and $Z \subset A$, our assumption is equivalent to $h^1(Q, \mathcal{I}_Z(x,y)) > 0$. Assume also $\deg(Z) \leq x+y+1$ and $\deg(Z \cap A) \leq y+1$. See Z as a closed subscheme of Q to compute $\mathrm{Res}_D(Z)$. Since $\deg(Z \cap D) \leq y+1$, we have $h^1(D, \mathcal{I}_{Z\cap D, D}(x,y)) = 0$. Hence (2) with $H := D$ and $(v, v') = (x,y)$ gives $h^1(Q, \mathcal{I}_{\mathrm{Res}_{D(Z)}}(x-1, y)) > 0$. Since $A \subset D \cup D'$, we have $\mathrm{Res}_D(Z) \subset D'$. Hence $h^1(Q, \mathcal{I}_{\mathrm{Res}_{D(Z)}}(x-1, y)) = h^1(D', \mathcal{I}_{\mathrm{Res}_{D(Z)}, D'}(x-1, y))$. Hence $\deg(\mathrm{Res}_D(Z)) \geq x+1$. Since $Z \cap D \subseteq \mathrm{Res}_D(Z)$, we get $\deg(Z \cap D') = \deg(\mathrm{Res}_D(Z)) = x+1$. Now we reverse the role of D and D'. Since $\deg(D'\cap Z) \le x+1$, we have $h^1(D',\mathcal{I}_{Z\cap D',D'}(x,y)) = 0$. Hence (2) with $(m,m') = (0,1)$ gives $h^1(Q,\mathcal{I}_{\mathrm{Res}_{D'}(Z)}(x,y-1)) > 0$. Since $\mathrm{Res}_{D'}(Z) \subset D'$, the first part of the proof gives $\deg(\mathrm{Res}_{D'}(Z)) \ge y+1$. Hence $\deg(Z) = \deg(\mathrm{Res}_{D'}(Z)) + \deg(D'\cap Z) \ge x+y+2$. This completes the proof.

The proof of Lemma 3.5 gives the following result.

Lemma 3.6. *Fix positive integers x, y, $D \in |\mathcal{O}_Q(1,0)|$, $D' \in |\mathcal{O}_Q(0,1)|$ and $A \in |\mathcal{O}_Q(1,1)|$. Fix zero-dimensional schemes $Z_1 \subset D$, $Z_2 \subset D'$ and $Z_3 \subset A$ such that $\deg(Z_1) = y+2$, $\deg(Z_2) = x+2$ and $\deg(Z_3) = x+y+2$. If A is reducible, say $A = D_1 \cup D_2$ with $D_1 \in |\mathcal{O}_Q(1,0)|$ and $D_2 \in |\mathcal{O}_Q(0,1)|$ then assume $\deg(Z_3\cap D_1) \le y+1$ and $\deg(Z_3 \cap D_2) \le x+1$ (equivalently, assume $Z_3 \cap D_1 \cap D_2 = \emptyset$, $\deg(Z_3\cap D_1) = y+1$ and $\deg(Z_3\cap D_2) = x+1$). Then $h^1(Q,\mathcal{I}_{Z_i}(x,y)) = 1$, $i = 1,2,3$.*

Lemma 3.7. *Fix non-negative integer x, y, z such that $x \ge y \ge 0$ and $x > 0$. Let $Z \subset Q$ be any zero-dimensional scheme such that $\deg(Z) = z$.*

(i) If $z \le y+1$, then $h^1(Q,\mathcal{I}_Z(x,y)) = 0$.

(ii) Assume $y+2 \le z \le 3y-1$; if $x = y$, then assume $z \le 3y-2$. Then $h^1(Q,\mathcal{I}_Z(x,y)) > 0$ if and only if either there is a line $D \subset Q$ of type $(1,0)$ such that $\deg(Z\cap D) \ge y+2$ or $z \ge x+2$ and there is a line $D' \subset$ of type $(0,1)$ such that $\deg(D'\cap Z) \ge x+2$ or $z \ge x+y+2$ and there is $A \in |\mathcal{O}_Q(1,1)|$ such that $\deg(A\cap Z) \ge x+y+2$.

Proof. Remark 3.4 proves the “ if ” part of (ii).

(a) Now we prove (i) and the “ only if ” part of (ii). If $z = 0$, i.e. if $Z = \emptyset$, then (i) is true (Remark 3.1). Hence we may assume $z > 0$ and prove simultaneously (i) and the “ only if ” part of (ii) by induction on z. We also use induction on $x+y$, the case $(x,y) = (1,0)$ being obvious.

