Maximal curves over finite fields

Maria Montanucci

Technical University of Denmark (DTU)

Joint work with: Daniele Bartoli, Peter Beelen, Massimo Giulietti, Leonardo Landi, Vincenzo Pallozzi Lavorante, Luciane Quoos, Fernando Torres, Giovanni Zini

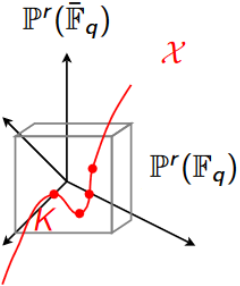
DTU Compute
Department of Applied Mathematics and Computer Science

Outline

- Maximal curves over finite fields
  - Notation and terminology
  - The three main problems
- Classification and construction of maximal curves
  - Natural embedding Theorem: (Galois-)subcovers of the Hermitian curve
  - The Giulietti-Korchmáros (GK) curve
  - The case of $\mathbb{F}_{p^2}$-maximal curves, p prime
  - The second generalized GK curve
- Spectrum of genera of maximal curves
  - The Galois-covering problem for maximal curves
  - Our method: spectrum of genera of Galois-subcovers of the Hermitian curve
- Weierstrass semigroups on points of known maximal curves
  - Weierstrass semigroups on the GK curve: Duursma's conjecture

Notation and terminology

- $\mathcal{X} \subseteq \mathbb{P}^r(\overline{\mathbb{F}}_q)$ projective, geometrically irreducible, non-singular algebraic curve defined over $\mathbb{F}_q$
- g genus of $\mathcal{X}$
  If $r = 2$ then $g = \frac{(d-1)(d-2)}{2}$, where $d = \deg(\mathcal{X})$
- $\mathcal{X}(\mathbb{F}_q) = \mathcal{X} \cap \mathbb{P}^r(\mathbb{F}_q)$
- $Aut(\mathcal{X})$ automorphism group of $\mathcal{X}$ over $\overline{\mathbb{F}}_q$



Maximal curves

$\mathcal{X}$ defined over $\mathbb{F}_q$

Hasse-Weil bound

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

Definition

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

A necessary condition is that q is a square or $g = 0$

Example

Hermitian curve:

$$\mathcal{H}_\ell : Y^{\ell+1} = X^\ell + X, \quad \ell = p^h, \quad q = \ell^2$$

$g = \ell(\ell - 1)/2, \qquad |\mathcal{H}_\ell(\mathbb{F}_q)| = \ell^3 + 1, \qquad Aut(\mathcal{H}_\ell) \cong PGU(3, \ell)$

Problems

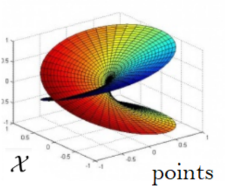
1. Classification and construction: how can we construct maximal curves?

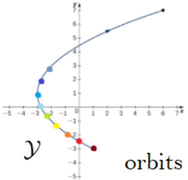
2. Spectrum of genera: which values $g > 0$ occur as genera of $\mathbb{F}_q$-maximal curves for a given q?

3. Applications to AG codes: how can we compute the Weierstrass semigroup at every point of a given maximal curve?

Coverings and Galois-coverings

- $\mathcal{X} \subseteq \mathbb{P}^r(\mathbb{F}_q)$ and $\mathcal{Y} \subseteq \mathbb{P}^s(\mathbb{F}_q)$
- If we have a non-constant $\phi : \mathcal{X} \to \mathcal{Y}$ then $\mathcal{Y}$ is covered by $\mathcal{X}$ (*subcover* of $\mathcal{X}$)
- $\overline{\mathbb{F}}_q(\mathcal{X}) : \phi^*(\overline{\mathbb{F}}_q(\mathcal{Y}))$ is a finite field extension
- $\overline{\mathbb{F}}_q(\mathcal{X}) : \phi^*(\overline{\mathbb{F}}_q(\mathcal{Y}))$ is Galois $\to$ $\mathcal{Y}$ is Galois-covered by $\mathcal{X}$ (*Galois-subcover* of $\mathcal{X}$)





(Kleiman-Serre, 1987)

If $\mathcal{X}$ is $\mathbb{F}_q$-maximal and $\mathcal{Y}$ is covered by $\mathcal{X}$ then $\mathcal{Y}$ is $\mathbb{F}_q$-maximal

Conjecture

Every $\mathbb{F}_q$-maximal curve is (Galois-)covered by the Hermitian curve $\mathcal{H}_q$

The conjecture is false: Natural Embedding Theorem

(Garcia-Stichtenoth, 2006)

The GS curve $X^9 - X = Y^7$ is $\mathbb{F}_{3^6}$-maximal and not Galois-covered by $\mathcal{H}_{3^3}$.

