Minimal weight codewords of some codes from the GK curve

Matteo Bonini

Università degli Studi di Trento

(Joint work with Daniele Bartoli — University of Perugia)

5 June 2017

Giulietti-Korchmáros curve

Let ℓ be a prime power.

Definition

The GK curve $\mathcal{X}$ (Giulietti, Korchmáros, [5]), over $\mathbb{F}_{\ell^6}$ is a non-singular curve defined by the equations

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

Giulietti-Korchmáros curve

Let ℓ be a prime power.

Definition

The GK curve $\mathcal{X}$ (Giulietti, Korchmáros, [5]), over $\mathbb{F}_{\ell^6}$ is a non-singular curve defined by the equations

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

The GK curve has:

- genus $g = \frac{(\ell^3+1)(\ell^2-2)}{2} + 1$;
- $\ell^8 - \ell^6 + \ell^5$ $\mathbb{F}_{\ell^6}$ rational affine points;
- one single point at the infinity, namely P_∞.

Maximal Curves

Definition

A curve is said to be maximal if it attains the Hasse-Weil bound

$$|\mathcal{X}(\mathbb{F}_q)| = q + 1 + 2g\sqrt{q}.$$

Examples of maximal curves:

Maximal Curves

Definition

A curve is said to be maximal if it attains the Hasse-Weil bound

$$|\mathcal{X}(\mathbb{F}_q)| = q + 1 + 2g\sqrt{q}.$$

Examples of maximal curves:

- Hermitian curve;
- Ree Curve;
- Suzuki Curve.

Maximal Curves

Definition

A curve is said to be maximal if it attains the Hasse-Weil bound

$$|\mathcal{X}(\mathbb{F}_q)| = q + 1 + 2g\sqrt{q}.$$

Examples of maximal curves:

- Hermitian curve;
- Ree Curve;
- Suzuki Curve.

The GK curve is the first example of maximal curve not covered by the Hermitian curve.

Codes on the GK curve

AG codes on the GK curve

Algebraic-Geometric codes from the GK curve are widely studied for their interesting properties:

- Fanali and Giulietti in [4] studied one-point codes.
- Castellanos and Tiziotti then examined in [2] classes of two points codes.
- Bartoli, Montanucci and Zini in [1] analyzed the properties of some families of multi-points codes.
- Mascia, Rinaldo and Sala showed in [7] that any one-point code on the GK curve is an order domain code for certain values of q.

One-point AG codes

Definition

The Riemann-Roch space associated to a divisor D of a curve $\mathcal{X}$ is the vector space $\mathcal{L}(D)$ over $\mathbb{F}_q(\mathcal{X})$ is defined as

$$\mathcal{L}(D) = \{f \in \mathbb{F}_q[\mathcal{X}] \mid (f) + D \geq 0\} \cup \{0\}$$

where $\mathbb{F}_q[\mathcal{X}]$ is a rational function field on $\mathcal{X}$ and (f) indicates the principal divisor of f.

One-point AG codes

Definition

The Riemann-Roch space associated to a divisor D of a curve $\mathcal{X}$ is the vector space $\mathcal{L}(D)$ over $\mathbb{F}_q(\mathcal{X})$ is defined as

$$\mathcal{L}(D) = \{f \in \mathbb{F}_q[\mathcal{X}] \mid (f) + D \geq 0\} \cup \{0\}$$

where $\mathbb{F}_q[\mathcal{X}]$ is a rational function field on $\mathcal{X}$ and (f) indicates the principal divisor of f.

Let $D = \sum_{P \in \mathcal{X} \setminus \{P_\infty\}} P$.