Set $Z_0 := Z$ and $z_0 := z$. Fix $D_1 \in |\mathcal{O}_Q(1,0)|$ such that $a_1 := \deg(Z\cap D_1)$ is maximal and set $Z_1 := \mathrm{Res}_{D_1}(Z)$ and $z_1 := z - a_1$. For all integers $i \ge 2$ define recursively the divisors $D_i \in |\mathcal{O}_Q(1,0)|$, the scheme $Z_i \subseteq Z_{i-1}$ and the integers a_i, z_i in the following way. Take as D_i any divisor $D_i \in |\mathcal{O}_Q(1,0)|$ such that $a_i := \deg(Z_{i-1}\cap D_i)$ is maximal and set $Z_i := \mathrm{Res}_{D_i}(Z_{i-1})$ and $z_i := z_{i-1} - a_i$. Notice that $z_i = \deg(Z_i)$ and in particular

$z_i \ge 0$. Since $a_i \ge 0$, the sequence $\{z_i\}$ is non-increasing. Since $Z \ne \emptyset$, the maximality of the integer a_1 implies $a_1 > 0$, i.e. $z_1 < z_0$. For the same reason if $z_i > 0$ then $a_i > 0$ and $0 \le z_{i+1} < z_i$. Hence $z_i = 0$ and $Z_i = \emptyset$ if $i \ge \deg(Z)$. If $z_1 \ge y+2$, then we are done. Hence we may assume $1 \le a_1 \le y+1$. Hence $a_i \le y+1$ for all i. Hence $h^1(D_i, \mathcal{I}_{D_i \cap Z_{i-1}, D_i}(x,y)) = 0$ for all $i > 0$. Applying (2) for $(m,m',v,v') = (1,0,x-i+1,y)$ we get $h^1(Q, \mathcal{I}_{Z_i}(x-i,y)) \ge h^1(Q, \mathcal{I}_{Z_{i-1}}(x-i+1,y))$. Starting from the case $i=1$ we get $h^1(Q, \mathcal{I}_{Z_i}(x-i,y)) > 0$ for all i. Let k be the first positive integer such that $z_k = 0$. Since $h^1(Q, \mathcal{O}_Q(v,y)) = 0$ for all $v \ge -1$, we get $k \ge x+2$. Hence $z \ge x+2$. Fix $R_1 \in |\mathcal{O}_Q(0,1)|$ such that $b_1 := \deg(Z \cap R_1)$ is maximal. If $w_1 \ge x+2$, then we are done. Hence we may assume $1 \le b_1 \le x+1$.

(b) Set $M_0 := Z$ and $m_0 := z$. Fix any $A_1 \in |\mathcal{O}_Q(1,1)|$ such that $e_1 := \deg(Z \cap A)$ is maximal among all elements of $|\mathcal{O}_Q(1,1)|$. For all integers $i \ge 2$ define recursively the divisors $A_i \in |\mathcal{O}_Q(0,1)|$, the scheme $M_i \subseteq M_{i-1}$ and the integer e_i in the following way. Take as A_i any divisor $A_i \in |\mathcal{O}_Q(1,1)|$ such that $e_i := \deg(M_{i-1} \cap A_i)$ is maximal and set $M_i := \mathrm{Res}_{A_i}(M_{i-1})$ and $m_i := m_{i-1} - e_i$. Notice that $m_i = \deg(M_i)$ and in particular $m_i \ge 0$. Since $e_i \ge 0$, the sequence $\{m_i\}$ is non-increasing. Since $h^0(Q, \mathcal{O}_Q(1,1)) = 4$, any degree ≤ 3 zero-dimensional subscheme of Q is contained in some divisor of type $(1,1)$. Hence either $e_i \ge 3$ or $m_i = 0$. Hence the first integer, s, such that $e_s = 0$ satisfies $s \le \lceil \deg(Z)/3 \rceil$. Since $z < 3y$, we have $e_y = 0$. Since $s \le y \le x$, we have $h^1(Q, \mathcal{O}_Q(x-s, y-s)) = 0$. Hence applying s times (2) with integers $(m,m') := (x+1-i, y+1-i)$, $1 \le i \le s$, with $H = A_i$ and taking M_{i-1} instead of Z, we get the existence of an integer $t \in \{1, \dots, s-1\}$ such that $h^1(A_t, \mathcal{I}_{A_t \cap M_{t-1}}(x-t+1, y-t+1)) > 0$. Call t the minimal such an integer. Recall that $t \le y$.

(b1) First assume that A_t is irreducible. Hence $A_t \cong \mathbb{P}^1$. Since $\deg(\mathcal{O}_{A_t}(x-t+1, y-t+1)) = x+y-2t+2$, we get $e_t \ge x+y-2t+4$. Since $e_c \ge e_t$ for all $c \le t$, we get $z \ge t(x+y-2t+4)$. The function $\phi : \mathbb{Z} \to \mathbb{Z}$ defined by $\phi(c) = c(x+y-2c+4)$ is convex in the interval $[1, (x+y+4)/2]$ and it is increasing if $c \le (x+y+4)/4$ and decreasing in the interval $((x+y+4)/4, (x+y+4)/2]$. First assume $t=1$; we get $\deg(Z \cap A_1) \ge x+y+2$, concluding this case. Now assume $t=2$. We get $z \ge 2(x+y) \ge 4y$, absurd. Now assume $x+y$ odd and $t=(x+y+3)2$. Since $e_i \geq 3$ for all $i<t$, we get $z \geq 3(x+y+1)/2+(x+y+3)/2 \geq 3y$, absurd. Now assume $x+y$ even and $t=(x+y)/2$; we get $z \geq 3(x+y-2)/2+2 \geq 3y-1$ and equality only if $x=y$, a contradiction. Since $t \leq y$, we do not need to test cases with $t>(x+y)/2$ and hence we completed the proof if A_t is irreducible.

