Noname manuscript No.
(will be inserted by the editor)

On the weights of dual codes arising from the GK curve

Edoardo Ballico · Matteo Bonini

Abstract In this paper we investigate some dual algebraic-geometric codes associated with the Giulietti-Korchmáros maximal curve. We compute the minimum distance and the minimum weight codewords of such codes and we investigate the generalized Hamming weights of such codes.
Keywords: Giulietti-Korchmáros curve - algebraic-geometric codes - weight distribution
MSC Codes: 14G50 - 11T71 - 94B27

1 Introduction

Let $\mathcal{X}$ be an algebraic curve defined over the finite field $\mathbb{F}_q$ of order q. We recall that a curve $\mathcal{X}$ is called $\mathbb{F}_q$-maximal if its number of rational points over $\mathbb{F}_q$ attains the Hasse-Weil upper bound

$$|\mathcal{X}(\mathbb{F}_q)| = q + 1 + 2g(\mathcal{X})q^{1/2},$$

where $g(\mathcal{X})$ is the genus of $\mathcal{X}$.

Since codes with good parameters can be constructed from these curves, many authors studied their properties, see [8, 9, 15, 16, 18, 22, 23]. Most of the known examples have been shown to be subcovers of the Hermitian curve $\mathcal{H}$, which is the celebrated curve defined over $\mathbb{F}_{q^2}$ by the equation $Y^{q+1} = X^q + X$. This led to the question whether every maximal curve is a subcover of the Hermitian curve or not. This question has a negative answer: in [14], Giulietti and Korchmáros introduced an infinite family of curves $\mathcal{C}'$, the so called

Edoardo Ballico
Università di Trento, 38123 Povo (TN), Italy
E-mail: edoardo.ballico@unitn.it

Matteo Bonini
Università di Trento, 38123 Povo (TN), Italy
E-mail: matteo.bonini@unitn.it

GK curve(that we will denote with $\mathcal{GK}$), which is maximal over $\mathbb{F}_{q^6}$ and it is not covered by the Hermitian curve.

Codes from the $\mathcal{GK}$ have been widely investigated, see for example [7, 8, 10, 12].

One of the most interesting pattern of a linear code is its weight distribution, which is fundamental for the computation of its probability of undetectable error.

Unfortunately, the weight distribution of a given code is a very hard problem. Even the problem of computing the set of codewords of minimum weight can be a difficult task, apart from specific cases. In [7], the authors followed the approach of [11] to compute the number of minimum weight codewords of certain dual AG codes arising from $\mathcal{GK}$. For this purpose, they provided a useful algebraic-geometric description for codewords with a given weight which belong to a fixed affine-variety code. These techniques have been widely used in literature, see for example [1–4].

Another important pattern in a code are the so called generalized hamming weights, see [6, 13, 20, 25–27] for more information.

In this paper we investigate a class of codes arising from $\mathcal{GK}$ which is larger w.r.t. the one investigated in [7], giving tools to compute the number of minimum weight codewords of such codes, and the generalized Hamming weights of some codes arising from $\mathcal{GK}$, using the results introduced in [3].

2 Preliminaries

For a complete introduction to AG codes, we refer to [24].

Fix a field $K \subseteq \overline{\mathbb{F}}_q$. For any positive integer d we will denote with $H^0(\mathcal{O}_{\mathbb{P}^n}(d))$ the K-vector space of all degree d homogeneous polynomials in $n+1$ variables over the field K. Note that $\dim H^0(\mathcal{O}_{\mathbb{P}^n}(d)) = \binom{n+d}{n}$. Let $Z \subset \mathbb{P}^n(\overline{F}_q)$ be a zero-dimensional scheme defined over K. Let $H^0(\mathcal{I}_Z(d))$ denote the set of all $f \in H^0(\mathcal{O}_{\mathbb{P}^n}(d))$ vanishing on Z, then $H^0(\mathcal{I}_Z(d))$ is a K-vector space and

$$\max\{0, \binom{n+d}{n} - \deg(Z) \leq \dim H^0(\mathcal{I}_Z(d)) \leq \binom{n+d}{n}\}.$$

Set $h^1(\mathcal{I}_Z(d)) := H^0(\mathcal{I}_Z(d)) + \deg(Z) - \binom{n+d}{n}$.

Let $C \subset \mathbb{P}^n$ be a smooth projective curve defined over $\mathbb{F}_q$. Let $E \subset C(\overline{F}_q)$ be a zero-dimensional scheme defined over $\mathbb{F}_q$. For any integer d let $H^0(C, \mathcal{O}_C(d)(-E))$ denote the $\mathbb{F}_q$-vector space obtained restricting the elements of $H^0(\mathcal{I}_E(d))$ to C.

We recall the following results (see [3, Theorem 1]).

Lemma 1 *Fix integers $r \geq 2$, $m > 0$ and $e > 0$. Let $Z \subset \mathbb{P}^r$ be a zero-dimensional scheme such that $\deg(Z) \leq 3m + r - 3$. If $r \geq 3$ assume that Z spans $\mathbb{P}^r$. We have $h^1(\mathcal{I}_Z(m)) \geq e$ if and only if there is $W \subseteq Z$ occurring in this list:*

(a) $\deg(W) = m + 1 + e$ *and W is contained in a line;*
(b) $\deg(W) = 2m + 1 + e$ *and W is contained in a reduced plane conic;*

(c) $r \geq 3$, $e \geq 2$, *and there are an integer* $f \in \{1, \dots, e-1\}$ *and lines* L_1, L_2, *such that* $L_1 \cap L_2 = \emptyset$, $\deg(L_1 \cap Z) = m+1+f$ *and* $\deg(L_2 \cap Z) = m+1+e-f$.