Definition

The one-point AG Goppa code is defined as follows

$$C(D, mP_\infty) = \{f(P_1), \ldots, f(P_{\ell^8 - \ell^6 + \ell^5 - \ell^3}) \mid f \in \mathcal{L}(mP_\infty)\}.$$

Designed minimal distance

Definition

Take a one-point algebraic-geometric code $C(D, mP_\infty)$ on $\mathcal{X}$, we call

- $d^* = n - \deg(mP_\infty) = \ell^8 - \ell^6 + \ell^5 - m(\ell^3 + 1)$ the designed minimum distace for $C(D, mP_\infty)$.
- $d^{**} = \deg(mP_\infty) - 2g + 2 = m(\ell^3 + 1) - \ell^5 + 2\ell^3 - \ell^2 + 2$ the designed minimum distace for $C(D, mP_\infty)^\perp$.

Designed minimal distance

Definition

Take a one-point algebraic-geometric code $C(D, mP_\infty)$ on $\mathcal{X}$, we call

- $d^* = n - \deg(mP_\infty) = \ell^8 - \ell^6 + \ell^5 - m(\ell^3 + 1)$ the designed minimum distace for $C(D, mP_\infty)$.
- $d^{**} = \deg(mP_\infty) - 2g + 2 = m(\ell^3 + 1) - \ell^5 + 2\ell^3 - \ell^2 + 2$ the designed minimum distace for $C(D, mP_\infty)^\perp$.

Remark

Let d and $d^\perp$ be respectively the minimum distances of $C(D, mP_\infty)$ and $C(D, mP_\infty)^\perp$, we have that

- $d \geq d^*$;
- $d^\perp \geq d^{**}$.

Results on the minimum distance of AG dual codes

Theorem (Couvreur, [3])

Let $\mathcal{X}$ be a non singular curve in $\mathbb{P}^r$, let $D = \sum_{P \in \mathcal{X} \setminus \{P_\infty\}} P$, let $m \geq 2$ and d be the minimum distance of the code $C(D, mP_\infty)^\perp$.

(i) $d = m + 2$ if and only if exists a set of points such that $m + 2$ of them on the curve that are collinear in $\mathbb{P}^r$;

(ii) $d = 2m + 2$ if and only if exists a set of points such that $2m + 2$ of them lie on the intersection of the curve with a plane conic (possibly reducible) and such that no $m + 2$ of them are collinear;

(iii) $d = 3m$ if and only if there exists a set of points such that no $m + 2$ of them are collinear, no $2m + 2$ of them lie on a plane conic and $3m$ of them are coplanar and lie at the intersection of a cubic and a curve of degree m having no common irreducible component;

(iv) $d \geq 3m + 1$ if and only if no sub-family of the points of the curve satisfies one of the three above-cited configurations.

Intersections of the GK curve

Proposition

The maximal number of intersections between the GK curve and a line is $\ell^2 - \ell + 1$. Moreover if a line r meets the GK curve in more than $\ell + 1$ points then r is a $\ell^2 - \ell + 1$ secant and r can be written in the form

$$r : \begin{cases} X = \bar{x} \\ Y = \bar{y} \end{cases}.$$

Intersections of the GK curve

Proposition

The maximal number of intersections between the GK curve and a line is $\ell^2 - \ell + 1$. Moreover if a line r meets the GK curve in more than $\ell + 1$ points then r is a $\ell^2 - \ell + 1$ secant and r can be written in the form

$$r : \begin{cases} X = \bar{x} \\ Y = \bar{y} \end{cases}.$$

Proposition

The maximal number of intersections between the GK curve and a plane conic is

- $2(\ell + 1)$ if the conic is irredubible;
- $2(\ell^2 - \ell + 1)$ if the conic is reducible.

Codes under investigation

The designed minimum distance for the code $C(D, mP_\infty)^\perp$ is

$$d^{**} = \deg G - 2g + 2 = m(\ell^3 + 1) - \ell^5 + 2\ell^3 - \ell^2 + 2.$$

On the other hand, by [3] it is possible to determine the exact minimum distance of the code $C(D, mP_\infty)^\perp$ under certain conditions. In particular

- $\overline{d} = m + 2$ if we can find $m + 2$ collinear points.
- $\overline{d} = 2m + 2$ if we can find $2m + 2$ points on the GK curve which lie on a plane conic, and such that no $m + 2$ of them are collinear.