(b2) Now assume that A_t is reducible and write $A_t = D \cup D'$ with $D \in |\mathcal{O}_Q(1,0)|$ and $D' \in |\mathcal{O}_Q(0,1)|$. By the proof of step (b1) we may assume $e_t \leq x+y-2t+3$. Lemma 3.5 gives that either $\deg(D \cap M_{t-1}) \geq y-t+3$ or $\deg(D' \cap M_{t-1}) \geq x-t+3$. First assume $\deg(D \cap M_{t-1}) \geq y-t+3$; since $e_t \geq \deg(D \cap M_{t-1})$, we get $z \geq t(y-t+3)$. If $3 \leq t \leq y$, we get $z \geq 3y$, absurd. Recall that $t \leq y$. Assume $t=2$. Since $a_1 \geq \deg(D \cap Z) \geq \deg(D \cap M_1)$, we get $a_1 = y+1$. Since $h^1(Q, \mathcal{I}_{Z_1}(x-1,y))>0$. Since $\deg(Z_1) = z-y-1 < \min\{3(y-1), 3(x-1)\}$, we may apply the lemma for $(x-1,y)$ and get that either $a_2 \geq y+2$ (absurd) or there is a line $D' \in |\mathcal{O}_Q(0,1)|$ such that $\deg(D' \cap Z_1)) \geq x+1$ or there is $F \in |\mathcal{O}_Q(1,1)|$ such that $\deg(F \cap \mathrm{Res}_D(F \cap Z)) \geq x+y+1$. If F exists, then $z \geq y+1+(x+y-1) \geq 3y$, absurd. If D' exists, then we are done, because $\deg(Z \cap (D \cap D') = \deg(Z \cap D) + \deg(Z_1) \cap D') \geq x+y+2$. Now assume $t=1$. Applying Lemma 3.5 to the reducible curve A_1 we get that either $a_1 \geq y+2$ or $b_1 \geq x+2$ or $\deg(Z \cap A_1) \geq x+y+2$.

Now assume $\deg(D' \cap M_{t-1}) \geq x-t+3$. Hence $z \geq t(x-t+3)$. Recall that $t \leq y$. If $3 \leq t \leq y$, then we get $z \geq 3y$, absurd. Assume $t=2$. Since $b_1 \geq \deg(D' \cap Z) \geq x-t+3 = x+1$, we get $b_1 = x+1$ and $\deg(D' \cap Z) = x+1$. Since $h^1(D', \mathcal{I}_{Z \cap D'}(x,y)) = 0$, (2) with $H = D'$ gives $h^1(Q, \mathcal{I}_{\mathrm{Res}_{D'(Z)}}(x,y-1)) > 0$. Assume for the moment $x \geq 2$. Since $\deg(\mathrm{Res}_{D'}(Z)) = z-x-1 < 3y-4$, we may use the inductive assumption on $x+y$ and conclude. If $x=1$, then $z=0$ by our numerical assumptions. This completes the proof.

Proposition 3.8. *Take the set-up of Theorem 1.2. Assume $E \neq \emptyset$. If $x=y$, then assume $\deg(E) \geq 2$. Assume that $\mathcal{C}^\perp$ has minimum distance $y+2-\deg(E)$. The curve D or D' is uniquely determined by E and that not both may occur. Call D'' the one which occur and $w = \sharp(D \cap B)$. Let $\mathcal{S}$ be the set of all $S \subseteq B \cap D''$ such that $\sharp(S) = y+2-\deg(E)$.*

There are $(\sharp(K)-1)\binom{w}{y+2-\deg(E)}$ codewords with minimal weight, each of them having as support an element of $\mathcal{S}$, while any $S \in \mathcal{S}$ is the support (up to a non-zero scalar) of a codeword with minimum weight.

Proof. Each codeword of $\mathcal{C}^{\perp}$ has as support some $S \in \mathcal{S}$ (Lemma 2.1).The fact that each $S \in \mathcal{S}$ is the support of a codeword follows from Lemma 3.7, which also shows that the codeword has minimal weight. The uniqueness (up to a non-zero constant) of the codeword supported from each $S \in \mathcal{S}$ follows from (and it is equivalent to) Lemma 3.6. This completes the proof.

Proposition 3.9. *Take the set-up of Proposition 3.8 and set $B_1 := B \setminus B \cap D''$ and $n_1 := \sharp(B_1)$. Assume $n_1 > by + a(x-1)$ if $D'' \in |\mathcal{O}_Q(1,0)|$ and $n_1 > b(y-1) + ax$ if $D'' \in |\mathcal{O}_Q(0,1)|$. Set $\mathcal{C}_1 := \mathcal{C}(B_1, \mathcal{O}_C(x,y)(-E))$. Then the code $\mathcal{C}_1$ is an $[n_1, k]$-code and its dual $\mathcal{C}_1^{\perp}$ has minimum distance $\geq y+2$ (case $y \neq x$) or $\geq y+1$ (case $x = y$).*

Proof. The parameters n_1 and $k := (y+1)(x+1) - \deg(E)$ of the code are obvious, because our assumptions imply $\sharp(B_1) + \deg(E) > ay + bx = \deg(\mathcal{O}_C(x,y))$.