- Hermitian Variety in $\mathbb{P}^r(\overline{\mathbb{F}}_q)$:
  $\mathcal{H}_{r,q} : X_2^{q+1} + X_3^{q+1} + \ldots + X_r^{q+1} = X_1^q X_0 + X_1 X_0^q$

(Korchmáros-Torres, 2001)

Un to isomorphisms, $\mathbb{F}_{q^2}$-maximal curves are

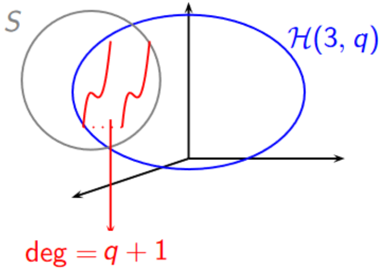
- contained in some $\mathcal{H}_{r,q}$ for some $r \geq 2$
- of degree $q + 1$
- not contained in any hyperplane of $\mathbb{P}^r(\overline{\mathbb{F}}_q)$

Definition

$r \geq 2$ is the geometrical Frobenius dimension of $\mathcal{X}$.

- If $r = 2$ then $\mathcal{X}$ is the Hermitian curve (up to isomorphism)

The conjecture is false: The case $r = 3$ and the GK curve



(Giulietti-Korchmáros, 2009)

Let q be a prime power of a prime p. The GK-curve

$$\mathcal{C} : \begin{cases} Z^{\frac{q^3+1}{q+1}} = Y^{q^2} - Y, \\ X^q + X = Y^{q+1} \rightarrow \text{Hermitian curve!} \end{cases}$$

if $\mathbb{F}_{q^6}$-maximal. if $q > 2$, $\mathcal{C}$ is not $\mathbb{F}_{q^6}$-covered by $\mathcal{H}_{q^3}$

Question: Why are both the GK and the GS curve $\mathbb{F}_{q^6}$-maximal?

The case of $\mathbb{F}_{p^2}$-maximal curves

Conjecture, 2000

Every $\mathbb{F}_{p^2}$-maximal curve is a subcover of the Hermitian curve $\mathcal{H}_p$

- The conjecture is true for $p \leq 5$
- No $\mathbb{F}_{p^2}$-maximal curves not Galois-covered by $\mathcal{H}_p$ are known
- Known $\mathbb{F}_{q^2}$-maximal curves have many automorphisms

Theorem (Bartoli-M.-Torres, Adv. in Geom., 2020)

Let $\mathcal{X}$ be an $\mathbb{F}_{p^2}$-maximal curves of genus g with $p \geq 7$. If $|Aut(\mathcal{X})| > 84(g-1)$ then $\mathcal{X}$ is Galois covered by $\mathcal{H}_p$

- Can Theorem be extended when $|Aut(\mathcal{X})| \leq 84(g-1)$? NO!
- First known example: $\mathbb{F}_{71^2}$-maximal Fricke-MacBeath curve
- (Bartoli-Güneş-M., in progress) The same result is true for $\mathbb{F}_{p^4}$-maximal curves unless $Aut(\mathcal{X})$ has a very special orbits-structure

A generalization of the GK-curve

(Garcia-Güneri-Stichtenoth, 2010)

Let q be a power of a prime p, $n \geq 3$ odd. The $\mathbb{F}_{q^{2n}}$-maximal GGS-curve is

$$\mathcal{C}_n : \begin{cases} Z^{\frac{q^n+1}{q+1}} = Y^{q^2} - Y, \\ Y^{q+1} = X^q + X. \end{cases}$$

Theorem (Duursma-Mak, 2012) → Conjecture for $q = 2$ (Bulletin of the Brazilian Math. Soc.)

For $q \geq 3$ and $n \geq 5$ odd, $\mathcal{C}_n$ is not Galois-covered by $\mathcal{H}_{q^n}$ over $\mathbb{F}_{q^{2n}}$

Theorem (Giulietti-M.Zini, FFA, 2016) → From my Master Degree Thesis

For $q = 2$ and $n \geq 5$ odd, $\mathcal{C}_n$ is not Galois-covered by $\mathcal{H}_{2^n}$ over $\mathbb{F}_{2^{2n}}$