We look for the cases in which $\overline{d} > d^{**}$ in order to find out the exact minimum distance of these codes.

Remark

In both cases $\overline{d} > d^{**}$ if and only if $m \leq \ell^2 - 2$.

Minimal distance of some classes of GK codes

Applying the results on the intersections given before, using the theorem given by Couvreur we can say what is the real minimum distance of the code $C(D, mP_\infty)^\perp$ for some values of m.

Theorem

The minimum distance of $C(D, mP_\infty)^\perp$ is

1. $d = m + 2$ when $\ell \leq m \leq \ell^2 - \ell - 1$;
2. $d = 2m + 2$ when $\ell^2 - \ell \leq m \leq \ell^2 - 2$;
3. $d \geq 3m$ when $m \geq \ell^2 - 1$.

Affine-variety codes

Let $t \geq 1$ and consider an ideal $I = \langle g_1, \ldots, g_s \rangle$ of $\mathbb{F}_q[x_1, \ldots, x_t]$, $\{x_1^q - x_1, \ldots, x_t^q - x_t\} \subset I$.
The ideal I is zero-dimensional and radical. Let $V(I) = \{P_1, \ldots, P_n\}$ be the variety of I and $R = \mathbb{F}_q[x_1, \ldots, x_t]/I$.

Definition

An affine-variety code $C(I, L)$ is the image $\phi(L)$ of $L \subseteq R$, a $\mathbb{F}_q$-vector subspace of R of dimension r, given by the isomorphism of $\mathbb{F}_q$ vector spaces

$$\begin{aligned} \phi : R &\longrightarrow \mathbb{F}_q^n \\ f &\longmapsto (f(P_1), \ldots, f(P_n)). \end{aligned}$$

Duals of affine-variety codes

Property

If L is generated by $b_1, \ldots, b_r$, then the matrix

$$H := \begin{pmatrix} b_1(P_1) & b_1(P_2) & \ldots & b_1(P_n) \\ b_2(P_1) & b_2(P_2) & \ldots & b_2(P_n) \\ \vdots & \vdots & \vdots & \vdots \\ b_r(P_1) & b_r(P_2) & \ldots & b_r(P_n) \end{pmatrix}$$

is a generator matrix for $C(I, L)$.

Duals of affine-variety codes

Property

If L is generated by $b_1, \ldots, b_r$, then the matrix

$$H := \begin{pmatrix} b_1(P_1) & b_1(P_2) & \ldots & b_1(P_n) \\ b_2(P_1) & b_2(P_2) & \ldots & b_2(P_n) \\ \vdots & \vdots & \vdots & \vdots \\ b_r(P_1) & b_r(P_2) & \ldots & b_r(P_n) \end{pmatrix}$$

is a generator matrix for $C(I, L)$.

We will focus on the duals of affine-variety codes, so H will be the parity-check matrix of the code $C(I, L)^{\perp}$.

Weight distribution

Definition

Let C be a linear code, $c \in C$ and $0 \leq w \leq n$. The *weight* of c, denoted by $w(c)$, is the number of its non-zero components and

$$A_w(C) = |\{c \in C \mid w(c) = w\}|.$$

Weight distribution

Definition

Let C be a linear code, $c \in C$ and $0 \leq w \leq n$. The *weight* of c, denoted by $w(c)$, is the number of its non-zero components and

$$A_w(C) = |\{c \in C \mid w(c) = w\}|.$$

Remark

The knowledge of the weight distribution of a code is fundamental to compute the probability of undetected error (PUE) of the code.