First assume $D'' \in |\mathcal{O}_Q(1,0)|$. Set $\mathcal{C}_2 := \mathcal{C}(B_1, \mathcal{O}_C(y, x-1))$. Since $n_1 > by + a(x-1)$, $\mathcal{C}_2$ is an $[n_1, k_1]$-code with $k_1 = (y+1)x$ (we are assuming $x \leq a$ and $y \leq b$). Since $E \subset D''$, $\mathcal{C}_1$ is a subcode of $\mathcal{C}$. Hence it is sufficient to prove that $\mathcal{C}_2^{\perp}$ has minimum distance $\geq y+2$ (case $y \neq x$) or $\geq y+1$ (case $x = y$). Apply Lemma 3.7 with $Z = S$, $\sharp(S) = \min\{y, x-1\}$, i.e. use Proposition3.8 for the integers $(x-1, y)$ and the scheme $\emptyset$ instead of E.

Now assume $D'' \in |\mathcal{O}_Q(0,1)|$. Hence $x = y$. We repeat the proof of the case $D'' \in |\mathcal{O}_Q(1,0)|$ taking $\mathcal{C}(B_1, \mathcal{O}_C(x, y-1))$ instead of $\mathcal{C}_2$. This completes the proof.

4. On an elliptic quadric surface

Let $U \subset \mathbb{P}^3$ be a smooth and elliptic quadric surface. Hence $\mathrm{Pic}(U)(K) \cong \mathbb{Z}$, $\mathcal{O}_U(1)$ is a generator of $\mathrm{Pic}(U)(K)$ and every curve on U defined over K is the complete intersection of U with a surface of $\mathbb{P}^3$ defined over K.

Proof of Theorem 1.3. The curve C is the complete intersection of U and a surface of degree a. Hence it is a complete intersection. Hence the restriction map $H^0(\mathbb{P}^3, \mathcal{O}_{\mathbb{P}^3}(x)) \to$

$H^0(C, \mathcal{O}_C(x))$ is surjective. Hence the restriction map $H^0(U, \mathcal{O}_U(x)) \to H^0(C, \mathcal{O}_C(x))$ is surjective. Since $h^1(U, \mathcal{O}_U(x-a)) = 0$ (Remark 3.1) we get $h^0(C, \mathcal{O}_C(x)) = (x+1)^2$ if $x < a$ and $h^0(C, \mathcal{O}_C(x)) = (x+1)^2 - (x-a+1)^2$ if $x \geq a$. Since $\deg(E) \leq x+1$, Lemma 3.7 gives $h^0(C, \mathcal{O}_C(x)) - \deg(E)$. Since $\sharp(B) > ax - \deg(E) = \deg(\mathcal{O}_C(x)(-E))$, we have $h^0(C, \mathcal{O}_C(x)(-E-B)) = 0$. Hence $\mathcal{C}$ is an $[n,k]$-code. Fix a set $S \subseteq B$ which is the support of a codeword of $\mathcal{C}^\perp$ with minimal weight. Lemma 2.1 gives $h^1(\mathbb{P}^3, \mathcal{I}_{E\cup S}(x)) > 0$ and $h^1(\mathbb{P}^3, \mathcal{I}_{E\cup S'}(x)) = 0$ for any $S' \subsetneq S$. Hence $h^1(U, \mathcal{I}_{E\cup S}(x)) > 0$ and $h^1(U, \mathcal{I}_{E\cup S'}(x)) = 0$ for any $S' \subsetneq S$.

Let K_1 be the quadratic extension of K. The surface U is defined over K_1, but over K_1 the degree 2 surface U_{K_1} is a hyperbolic quadric, Q. We apply Lemma 3.7 with $x = y$. We get the existence either of $D \in |\mathcal{O}_Q(1,0)|$ such that $\deg((S\cup E)\cap D) \geq x+2$ or the existence of $D' \in |\mathcal{O}_Q(1,0)|$ such that $\deg(D' \cap (B\cup E)) \geq x+2$ or the existence of $A \in |\mathcal{O}_Q(1,1)|$ such that $\deg((S\cup E)\cap A) \geq 2x+2$; the curves D (or D' or A) are defined over K_1.

We claim that neither D nor D' may exist. To prove this claim we first assume $\deg(E) \leq x$. Since $x+2 \geq 2+\deg(E)$, there would be $P, P' \in S\cap D$ (or $P, P' \in S\cap D'$) with $P \neq P'$. Each point of S is defined over K and hence the line D (or D') spanned by P and P' would be a line of U defined over K. Since $E\cup S$ is contained in D (or D') and $x+2 > 2$, Bezout theorem implies that U is contained in the quadric surface U, contradicting the assumption that U is an elliptic quadric surface. Now assume $\deg(E) = x+1$. Since $\deg(E) \geq 2$, D or D' is spanned by E. Hence D is defined over K. Again, Bezout theorem gives that U contains a line, absurd. Hence our claim is true. Hence there is $A \in |\mathcal{O}_Q(1,1)|$ such that $\deg((S\cup E)\cap A) \geq 2x+2$. Hence $\sharp(S) \geq \sharp(S\cap A) \geq 2x-2-\deg(E)$.