Let $E \subset \mathbb{P}^3$ be a zero-dimensional scheme. E is said to be a complete intersection of a degree s curve $C \subset \mathbb{P}^3$ and a surface a degree s surface $\mathcal{Y}$ if it it is the zero locus of all polynomials defining C and a degree s polynomial (unique up to a non-zero scalar multiple) defining $\mathcal{Y}$. In this case $\deg(E) = st$.

Lemma 2 *Let* $\mathbb{F}$ *be any field and let* $\mathbb{P}^n$ *denote the projective space of dimension* n *on* $\mathbb{F}$. *Let* $C \subseteq \mathbb{P}^r$ *be a smooth plane curve which is a complete intersection. Fix an integer* $d > 0$, *a zero-dimensional scheme* $E \subseteq C$ *and a finite subset* $B \subseteq C$ *such that* $B \cap E_{red} = \emptyset$[1]. *Denote by* $\mathcal{C}$ *the code obtained evaluating the vector space* $H^0(C, \mathcal{O}_C(d)(-E))$ *at the points of* B. *Set* $c = \deg(C)$, $n = |B|$ *and assume* $|B| > dc - \deg(E)$. *The following facts hold.*

1. *The code* $\mathcal{C}^\perp$ *has length* n *and dimension* $k = h^0(C, \mathcal{O}_C(d)) - \deg(E) + h^1(\mathbb{P}^n, \mathcal{I}_E(d))$.
2. *The minimum distance of* $\mathcal{C}^\perp$ *is the minimal cardinality, say* z, *of a subset of* $S \subseteq B$ *such that*
$$h^1(\mathbb{P}^n, \mathcal{I}_{S \cup E}(d)) > h^1(\mathbb{P}^n, \mathcal{I}_E(d)).$$
3. *A codeword of* $\mathcal{C}^\perp$ *has weight* z *if and only if it is supported by a subset* $S \subseteq B$ *such that*
   (a) $|S| = z$,
   (b) $h^1(\mathbb{P}^n, \mathcal{I}_{E \cup S}(d)) > h^1(\mathbb{P}^n, \mathcal{I}_E(d))$,
   (c) $h^1(\mathbb{P}^n, \mathcal{I}_{E \cup S}(d)) > h^1(\mathbb{P}^n, \mathcal{I}_{E \cup S'}(d))$ *for any* $S' \subsetneq S$.

A zero-dimensional subscheme Z of a smooth projective curve $\mathcal{Y}$ is just an effective divisor of $\mathcal{Y}$, i.e. a finite set $S \subset \mathcal{X}(\overline{\mathbb{F}}_q)$ in which each $o \in S$ has attached a positive integer m_o, its multiplicity. Set $\deg(Z) := \sum_{o \in S} m_o$. Note that Z is defined over a finite extension $\mathbb{F}_{q^e}$ of $\mathbb{F}_q$, the minimal extension of $\mathbb{F}_q$ containing for which each point of S is defined over $\mathbb{F}_{q^e}$. Let $F_q : \mathbb{F}_{q^e} \to \mathbb{F}_{q^e}$ denote the ?Frobenius map? We say that Z is defined over $\mathbb{F}_q$ if $F_q(o) \in S$ and $m_{F_q(o)} = m_o$ for all $o \in S$. Assume that Z is defined over $\mathbb{F}_q$. If $\mathcal{Y}$ has an embedding j defined over $\mathbb{F}_q$, then $j(Z)$ is embedded in $\mathbb{P}^n(\overline{\mathbb{F}}_q)$ and it is a degree $\deg(Z)$ zero-dimensional subscheme of $\mathbb{P}^n(\overline{\mathbb{F}}_q)$ defined over $\mathbb{F}_q$. More in general, a zero-dimensional subscheme of $\mathbb{P}^n(\overline{\mathbb{F}}_q)$ defined over $\mathbb{F}_q$ is the zero-locus (inside all $\mathbb{P}^n(\overline{\mathbb{F}}_q)$) of finitely many homogeneous polynomials with $\mathbb{F}_q$-coefficients, with the only restriction that the set-theoretic zero-locus inside $\mathbb{P}^n(\overline{\mathbb{F}}_q)$ is finite.

A zero-dimensional scheme $Z \subset \mathbb{P}^r$ is said to be *curvilinear* if at each $P \in Z_{red}$ the Zariski tangent space of Z has dimension ≤ 1. Each zero-dimensional scheme Z contained in a smooth curve is curvilinear, vice-versa each curvilinear zero-dimensional scheme is contained in a smooth curve. In this note we point out the following partial extension of [1], Theorem 1, to the case of non-reduced, but curvilinear subschemes.

We recall the following results ([4, Theorem 1]).

Theorem 1 *Fix an integer* $m \geq 3$. *Let* $Z \subset \mathbb{P}^r$, $r \geq 3$, *be a curvilinear zero-dimensional scheme spanning* $\mathbb{P}^r$. *If* $r = 3$, *then assume* $\deg(Z) < 3m$. *If* $r \geq 4$, *then assume* $\deg(Z) \leq 4m + r - 5$ *and* $\deg(Z \cap M) < 3m$ *for all* 3*-dimensional linear subspaces* $M \subset \mathbb{P}^r$. *We have* $h^1(\mathcal{I}_Z(m)) > 0$ *if and only if either there is a line* D *with* $\deg(D \cap Z) \geq m+2$ *or there is a conic* D' *with* $\deg(D' \cap Z) \geq 2m+2$.

[1] Here E_{red} denotes the reduction of the scheme E.