Results on words of given weight

Lemma (Marcolla, Pellegrini, Sala, [6])

Let $1 \leq w \leq n$. Let $I = \langle g_1, \ldots, g_s \rangle$ be such that $\{x_1^q - x_1, \ldots, x_t^q - x_t\} \subset I$. Let L a subspace of $\mathbb{F}_{q^2}[x_1, \ldots, x_t]/I$ of dimension r generated by $\{b_1, \ldots, b_r\}$. Let J_w be the ideal in $\mathbb{F}_q[x_{1,1}, \ldots, x_{1,t}, \ldots, x_{w,t}, z_1, \ldots, z_w]$ generated by

$$J_w = \left\langle \left\{ \sum_{i=1}^{w} z_i b_j(x_{i,1}, \ldots, x_{i,t}) \right\}_{j=1,\ldots,r}, \{g_h(x_{i,1}, \ldots, x_{i,t})\}_{\substack{i=1,\ldots,w \\ h=1,\ldots,s}}, \right.$$
$$\left. \left\{ z_i^{q-1} - 1 \right\}_{i=1,\ldots,w}, \left\{ \prod_{1 \leq l \leq t} ((x_{j,l} - x_{i,l})^{q-1} - 1) \right\}_{1 \leq j < i \leq w} \right\rangle$$

Then :

$$\mathrm{A}_w(C(I,L)^{\perp}) = \frac{|V(J_w)|}{w!}.$$

Correspondence between AG codes and AV codes

Let $I = \langle Z^{\ell^2-\ell+1} - Y^{\ell^2} + Y, Y^{\ell+1} - X^{\ell} - X, X^{\ell^6} - X, Y^{\ell^6} - Y, Z^{\ell^6} - Z \rangle$ and let $R = \mathbb{F}_{\ell^6}[X, Y, Z]/I$. We take $L \subseteq R$ generated by

$$\mathcal{B}_{\ell,m} = \left\{ X^i Y^j Z^k + I \mid i \in [0, \ldots, \ell - 1],\ j \in [0, \ldots, \ell^2 - \ell],\ k \in [0, \ldots, m] \right\}$$

Remark

Under the previous conditions $\mathcal{B}_{\ell,m}$ is a basis for $\mathcal{L}(mP_\infty)$.

Remark

In this case we have that $C(D, mP_\infty) = C(I, L)$ and then $C(D, mP_\infty)^\perp = C(I, L)^\perp$

Number of minimal weight codewords of some GK codes

Our aim now is to count the exact number of the codewords of $C(D, mP_\infty)^\perp$ with minimum weight. Considering our codes as affine-variety codes is possible to obtain this result.

Theorem

Let $\ell + 1 \leq m \leq \ell^2 - \ell + 1$, then the number of minimum weight codewords of $C(D, mP_\infty)^\perp$ is

$$A_d(C(D, mP_\infty)^\perp) = (\ell + 1)(\ell^5 - \ell^3)(\ell^6 - 1)\binom{\ell^2 - \ell + 1}{d}$$

Bibliography

[1] 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.

[2] A.S. Castellanos , G.C. Tizziotti, Two-point AG Codes on the GK maximal curves, IEEE Trans. Inf. Theory 62/2 (2016) 681–686.

[3] A. Couvreur, The dual minimum distance of arbitrary-dimensional algebraic-geometric codes, Journal of Algebra, 350/1 (2012) 84–107.

[4] S. Fanali, M. Giulietti, One-point AG codes on the GK maximal curves, IEEE Transactions on Information Theory, 56/1 (2010) 202–210.

[5] M. Giulietti, G. Korchmáros, A new family of maximal curves over a finite field, Mathematische Annalen, 343/1 (2009) 229–245.

[6] C, Marcolla, M. Pellegrini, M. Sala, On the small-weight codewords of some Hermitian codes, Journal of Symbolic Computation 73 (2016) 27–45.

[7] C. Mascia, G. Rinaldo, M. Sala, Hilbert quasi-polynomial for order domain codes, arXiv:1607.07241v1.

THANK YOU
FOR THE ATTENTION