Now assume that $\mathcal{C}^\perp$ has minimum weight $2x+2-\deg(E)$. Since $h^1(U, \mathcal{I}_{E\cup S'}(x)) = 0$ for any $S' \subsetneq S$, Lemma 3.5 gives $S \subset A$ and $\sharp(S) = 2x+2-\deg(E)$. Assume for the moment $E\cup S \subset A_1$ with $A_1 \in |\mathcal{O}_Q(1,1)|$, A_1 defined over any extension of K, and $A_1 \neq A$. Since $\mathcal{O}_Q(1,1)\cdot\mathcal{O}_Q(1,1) = 2 > \deg(E\cup S)$, we get that A and A_1 are reducible and with a common irreducible component, M. Write $A = M\cup M'$ and $A_1 = M\cup M''$ with $M'' \neq M'$ and, say, M of type $(1,0)$. Since $A\cap A_1 = M$ and $\sharp(S) \geq 2x+2-\deg(E) \geq 2$,

M contains at least two points of S. Since each point of S is defined over K, the line M must be defined over K. Since $S \subseteq U(K)$ and U contains no line, we get a contradiction. Hence A is the unique element of $|\mathcal{O}_Q(1,1)|$ containing $S \cup E$. Since $S \cup E$ is defined over K, A is defined over K. Since $\sharp(S) \geq 2$ and U contains no line defined over K, as above we get that A is geometrically irreducible. Hence A is a smooth hyperplane section of U defined over K. This completes the proof.

5. On a quadric cone

Let $T \subset \mathbb{P}^3$ be a quadric cone defined over K and $O \in T(K)$ its vertex. We will look at integral curves $Y \subset T$ defined over K and to their normalizations, C. Set $c := \lfloor \deg(Y)/2 \rfloor$. In the statement of Theorem 1.4 we take Y smooth and $a = c$. We assume that Y is not a line, i.e. we assume $a > 0$. We will always assume that either $O \notin Y$ or that Y is smooth at O. We use the following classical fact: if $O \notin Y$, then $\deg(Y)$ is even and Y is the complete intersection of T and a surface of degree $\deg(Y)/2$, while if O is a smooth point of Y, then $\deg(Y)$ is odd and Y has very strong cohomological properties (see Lemmas 5.3, 5.4 and 5.5). An excellent source for the geometry of T is [4], V.2.11.4 and Ex. V.2.9. Unfortunately, in the case in which Y is singular we cannot quote [4], Ex. V.2.9, but need to use the following set-up implicit in its proof.

Let $\alpha : \widetilde{\mathbb{P}}^3 \to \mathbb{P}^3$ be the blowing-up of O. Since $O \in \mathbb{P}^3(K)$, $\widetilde{\mathbb{P}}^3$ and α are defined over K. Let $T_2 \subset \widetilde{\mathbb{P}}^3$ be the closure of $\alpha^{-1}(T \setminus \{O\})$ in $\widetilde{\mathbb{P}}^3$. Set $u := \alpha|T_2$. T_2 is a geometrically integral smooth surface defined over K and u is defined over K. Set $h := \alpha^{-1}(O)$. We have $h \cong \mathbb{P}^1$ over K. The surface T_2 is isomorphic over K to Hirzebruch surface F_2 ([4] §V.2) and hence it has a ruling $\pi : T_2 \to \mathbb{P}^1$ and each fiber of π is mapped isomorphically by u onto one of the lines of T. We call f any fiber of π seen as an effective divisor of T_2. The morphism $\pi|h : h \to \mathbb{P}^1$ is an isomorphism, i.e. h intersects transversally each fiber of π at exactly one point. We have $\mathrm{Pic}(T_2) \cong \mathbb{Z}^2$, h and f are free generators of $\mathrm{Pic}(T_2)$. We have $f^2 = 0$, $h \cdot f = 1$ and $h^2 = -2$ (in the set-up of [4], §V.2 , we have $e = 2$ and $H = h + 2f$). Let $Y \subset T$ be any geometrically integral curve defined over K. Let Y' be the closure of $u^{-1}(Y \setminus \{O\})$ inside T_2. Y' is a geometrically integral curve defined over

K and $u|Y' : Y' \to Y$ is a birational morphism, which is an isomorphism, except perhaps at the points of $Y' \cap h$. If $O \notin Y$, then $h \cap Y = \emptyset$ and hence $Y' \cong Y$ over K. If O is a smooth point of Y, then $\alpha|Y'$ is an isomorphism. Hence our standing assumptions imply $Y' \cong Y$. In particular if Y is smooth, then $Y' \cong Y$ over K. We recall that the morphism u is induced by the complete linear system $|\mathcal{O}_{T_2}(h+2f)|$, that u send isomorphically $T_2 \setminus h$ onto $T \setminus \{O\}$. Let a, b be the only integers such that $Y' \in |\mathcal{O}_{T_2}(ah+bf)|$.

Remark 5.1. Since T is a surface of $\mathbb{P}^3$, for each integer t the restriction map $\rho_t : H^0(\mathbb{P}^3, \mathcal{O}_{\mathbb{P}^3}(t)) \to H^0(T, \mathcal{O}_T(t))$ is surjective. Since $\mathrm{Ker}(\rho_t) \cong H^0(\mathbb{P}^3, \mathcal{O}_{\mathbb{P}^3}(t-2))$, we get $h^0(T, \mathcal{O}_T(t)) = \binom{t+3}{3} - \binom{t+1}{3}$ for all $t \in \mathbb{N}$.