With minimal modifications of the proof of [1] we get the following result

Lemma 3 *Let $Y \subset \mathbb{P}^3$ be a smooth and connected projective curve defined over an algebraically closed field. Fix a zero-dimensional scheme $A \subset Y$ and a finite set $B \subset Y$ such that $A \cap B = \emptyset$. Set $Z := A \cup B$. Assume $\deg(A) < 3m$, $\deg(Z) \leq 4m+2$ and $\deg(Z \cap H) \leq 4m-5$ for each plane $H \subseteq \mathbb{P}^r$ We have $h^1(\mathcal{I}_Z(m)) > 0$ if and only if there is $W \subseteq Z$ as in one of the following cases:*

(a) $\deg(W) = m+2$ *and W is contained in a line;*
(b) $\deg(W) = 2m+2$ *and W is contained in a plane conic;*
(c) $\deg(W) = 3m$ *and W is the complete intersection of a degree 3 plane curve and a degree m surface;*
(d) $\deg(W) \geq 3m+1$ *and W is contained in a degree 3 plane curve;*
(e) $\deg(W) = 3m+2$ *and W is contained in a reduced and connected degree 3 curve spanning $\mathbb{P}^3$.*

3 GK curve

Denote by $\mathrm{PG}(3, q^6)$ the three dimensional projective space over the field $\mathbb{F}_{q^6}$ with q^6 element. The Giulietti-Korchmáros curve $\mathcal{GK}$ is a non-singular curve in $\mathrm{PG}(3, q^6)$ defined by the affine equations

$$\begin{cases} Z^{q^2-q+1} = Y^{q^2} - Y \\ Y^{q+1} = X^q + X \end{cases} . \tag{1}$$

Arbitrary complete intersections in $\mathbb{P}^r$ are defined and studied in [19, Ex. II.8.4 and III.5.5]. We always consider the case of smooth space curves, complete intersection of a surface S of degree a and a surface of degree $b \geq a$ (on the GK curve $a = q+1$ and $b = q^2$). We have $h^1(\mathbb{P}^3, \mathcal{I}_C(t)) = 0$ for all $t \in \mathbb{Z}$ and hence (for a smooth curve and any zero-dimensional scheme $Z \subset C$) we have $h^1(C, \mathcal{O}_C(t)(-Z)) = h^1(\mathcal{O}_C(t)) + h^1(\mathbb{P}^3, \mathcal{I}_Z(t))$. We have the exact sequences

$$0 \to \mathcal{O}_{\mathbb{P}^3}(t-a) \to \mathcal{O}_{\mathbb{P}^3}(t) \to \mathcal{O}_S(t) \to 0 \tag{2}$$

$$0 \to \mathcal{O}_S(t-b) \to \mathcal{O}_S(t) \to \mathcal{O}_C(t) \to 0 \tag{3}$$

We have $h^0(\mathcal{O}_{\mathbb{P}^3}(t)) = \binom{t+3}{3}$ for all $t \geq 0$. From (2) and (3) we get $h^0(\mathcal{O}_C(t)) = \binom{t+3}{3}$ for all $t < a$ and $h^0(\mathcal{O}_C(t)) = \binom{t+3}{3} - \binom{t-a+3}{3}$ if $a \leq t < b$ (see below the proof of the case $t \geq b$). From (2) and the fact that $h^i(\mathcal{O}_{\mathbb{P}^3}(x)) = 0$ for $i = 1, 2$ and all $x \in \mathbb{Z}$ we get $h^1(\mathcal{O}_S(x)) = 0$ for all $x \in \mathbb{Z}$ and $h^0(\mathcal{O}_C(t)) = h^0(\mathcal{O}_S(t))$ if $t < b$ and $h^0(\mathcal{O}_C(t)) = h^0(\mathcal{O}_S(t)) - h^0(\mathcal{O}_S(t-b))$ for all $t \geq b$. Thus, for all $t \geq b$, $h^0(\mathcal{O}_C(t)) = \binom{t+3}{3} - \binom{t-a+3}{3} + \binom{t-b}{3} - \epsilon$, where $\epsilon = 0$ if $t < b+a$ and $\epsilon = \binom{t-b-a}{3}$ if $t \geq b+a$.

Proposition 1 *Let L be a tangent to $\mathcal{GK}$ at a point P. Then $I(L, \mathcal{GK}, P) = q^2-q+1$ or $I(L, \mathcal{GK}, P) = q+1$.*

Proof We know that the tangent to an affine point of this curve $P = (x_0, y_0, z_0)$ has equation

$$\begin{cases} (Y - y_0) + z_0^{q^2-q}(Z - z_0) = 0 \\ -(X - x_0) + y_0^q(Y - y_0) = 0 \end{cases}$$

The parametric equation of this line is, for $z_0 \neq 0$

$$\begin{cases} X = x_0 + y_0^q t - y_0^{q+1} \\ Y = t \\ Z = \frac{-t+y_0+z_0^{q^2-q+1}}{z_0^{q^2-q}} = \frac{t+y_0^{q^2}}{z_0^{q^2-q}} \end{cases}$$

while for $z_0 = 0$ it is

$$\begin{cases} X = x_0 \\ Y = y_0 \\ Z = t \end{cases}$$

and the solution corresponding to P is $t = y_0$ and $t = z_0$ respectively.

Suppose $z_0 \neq 0$.

Substituting the equation of the affine equation of $\mathcal{GK}$ gives us

$$\begin{cases} \left(\frac{-t+y_0^{q^2}}{z_0^{q^2-q}}\right)^{q^2-q+1} - t^{q^2} + t = 0 \\ -t^{q+1} + (x_0 + y_0^q t - y_0^{q+1})^q + x_0 + y_0^q t - y_0^{q+1} = 0 \end{cases} \tag{4}$$

The first equation becomes

$$\begin{aligned} 0 &= (-t + y_0^{q^2})^{q^2-q+1} - (t^{q^2} - t) z_0^{(q^2-q)(q^2-q+1)} \\ &= (y_0^{q^2} - t)^{q^2-q+1} - (t^{q^2} - t)(y_0^{q^2} - y_0)^{q^2-q} \end{aligned}$$

which has $t = y_0$ as a root, its derivative is

$$-(y_0^{q^2} - t)^{q^2-q} + (y_0^{q^2} - y_0)^{q^2-q} = (-(y_0^{q^2} - t)^{q-1} + (y_0^{q^2} - y_0)^{q-1})^q$$

and since $t = y_0$ is a root of $-(y_0^{q^2} - t)^{q-1} + (y_0^{q^2} - y_0)^{q-1}$ we have that $t = y_0$ is a root of (4) with multiplicity at least $q + 1$.

By direct computations the second equation becomes

$$\begin{aligned} 0 =& - t^{q+1} + x_0^q + y_0^{q^2} t^q - y_0^{q^2+q} + x_0 + y_0^q t - y_0^{q+1} = -t^{q+1} + y_0^{q^2} t^q - y_0^{q^2+q} + y_0^q t \\ =& t^q(-t + y_0^{q^2}) - y_0^q(-t + y_0^{q^2}) = (-t + y_0^{q^2})(t - y_0)^q \end{aligned}$$

and from this we get that $t = y_0$ is a root with multiplicity $q+1$ if $y_0 \in \mathbb{F}_{q^2}$ or q is $y_0 \notin \mathbb{F}_{q^2}$.

Now we deal with the remaining case $z_0 = 0$. Substituting the equation of the affine equation of $\mathcal{GK}$ gives us

$$\begin{cases} t^{q^2-q+1} = y_0^{q^2} - y_0 \\ y_0^{q+1} = x_0^q + x_0 \end{cases}$$

where the second is not an equation in t but just a compatibility condition. If this holds, we get that

$$t^{q^2-q+1} = 0$$

In this case the tangent in P is a q^2-q+1-secant.

The only point left to study is $P_\infty = (1:0:0:0)$. Recalling that the homogenized equations of $\mathcal{GK}$ are

$$\begin{cases} Z^{q^2-q+1}T^{q-1} = Y^{q^2} - YT^{q^2-1} \\ Y^{q+1} = X^qT + XT^q \end{cases}. \tag{5}$$

the equation of the tangent line will be then

$$\begin{cases} X = 1 \\ Y = 0 \end{cases}$$

and the intersection multiplicity at this point with the tangent is q^2-q+1.

4 Codes from $\mathcal{GK}$

We now recall results for intersections of algebraic curves of and $\mathcal{GK}$, and their link to the minimum distance of dual AG codes $C(D, G_m)^\perp$, where $G_m = m(q^3+1)P_\infty$, $P_\infty = (1:0:0:0)$, and $D = \sum_{P \in \mathcal{GK}(\mathbb{F}_{q^6}) \setminus \{P_\infty\}} P$, see [7] for a more detailed tractation.

Proposition 2 *Let $r \subset \mathrm{PG}(3, q^6)$ be a line. Then*

$$|r \cap \mathcal{GK}| \leq q^2 - q + 1.$$

Also, any (q^2-q+1)-secant is parallel to the z-axis and all the (q^2-q+1) common points are not $\mathbb{F}_{q^2}$-rational.

Proposition 3 *The total number of (q^2-q+1)-secants of the $\mathcal{GK}$ is $(q+1)(q^5-q^3)$.*

Remember that each point lies in exactly one of such secants.

Proposition 4 *Let $\mathcal{X}$ be a curve of degree $\alpha \leq q$ in $\mathrm{PG}(3, q^6)$. Then the size $|\mathcal{X} \cap \mathcal{GK}(\mathbb{F}_{q^6})|$ is at most*

$$\begin{cases} \alpha(q^2-q+1), & \text{if } \mathcal{X} \text{ is reducible,} \\ \alpha(q+1), & \text{if } \mathcal{X} \text{ is absolutely irreducible.} \end{cases}$$

Proposition 5 *Let $d^* \leq d$ be the designed Goppa minimum distance of $C(D, G_m)^\perp$, $m \geq 2$. Then*

1. *$d = m + 2$ when $m \leq q^2 - q - 1$;*
2. *$d = 2m + 2$ when $m = q^2 - q$;*
3. *$d = 3m$ when $m = q^2 - q + 1$;*
4. *$d \geq 3m + 1$ when $q^2 - q + 1 < m \leq q^2 - 1$;*
5. *$d \geq d^*$ when $m > q^2 - 1$.*

4.1 The family $\overline{C}_S$

Condider now a set $S \subset \mathcal{GK}(\mathbb{F}_{q^6})$ and the corresponding divisor

$$D_S = D - \sum_{P \in S} P$$

and call

$$S_1 = \{P \in S \,:\, P \in \mathcal{GK}(\mathbb{F}_{q^2})\}, \quad S_2 = S \setminus S_1.$$

The following result comes from a straightforward application of Proposition 3.