Remark 5.2. Fix integers $y > 0$ and $x \geq 2y$. We have $h^1(T_2, \mathcal{O}_{T_2}(yh+wf)) = 0$ if and only if $w \geq 2y-1$ ([4], Lemma V.2.4, and the cohomology of line bundles on $\mathbb{P}^1$ as in [4], p. 380). We recall the existence of an integral $A \in |\mathcal{O}_{T_2}(yh+xf)|$ ([4], Corollary V.2.18) and that $h^0(T_2, \mathcal{O}_{T_2}(yh+xf) = \sum_{i=0}^{y}(x-2i+1) =$ ([4], Lemma V.2.4). In particular we have $h^0(T_2, \mathcal{O}_Y(yh+(2y)f)) = (y+1)^2$, i.e. every section of $\mathcal{O}_{T_2}(yh+(2y)f)$ is the pull-back of a section of $\mathcal{O}_{T_2}(y)$. For all $(x, y) \in \mathbb{N}^2$ we have $h^0(T_2, \mathcal{O}_{T_2}(yh+xf)) = \sum_{i=0}^{y}(x+1-2i)$. In particular we have $h^0(T_2, \mathcal{O}_{T_2}(th+2tf)) = (t+1)^2$ and $h^0(T_2, \mathcal{O}_{T_2}(th+(2t+1)f)) = (t+1)(t+2)$ for all $t \geq 0$.

Lemma 5.3. *If $O \notin Y$, then $a = c$ and $b = 2c$. If $O \in Y$ and Y is smooth at O, then $a = c$ and $b = 2c+1$.*

Proof. Since $u^*(\mathcal{O}_T(1)) \cong \mathcal{O}_{T_2}(h+2f)$, we have $\deg(Y) = \mathcal{O}_{T_2}(ah+bf) \cdot \mathcal{O}_{T_2}(h+2f) = b$. The integer $\mathcal{O}_{T_2}(h) \cdot \mathcal{O}_{T_2}(ah+bf) = b-2a$ measures the multiplicity of Y at O. Hence this integer is 0 if $O \notin Y$, while it is 1 if O is a smooth point of Y. Hence $a = c$ and $b = 2c$ if $O \notin T$, while $a = c$ and $b = 2c+1$ if O is a smooth point of Y. This completes the proof.

Lemma 5.4. *Assume $O \notin Y$. Then $\deg(Y) = 2c$ is even, $Y' \cong Y$, Y is the complete intersection of T and a surface of degree c, $Y' \in |\mathcal{O}_{T_2}(ch+2cf)|$, $p_a(Y) = p_a(Y')$. For each integer t such that $1 \leq t < c$ we have $h^0(Y, \mathcal{O}_Y(t)) = (t+1)^2$ and $h^1(Y, \mathcal{O}_Y(t)) = (c-1-t)^2$. For each integer $t \geq c$ we have $h^0(Y, \mathcal{O}_Y(t)) = (t+1)^2 - (t-c+1)^2$ and $h^1(Y, \mathcal{O}_Y(t)) = 0$.*

Proof. Lemma 5.3 gives $\deg(Y) = 2c$ and $Y' \cong Y$. This isomorphism sends $\mathcal{O}_Y(t)$ isomorphically onto $\mathcal{O}_{Y'}(th+(2t)f)$. Remark 5.2 gives that Y is the complete intersection of T_2 and a degree c surface. The cohomological properties of complete intersection curves (even the non-smooth ones. We have $\omega_Y \cong \mathcal{O}_Y(c-2)$. Hence $h^i(Y, \mathcal{O}_Y(t)) = h^{1-i}(Y, \mathcal{O}_Y(c-2-t))$ for all $i \in \{0,1\}$ and $t \in \mathbb{Z}$ by duality. Since $h^1(T, \mathcal{O}_T(x)) = 0$ for all $x \in \mathbb{Z}$, the exact sequence of sheaves on T:

$$0 \to \mathcal{O}_T(t-c) \to \mathcal{O}_T(t) \to \mathcal{O}_Y(t) \to 0 \tag{3}$$

gives $h^0(Y, \mathcal{O}_Y(t)) = 0$ if $t < 0$, $h^0(Y, \mathcal{O}_Y(t)) = (t+1)^2$ if $0 \le t < c$ and $h^0(Y, \mathcal{O}_Y(t)) = (t+1)^2 - (t+1-c)^2$ for all $t \ge c$. This completes the proof.

Lemma 5.5. *Assume $O \in Y$ and Y smooth at O. Then $\deg(Y) = 2c+1$, $p_a(Y') = p_a(Y) = c^2 - c$ and Y is arithmetically Cohen-Macaulay. Take any line $L \subset T$. Then $Y \cup L$ is the complete intersection of T and a surface of degree $(c+1)/2$. We have $Y' \in |\mathcal{O}_{T_2}(ch + (2c+1)f)|$. Since $\omega_{T_2} \cong \mathcal{O}_{T_2}(-2h-4f)$, the adjunction formula gives $\omega_{Y'} \cong \mathcal{O}_{Y'}((c-2)h+(2c-3f))$. Hence $2p_a(Y')-2 = \deg(\omega_{Y'}) = (ch+(2c+1)f)\cdot((c-2)h+(2c-3)f)) = -2c(c-2)+(2c+1)(c-2)+c(2c-3) = 2c^2-2c-2$. Hence $p_a(Y) = p_a(Y') = c^2-c$. If $0 \le t < c$, then $h^0(Y, \mathcal{O}_Y(t))$. If $0 \le t < c$, then $h^0(Y', \mathcal{O}_{Y'}(th+2tf)) = (t+1)^2$. If $t \ge c$, then $h^0(Y', \mathcal{O}_{Y'}(th+2tf)) = (t+1)^2 - (t-c)(t-c+1)$.*