Proposition 6 *Let $q + 1 \leq m \leq 2(q + 1)$ and D_S defined as before. Consider the code $\overline{C}_S = C(D_S, (q^3 + 1)mP_\infty)^\perp$. If*

$$|S_2| < (q^2 - q + 1 - m)(q + 1)(q^5 - q)$$

then $\overline{C}_S$ is a $[n - |S|, \ell(D_S) - \ell(D_S - G_m), m + 2]_q$-code. Moreover, if $S = S_1$ then the number of minimum weight codewords of $\overline{C}_S$ is given by

$$A_{m+2}(\overline{C}_S) = (\ell + 1)(\ell^5 - \ell^3)(\ell^6 - 1)\binom{\ell^2 - \ell + 1}{m + 2}.$$

Proof Going through the proof of Proposition 5 and noticing that if $|S_2| < (q^2 - q + 1 - m)(q + 1)(q^5 - q)$ there is at least a $(m + 2)$-secant line the result holds.

Remark 1 Actually this bound can be improved depending on the composition of S_2.

If $m + 2$ points in S_2 are lie in the intersection between one line and $\mathcal{GK}$, then all the other ones can be be chosen at will. In this way, the minimum distance remains unchanged, while the dimension of the code decreases (and so, the obtained code improves its paramers).

Similar chooses adopted for the configuration of $2m + 2$ points on a (possibly reducible) conic, but this choice will give only provide variation to the codewords of the first non-minimum weight.

4.2 Three-point codes

Theorem 2 *Fix any three distinct points $P_1, P_2, P_3 \in \mathcal{GK}(\mathbb{F}_{q^6}) \setminus \{P_\infty\}$ and assume P_1, P_2 and P_3 to span $\mathbb{P}^2$ and be such that their connecting lines are not parallel to the z axis. Set $B := \mathcal{GK}(\mathbb{F}_{q^6}) \setminus \{P_1, P_2, P_3\}$. Fix an integer $d \geq 5$ such that $1 \leq d \leq q-1$ and integers $a_1, a_2, a_3 \in \{1, \dots, d\}$ such that $a_1 + a_2 + a_3 \leq 3d - 5$ and $a_i = d$ for at most one index $i \in \{1, 2, 3\}$. Set $E := a_1P_1 + a_2P_2 + a_3P_3$. Let $\mathcal{C} := \mathcal{C}(B, d, -E)$ be the code obtained evaluating the vector space $H^0(\mathcal{GK}, \mathcal{O}_{\mathcal{GK}}(d)(-E))$ on the set B. Then $\mathcal{C}$ is a code of length $n = |B| = q^8 - q^6 + q^5 - 2$ and dimension $k = \binom{d+3}{3} - a_1 - a_2 - a_3$. For any $i \in \{1, 2, 3\}$ let L_i denote the line spanned by P_j and P_h with $\{i, j, h\} = \{1, 2, 3\}$. Then $\mathcal{C}^\perp$ has minimum distance d and its minimum-weight codewords are exactly the ones whose support is formed by d points of $B \cap L_i$ for some $i \in \{1, 2, 3\}$.*

Proof The length of $\mathcal{C}$ is obviously $n = q^8 - q^6 + q^5 - 2$. From what we said previously we have $h^0(\mathcal{GK}, \mathcal{O}_{\mathcal{GK}}(d)) = \binom{d+3}{3}$. If, say, $a_1 \geq a_2 \geq a_3$, the assumptions $a_1 \leq d$ and $a_1 + a_2 + a_3 \leq 3d - 1$ give $a_i \leq d + 2 - i$ for all i. Hence our previous computations tell us that $h^1(\mathbb{P}^2, \mathcal{I}_E(d)) = 0$ and so $h^0(\mathcal{GK}, \mathcal{O}_{\mathcal{GK}}(d)(-E)) = \binom{d+3}{3} - a_1 - a_2 - a_3 = k$.

Since $|B| > d \cdot \deg(\mathcal{GK})$, there is not a non-zero element of $H^0(\mathcal{GK}, \mathcal{O}_{\mathcal{GK}}(d))$ vanishes at all the points of B. Hence $\mathcal{C}$ has dimension k. By Lemma 2 it is sufficient to prove the following two facts.

(a) $h^1(\mathbb{P}^3, \mathcal{I}_{E \cup A}(d)) = 0$ for all $A \subseteq B$ such that $|A| \leq d - 1$.
(b) For any $S \subseteq B$ such that $|S| = d$ we have $h^1(\mathbb{P}^3, \mathcal{I}_{E \cup S}(d)) > 0$ if and only if $S \subseteq L_i$ for some $i \in \{1, 2, 3\}$.

Each line L_i contains at most $q - 1$ points of B while $\deg(E \cap L_i) = 2$. Hence for any $S \subseteq L_i \cap B$ with $|S| = d$ we have $h^1(\mathbb{P}^2, \mathcal{I}_{E \cup S}(d)) > 0$ from Lemma 2.

Let $E_i := a_iP_i$, clearly $E = E_1 + E_2 + E_3$ (seen as a divisor).

Fix a set $S \subseteq B$ such that $|S| \leq d$ and assume $h^1(\mathbb{P}^3, \mathcal{I}_{E \cup S}(d)) > 0$. We have $S \cap \{P_1, P_2, P_3\} = \emptyset$ and $\deg(E \cup S) = a_1 + a_2 + a_3 + |S|$. Since $a_1 + a_2 + a_3 + |S| \leq 4d - 5$, we may apply Proposition 3 to the scheme $E \cup S$.

Let $T \subseteq \mathbb{P}^n$ be the curve arising from the three possible cases of Lemma 3. Set $x := \deg(T) \in \{1, 2, 3\}$ and $e_i := \deg(T \cap E_i)$ for $i \in \{1, 2, 3\}$. We have $0 \leq e_i \leq a_i$.

If $e_i \geq x + 1$ then we have that the tangent at P_i is $L_{\mathcal{GK},P_i} \subseteq T$. Assume $e_i \leq x$ for all $i \in \{1, 2, 3\}$. For $x = 2$ we get $\deg(T \cap (E \cup S)) \leq 2d + 1$. For $x = 3$ we get $\deg(T \cap (E \cup S)) \leq 3d - 1$. Finally, for $x = 1$ we may have $e_i > 0$ only for at most two indices, say $i = 1, 2$. Since $|S| \leq d$, we get $|S| + e_1 + e_2 \geq d + 2$ and $|S| + e_1 + e_2 = d + 2$ if and only if $T = L_3$, $S \subseteq L_3 \cap B$ and $|S| = d$.

Now assume that T contains one of the lines $L_{\mathcal{GK},P_i}$, say $L_{\mathcal{GK},P_1}$. Let T' be the curve whose equation is obtained dividing an equation of T by an equation of $L_{\mathcal{GK},P_1}$. We have $\deg(T') = x - 1$, $T' + L_{\mathcal{GK},P_1} = T$ (as divisors of $\mathbb{P}^2$) and $T = L_{\mathcal{GK},P_1} \cup T'$ (as sets). Since $L_{\mathcal{GK},P_1} \cap B = \emptyset$, we have $T \cap S = T' \cap S$ and $\deg(T \cap (E \cup S)) = \deg(T' \cap (E_2 \cup E_3 \cup S))$.

(i) If $x = 1$, we get $T \cap S = \emptyset$ and $\deg(T \cap E) = a_1 \leq d$, a contradiction.
(ii) Assume $x = 2$. The curve T' must be a line such that $\deg(T' \cap (E_2 \cup E_3 \cup S)) \geq 2d + 2 - a_1$. If either $T' = L_{\mathcal{GK},P_2}$, or $T' = L_{\mathcal{GK},P_3}$, we get $T' \cap S = \emptyset$ and $\deg(T' \cap (E_2 \cup E_3 \cup S)) \leq \max\{e_2, e_3\} \leq d$, a contradiction. If neither $T' = L_{\mathcal{GK},P_2}$, nor $T' = L_{\mathcal{GK},P_3}$, then $\deg(T' \cap E_2) \leq 1$, $\deg(T \cap E_3) \leq 1$ and

$\deg(T' \cap (E_2 \cup E_3)) = 2$ if and only if $T' = L_1$. Since $|S| \leq d$ we deduce $\deg(T \cap (E \cup S)) \leq a_1 + 2 + |S|$. Moreover, the equality holds if and only if $T' = L_1$ and $S \subseteq L_1$. Since $\deg(T \cap (E \cup S)) \geq 2d + 2$ by assumption, $|S| = d$ and $S \subseteq L_1$, as claimed.

(iii) Now assume $x = 3$. We get $\deg(T' \cap (E_2 \cup E_3 \cup S)) \geq 3d - a_1$ and T' is a conic. If neither $L_{\mathcal{GK},P_2}$, nor $L_{\mathcal{GK},P_3}$, is a component of T then $e_2 \leq 2$ and $e_3 \leq 2$ and so $|T' \cap S| \geq 3d - 4 - a_1 \geq 2d - 4 > d$. If, say, T' contains $L_{\mathcal{GK},P_2}$ and T'' is the line with $T' = T'' + L_{\mathcal{GK},P_2}$, then we get $|(S \cup E_3) \cap T''| \geq 3d - a_1 - a_2$. Since $a_1 + a_2 \leq 2d - 1$ we deduce $\deg(T'' \cap (E_3 \cup S)) \geq d + 1$. Since $\deg(T'' \cap E_3) \leq 1$, we get $a_1 + a_2 = 2d - 1$, say $a_1 = d$, $a_2 = d - 1$ and that S is formed by d points on a line T'' through P_3. If either $T'' = L_1$ or $T'' = L_3$, then we are done. In any case it is sufficient to prove that $E_1 \cup E_2 \cup \{P_3\} \cup S$ is not the complete intersection of $T = L_{\mathcal{GK},P_1} \cup L_{\mathcal{GK},P_2} \cup T''$ and a degree d curve, say C_d. Since $a_2 = d - 1$, E_2 is not the complete intersection of $L_{\mathcal{GK},P_2}$ and C_d, while $L_{\mathcal{GK},P_2} \cap (\{P_3\} \cup S) = \emptyset$, a contradiction.

Corollary 1 *Using the notation of the previous theorem, the number of minimum weight codewords of the code above is given by*

$$A_d(\mathcal{C}) = (q^6 - 1) \sum_{i=1}^{3} \binom{|L_i \cap \mathcal{GK}|}{d} \leq (q^6 - 1) 3 \binom{p+1}{d}.$$

where the binomial coefficient is meant to be zero if $d > |L_i \cap \mathcal{GK}|$ for some i.

Example 1 Let $q = 7$ and consider the affine equation of $\mathcal{GK}$ over the field $\mathbb{F}_{q^6}$

$$\begin{cases} Z^{43} = Y^{49} - Y \\ Y^8 = X^7 + X \end{cases}.$$

Consider $P_1 = (0 : 0 : 0 : 1)$, $P_2 = (1 : 3 : 0 : 1)$ and $P_3 = (1 : 4 : 0 : 1)$. The three points are in general position and their connecting line are not parallel to the Z axis, so the conditions of the previous theorem are satisfied. Moreover, by direct computation, the three lines L_1, L_2 and L_3 are 8-secants of $\mathcal{GK}$. Consider now $d = 6$ and $a_1 = 6$, $a_2 = a_3 = 3$ and call $\mathcal{C} = \mathcal{C}(B, 6, 6P_1 + 3P_2 + 3P_3)$. From Theorem 2 we have that the minimum distance of $\mathcal{C}$ is $d = 6$ and the minimum weight codewords are exactly