Proof. We have $Y' \in |\mathcal{O}_{T_2}(ch + (2c+1)f)|$. Since $\omega_{T_2} \cong \mathcal{O}_{T_2}(-2h-4f)$, the adjunction formula gives $\omega_{Y'} \cong \mathcal{O}_{Y'}((c-2)h + (2c-3f))$. Hence $2p_a(Y') - 2 = \deg(\omega_{Y'}) = \mathcal{O}_{T_2}(ch + (2c+1)f) \cdot \mathcal{O}_{T_2}((c-2)h+(2c-3)f)) = -2c(c-2)+(2c+1)(c-2)+c(2c-3) = 2c^2-2c-2$. Hence $p_a(Y) = p_a(Y') = c^2-c$. Take $F \in |f|$ such that $u(F) = L$. We have $Y' \cup (F \cup h) \in |\mathcal{O}_{T_2}((c+1)h+(2c+2)f)|$. Since $u^* : H^0(T, \mathcal{O}_T((c+1))) \to H^0(T_2, \mathcal{O}_{T_2}((c+1)h+(2c+2)f))$ is an isomorphism (case $u = c+1$ of Remark 5.2) we get that $Y \cup L$ is a complete intersection of T and a degree $c+1$ surface. Recall that a curve (even not integral) $D \subset \mathbb{P}^3$ is said to be arithmetically Cohen-Macaulay if for all integers $t \ge 0$ the restriction map $H^0(D, \mathcal{O}_D(t))$ is surjective. Any line is arithmetically Cohen-Macaulay. Since L is arithmetically Cohen-Macaulay and the scheme $Y' \cup L$ is a complete intersection, Y is arithmetically Cohen-Macaulay ([3], part (b) of Theorem 21.23, [9], Theorem A.9.1).

Hence for all integers $t \geq 0$ the restriction map $H^0(T, \mathcal{O}_T(t)) \to H^0(Y, \mathcal{O}_Y(t))$ is surjective. Since $Y' \cong Y$ and $u^* : H^0(T, \mathcal{O}_T(t)) \to H^0(T_2, \mathcal{O}_{T_2}(th + 2tf))$ is surjective, we get the surjectivity of the restriction map $H^0(T_2, \mathcal{O}_{T_2}(th+2tf)) \to H^0(Y', \mathcal{O}_{Y'}(th+2tf))$. Since $Y' \in |\mathcal{O}_{T_2}(ch + (2c+1)f))|$, for all $y, x \in \mathbb{Z}$ we have an exact sequence

$$0 \to \mathcal{O}_{T_2}((y-c)h + (x-2c-1)f) \to \mathcal{O}_{T_2}(yh+xf) \to \mathcal{O}_{Y'}(yh+xf) \to$$

Hence $h^0(Y', \mathcal{O}_{Y'}(th+2tf)) = h^0(T_2, \mathcal{O}_{T_2}(th+2tf)) - h^0(T_2, \mathcal{O}_{T_2}((t-c)f + (t-2c-1)f))$ for all t. If $t < 0$, then we get $h^0(Y', \mathcal{O}_{Y'}(th+2tf)) = 0$. If $0 \leq t < c$, then we get $h^0(Y', \mathcal{O}_{Y'}(th+2tf)) = (t+1)^2$. Now assume $t \geq c$. Since $\mathcal{O}_{T_2}(h) \cdot \mathcal{O}_{T_2}((t-c)f + (t-2c-1)) = -2(t-c) + t - 2c - 1 = -1 < 0$, h is in the base locus of the linear system $|\mathcal{O}_{T_2}((t-c)h + (t-2c-1)f)|$. Hence $h^0(T_2, \mathcal{O}_{T_2}((t-c)f + (t-2c-1)f)) = h^0(T_2, \mathcal{O}_{T_2}((t-c-1)f + (t-2c-1)f))$. Hence $h^0(Y', \mathcal{O}_{Y'}(th+2tf)) = (t+1)^2 - (t-c)(t-c+1)$ for all $t \geq c$. This complete the proof.