$$A_6(\mathcal{C}) = (7^6 - 1) 3 \binom{8}{6} = (7^6 - 1) 84$$

5 Generalized Hamming Weights of codes arising from the GK curve

Let $\mathbb{K} = \mathbb{F}_q$ a finite field with q elements. Let $C \subset \mathbb{K}^n$ be a linear $[n, k]$ code over $\mathbb{K}$. We recall that the *support* of C is defined as follows

$$supp(C) = \{i \mid c_i \neq 0 \text{ for some } c \in C\}.$$

So $|supp(C)|$ is the number of nonzero columns in a generator matrix for C. Moreover, for any $1 \leq v \leq k$, the *v-th generalized Hamming weight* of C

$$d_v(C) = \min\{|supp(\mathcal{D})| \mid \mathcal{D} \text{ is a linear subcode of } C \text{ with } dim(\mathcal{D}) = v\}.$$

In other words, for any integer $1 \leq v \leq k$, $d_v(C)$ is the v-th minimum support weights, i.e. the minimal integer t such that there are an $[n, v]$ subcode $\mathcal{D}$ of C and a subset $S \subset \{1, \dots, n\}$ such that $\sharp(S) = t$ and each codeword of $\mathcal{D}$ has zero coordinates outside S. The sequence $d_1(C), \dots, d_k(C)$ of generalized Hamming weights (also called *weight hierarchy* of C) is strictly increasing (see Theorem 7.10.1 of [21]). Note that $d_1(C)$ is the minimum distance of the code C.

Lemma 4 *Let S be the set of points that form the support of a codeword of $C^{\perp}$. Let $E \subseteq \mathcal{X}$ be a zero dimensional scheme defined over $\mathbb{K}$ and assume that there exists a surface $T \subset \mathbb{P}^3$ such that $h^1(\mathbb{P}^3, \mathcal{I}_{Res_T(E \cup S)}(d-k)) = 0$, where $k = \deg(T)$. Then $S \subset T$.*

Proof Let W (reps. W') be the subcode of $C^{\perp}$ formed by the codewords whose support is contained in S (resp. $S \cap T$). Clearly $W' \subseteq W$. From Proposition 1 we get $h^1(\mathbb{P}^3, \mathcal{I}_{E \cup S}(d)) = h^1(\mathbb{P}^3, \mathcal{I}_{T \cap (E \cup S)}(d))$. From this we obtain $W = W'$, which means that the thesis is proved.

Theorem 3 *Fix a positive integer $d \leq \deg(\mathcal{GK}) - 1$, a zero dimensional scheme $E \subseteq \mathcal{X}$ defined over $\mathbb{K}$ and a set $B \subseteq \mathcal{GK}(\mathbb{K}) \setminus E_{red}$ such that $\deg(E) \leq d+1$ and set $C := C(B, \mathcal{O}_{\mathcal{GK}(d)(-E)})$. Assuming that each line is such that $\deg(L \cap (E \cup B)) \leq d+1$ and that there exists a conic such that*

(i) $\deg(D \cap E) + |B \cap D| \geq 2d + 2$;
(ii) for each conic $\mathcal{C}$ such that $T \neq D$ we have $\deg(T \cap (E \cup B)) \leq 2d + 1$.

For any integer s such that $2d + 2 - \deg(D \cap E) \leq s \leq |B \cap D|$ and for each integer h with $1 \leq h \leq \min\{|B \cap D| - 2d - 2 + \deg(D \cap E), d - 2 - \deg(E)\}$, each h-dimensional linear subspace of $C^{\perp}$ computing $d_h(C^{\perp})$ is supported by some $S \subset \Sigma(2d+h-1+\deg(D \cap E))$ and each element of $\Sigma(d+h-1+\deg(D \cap E))$ is in the support of a h-dimensional linear subspace.

Proof Fix an integer $e \geq 1$ and any $S \subseteq B$. Lemma 2 tell us that S contains the support of an e-dimensional subspace of $C^{\perp}$ if and only if $h^1(\mathbb{P}^3, \mathcal{I}_{E \cup S}(d)) \geq e$. Fix $S \subseteq B$ such that it is the support of a codeword of $C^{\perp}$ with weight $\leq 3d+1-\deg(E)$, hence $\deg(E \cup S) \leq 3d-1$ and Lemma 1 tells us the value of $h^1(\mathbb{P}^2, \mathcal{I}_{E \cup S}(d))$. Let t be the minimal integer such that $h^1(\mathbb{P}^3, \mathcal{I}_{E \cup S}(d)) \geq 0$, clearly $t \leq d$. If $\deg(T \sup S) \leq 2d + 1$ then there is a line L with $\deg(L \cap (E \cup B)) \geq \deg(L \cap (E \cup S)) \geq d+2$, but this cannot happen since we excluded this possibility. For this reason we can assume that $\deg(E \cup S) \geq 2d + 2$. Since $d \geq 4$, we have that there is a line L such that $\deg(L \cap (E \cup S)) \geq d$ scheme-theoretic base locus of the set $|\mathcal{I}_D(2))|$ of all quadric surfaces containing D. Take any quadric $T \supset D$. Since $\deg(Res_T(E \cup B)) \leq 3d - 1 - (2d + 2) \leq d - 1$, we have $h^1(\mathbb{P}^3, \mathcal{I}_{Res_T(E \cup B)}(d-2)) = 0$. Thus Lemma 4 gives $E \cup B \subset T$. Since D is scheme-theoretically the base locus of $|\mathcal{I}_D(2))|$, we get $E \cup B \subset D$.

6 Conclusions and open problems

In this paper we have found out some results that, while not providing the explicit distribution of the weights (and generalized weights) of the code, help in their research.

Such results are by their nature quite similar to those obtained for the Hermitian curve (and also the Norm-Trace curve). This leads us to suppose that they can also be extended to other classes of algebraic curves, and the first one that comes to mind is the GGS curve (see [17]), which represents the first generalization of $\mathcal{GK}$.

As for the norm-trace curve, also the GSS curve has a model with a unique singular point, and this singular point is unibranch. Thus, the smooth model of the GSS curve may easily use multiple of this point to define one-point codes. For such codes lines, conics and cubic curves give, in certain ranges, lower bounds for the Hamming weights. It is the converse that we do not know (it was done for the Trace-Norm curve in [5], but only in a smaller range, than for instance for the Hermitian curve, where the plane model is smooth). For this reason, we set the following open problem.

Open Problem 4. *Say whether it is possible to extend the results of Theorem 2 Theorem 3 to the GGS maximal curve.*

Acknowledgments

The research of M. Bonini was supported by the Italian National Group for Algebraic and Geometric Structures and their Applications (GNSAGA - INdAM).

References

1. E. Ballico, Finite subsets of projective spaces with bad postulation in a fixed degree, Beitrage zur Algebra und Geometrie 54 (2013), no. 1, 81–103.
2. E. Ballico, Finite defective subsets of projective spaces, Riv. Mat. Univ. Parma 4 (2013), 113-122.
3. E. Ballico, Generalized Hamming weights of duals of Algebraic-geometric codes, International Journal of Pure and Applies Mathematics, 97 (2014), no. 2, 241–251.
4. E. Ballico, Defective curvilinear subschemes in projective spaces, International Journal of Pure and Applies Mathematics, 81 (2012), no. 1, 49–53.
5. E. Ballico, A. Ravagnani. On the duals of geometric Goppa codes from norm-trace curves. Finite Fields Appl. **20**, 30-39, (2013).
6. A. I. Barbero, C. Munuera. The weight hierarchy of Hermitian codes, SIAM Journal on Discrete Mathematics, 13 (1), pp. 79–104 (2000).
7. D. Bartoli, M. Bonini. Minimum weight codewords in dual Algebraic-Geometric codes from the Giulietti-Korchmáros curve, Designs, Codes and Cryptography **87**, no. 6, 1433-1455, (2019). (https://doi.org/10.1007/s10623-018-0541-y)
8. D. Bartoli, M. Montanucci, G. Zini. Multi point AG codes on the GK maximal curve. Des. Codes Cryptogr. (2017). DOI:10.1007/s10623-017-0333-9.
9. M. Bonini, M. Sala. Intersections between the norm-trace curve and some low degree curves, Finite Fields and Their Applications, in press (arXiv:1812.08590).

10. A.S. Castellanos, G.C. Tizziotti. Two-point AG Codes on the GK maximal curves. IEEE Trans. Inf. Theory **62**(2), 681–686 (2016).
11. A. Couvreur. The dual minimum distance of arbitrary-dimensional algebraic-geometric codes. J. Algebra **350**(1), 84–107 (2012).
12. S. Fanali, M. Giulietti. One-point AG codes on the GK Maximal Curves. IEEE Trans. Inf. Theory **56**(1), 202–210 (2010).
13. G. L. Feng, K. K. Tzeng, V.K. Wei. On the generalized Hamming weights of several classes of cyclic cods, IEEE transactions on information theory, 38(3), pp. 1125–1130 (1992).
14. M. Giulietti, G. Korchmáros. A new family of maximal curves over a finite field. Math. Ann. 343(1), 229–245 (2009).
15. V.D. Goppa. Codes on algebraic curves. Dokl. Akad. NAUK SSSR **259**, 1289–1290 (1981).
16. V.D. Goppa. Algebraic-geometric codes. Izv. Akad. NAUK SSSR **46**, 75–91 (1982).
17. A. Garcia, C. Güneri, H. Stichtenoth, A generalization of the Giulietti-Korchmáros curve, Adv. Geom. **10**, 427-434 (2010).
18. J.P. Hansen. Codes on the Klein quartic, ideals and decoding. IEEE Trans. Inf. Theory **33**(6), 923–925 (1987).
19. R. Hartshorne, Algebraic Geometry, Springer-Verlag, Berlin–Heidelberg–New York, 1977.
20. J. W. P. Hirschfeld, M. A. Tsfasman, S. G. Vladut. The weight hierarchy of higher dimensional Hermitian codes, IEEE transactions on information theory, 40(1), 275-278 (1994).
21. W. C. Huffman and V. Pless. Fundamentals of error-correcting codes. Cambridge university press, 2003.
22. C. Marcolla, M. Pellegrini, M. Sala. On the small-weight codewords of some Hermitian codes. J. Symbolic Comput. **73**, 27–45 (2016).
23. G.L. Matthews. Codes from the Suzuki function field. IEEE Trans. Inf. Theory **50**(12), 3298–3302 (2004).
24. H. Stichtenoth. Algebraic function fields and codes. Graduate Texts in Mathematics 254, Springer, Berlin (2009).
25. M.A. Tsfasman, S. G. Vladut. Geometric approach to higher weights, IEEE Transactions on Information Theory 41(6), 1564–1588 (1995).
26. V. K. Wei. Generalized Hamming weights for linear codes, IEEE Transactions on information theory, 37(5), pp 1412–1418 (1991).
27. V. K. Wei, K. Yang. On the generalized Hamming weights of product codes, IEEE transactions on information theory, 39(5), pp. 1709–1713 (1993).