Proof of Theorem 1.4. Since C is arithmetically Cohen-Macaulay (Lemma 5.5), we have $h^1(\mathbb{P}^3, \mathcal{I}_C(y)) = 0$. We computed the integer $h^0(C, \mathcal{O}_C(y))$ in lemmas **??** and **??**. Since $\deg(E) \leq y+1$, we have $h^1(\mathbb{P}^3, \mathcal{I}_E(y)) = 0$ ([1], Lemma 34). Hence E gives $\deg(E)$ independent conditions to $H^0(\mathbb{P}^3, \mathcal{O}_{\mathbb{P}^3}(y))$. Since $E \subset C \subset \mathbb{P}^3$, E imposes $\deg(E)$ independent conditions to $h^0(C, \mathcal{O}_C(y))$. Hence in all cases we have $h^0(C, \mathcal{O}_C(y)(-E)) = h^0(C, \mathcal{O}_C(y)) - \deg(E)$. Since $\sharp(B) > \deg(C) \cdot y - \deg(E) = \deg(\mathcal{O}_C(y)(-E))$, no non-zero section of $\mathcal{O}_C(y)(-E)$ vanishes at all points of B. Hence $\mathcal{C}$ is an $[n,k]$ code. Assume that $\mathcal{C}^\perp$ and take a codeword $\mathbf{w}$ of $\mathcal{C}^\perp$ with minimal weight. Let S be the support of $\mathbf{w}$. Since $\mathcal{C}^\perp$ is linear and $\mathbf{w}$ has minimum weight, all non-zero codewords of $\mathcal{C}^\perp$ with support contained in S are of the form $\lambda \mathbf{w}$ for some $\lambda \in K \setminus \{0\}$. Lemma 2.1 gives $h^1(\mathbb{P}^3, \mathcal{I}_{E \cup S}(y)) > 0$. Since $\deg(E \cup S) \leq 2y+1$, there is a line $L \subset \mathbb{P}^3$ such that $\deg(L \cap (E \cup S)) \geq y+2$. Since $E \cup S \subset C \subset T$ and $y+2 > \deg(T)$, Bezout theorem gives $L \subset T$. Hence $L \in \mathcal{S}$. Fix any $J \in \mathcal{S}$ and take $S \subseteq B \cap J$ such that $\deg((E \cup S) \cap J) = y+2$. Lemma 2.1 gives the existence of a non-zero codeword $\mathbf{v}$ of $\mathcal{C}^\perp$ whose support is contained in S. Fix any $S' \subsetneq S$. Since $\deg((E \cup S) \cap J) = y+2 > \deg(E)$, we have $\deg((E \cup S') \cap J) \leq y+1$. Hence $h^1(\mathbb{P}^3, \mathcal{I}_{(E \cup S') \cap J)}(y)) = 0$.

Claim: $h^1(\mathbb{P}^3, \mathcal{I}_{E\cup S'}(y)) = 0$.

Proof of the Claim: Assume $h^1(\mathbb{P}^3, \mathcal{I}_{E\cup S'}(y)) > 0$. Let $H \subset \mathbb{P}^3$ be any plane containing J. Since $S' \subset J \subset H$ is a finite set, we have $\mathrm{Res}_H(E \cup S') = \mathrm{Res}_H(E) \subseteq E$. Since $\deg(\mathrm{Res}_H(E) \le \deg(E) \le y$, we have $h^1(\mathbb{P}^3, \mathcal{I}_{\mathrm{Res}_{H(E)}}(y-1)) = 0$. Hence (2) gives $h^1(H, \mathcal{I}_{H\cap(E\cup S'),H}(y)) > 0$. See J as an effective divisor of H and set $E' := \mathrm{Res}_J(H \cap E)$. Since $S' \subset J$, the exact sequence (2) gives the following exact sequence on $H \cong \mathbb{P}^2$:

$$0 \to \mathcal{I}_{E'}(y-1) \to \mathcal{I}_{(E\cup S',H}(y) \to \mathcal{I}_{(E\cup S')\cap J,J}(y) \to 0 \tag{4}$$

Since $\deg(E') \le \deg(E) \le y$, we have $h^1(H, \mathcal{I}_{E'}(y-1)) = 0$ ([1], Lemma 34). Since $J \cong \mathbb{P}1$ and $\deg((E \cup S') \cap J) \le y+1$, we have $h^1(J, \mathcal{I}_{(E\cup S')\cap J,J}(y)) = 0$. Hence (4) gives $h^1(H, \mathcal{I}_{H\cap(E\cup S'),H}(y)) = 0$, absurd. The contradiction proves the Claim.

By the Claim and Lemma 2.1 S' is not the support of a non-zero codeword of $\mathcal{C}^{\perp}$. Hence S is the support of $\mathbf{v}$. This completes the proof.

References

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

[2] A. Couvreur, The dual minimum distance of arbitrary dimensional algebraic-geometric codes. arXiv:0905.2345v3, *J. Algebra* (to appear).

[3] D. Eisenbud, Commutative Algebra, *Springer*, Berlin, 1995.

[4] R. Hatshorne, Algebraic Geometry, *Springer-Verlag*, Berlin, 1977.

[5] J. W. P. Hirschfeld, Projective geometries over finite fields, *Clarendon Press*, Oxford, 1979.

[6] J. W. P. Hirschfeld and J. A. Thas, General Galois Geometries, Clarendon Press, Oxford, 1991.

[7] 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.

[8] H. Stichtenoth, Algebraic Function Fields and Codes, *Springer*, Berlin, 1993.

[9] W. V. Vasconcelos, Computational methods in commutative algebra and algebraic geometry. With chapters by D. Eisenbud, D. R. Grayson, J. Herzog and M. Stillman. Algorithms and Computation in Mathematics, 2. *Springer-Verlag*, Berlin, 1998.

[10] J. H. van Lint, G. van der Geer, Introduction to coding theory and algebraic geometry. DMV Seminar, 12. *Birkhäuser Verlag*, Basel, 1988