- Key steps: If $\mathcal{C}_n \cong \mathcal{H}_{2^n}/G$: $|G| = \frac{2^n+1}{3}$ and G acts semiregularly on $\mathcal{H}_{2^n}$
- (Hartley, 1925): Maximal subgroups of $\mathrm{PSU}(3, 2^n)$ and their action on $\mathcal{H}_{2^n}$
- (Dickson, 1902): Classification of subgroups of $\mathrm{PSL}(2, 2^{2n})$

A new infinite family of maximal curves

- (Giulietti-Korchmáros, 2009) $Aut(\mathcal{C})/C_{(q^3+1)/(q+1)} \cong PGU(3,q)$ **entire** $Aut(\mathcal{H}_q)$
- (Guralnick-Malmskog-Pries, Güneri-Ozdemir-Stichtenoth, 2012-2013) If $n \geq 5$, $Aut(\mathcal{C}_n)/C_{(q^n+1)/(q+1)} \cong PGU(3,q)_{P_\infty}$ **maximal subgroup of** $Aut(\mathcal{H}_q)$
- (Mitchell 1911, Hartley 1925) Complete list of maximal subgroups of $Aut(\mathcal{H}_q)$.
- (M.-Zini, Comm. Algebra, 2018) Let ℓ be a non-tangent line to $\mathcal{H}_q$. Then $PGU(3,q)_\ell \cong SL(2,q) \rtimes C_{q+1}$ (maximal subgroup)

Question

Is it possible to construct another generalization $\{\mathcal{X}_n\}_n$ of $\mathcal{C}$ with $\mathcal{X}_3 \cong \mathcal{C}$ such that $Aut(\mathcal{X}_n)/C_{(q^n+1)/(q+1)} \cong PGU(3,q)_\ell$?

Let q be a power of a prime p, $n \geq 3$ odd,

$$\mathcal{X}_n : \begin{cases} Z^{\frac{q^n+1}{q+1}} = Y\frac{X^{q^2}-X}{X^{q+1}-1}, \\ Y^{q+1} = X^{q+1} - 1. \end{cases}$$

Some observations about the family $\{\mathcal{C}_n\}_n$, n odd

$\mathcal{H}_q : Y^{q+1} = X^q + X$ and P_∞ its unique point at infinity

- $Aut(\mathcal{H}_q)_{P_\infty} = \{\alpha_{b,c} | b, c \in \mathbb{F}_{q^2},\ b^{q+1} = c^q + c\} \rtimes \langle \beta_a \rangle$,

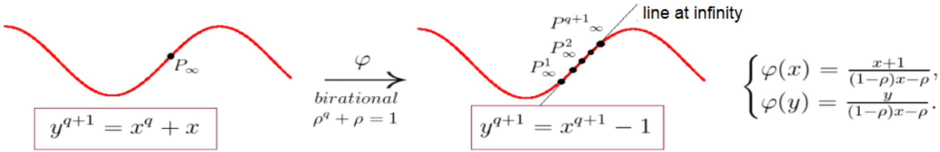
$$\alpha_{b,c}(X,Y) = (X + b^q Y + c, Y + b), \quad \beta_a(X,Y) = (a^{q+1}X, aY), \quad \langle a \rangle = \mathbb{F}_{q^2}^*$$

$$\mathcal{C}_n : \begin{cases} Y^{q+1} = X^q + X, \\ Z^{\frac{q^n+1}{q+1}} = Y^{q^2} - Y. \end{cases} \qquad Let\ \alpha \in Aut(\mathcal{H}_q)_{P_\infty}$$

- If $\alpha = \alpha_{b,c}$ then $\alpha(Y^{q^2} - Y) = Y^{q^2} - Y \implies$ we can define $\alpha(Z) = Z$
- if $\alpha = (\beta_a)^i$ then $\alpha(Y^{q^2} - Y) = a^i(Y^{q^2} - Y) \implies$ we can define $\alpha(Z) = \lambda_i Z$ where $\lambda_i^{(q^n+1)/(q+1)} = a^i$ so that

$$\alpha\left(Z^{\frac{q^n+1}{q+1}}\right) = \lambda_i^{\frac{q^n+1}{q+1}} Z^{\frac{q^n+1}{q+1}} = a^i(Y^{q^2} - Y) = \alpha(Y^{q^2} - Y)$$

The idea behind the construction of $\{\mathcal{X}_n\}_n$, n odd



- Define $\tilde{\varphi}(X,Y,Z) = (\varphi(X), \varphi(Y), -Z/(1-\rho)X-\rho)$ then $\tilde{\varphi}$ define a birational map

$$\mathcal{C} : \begin{cases} Y^{q+1} = X^q + X, \\ Z^{\frac{q^3+1}{q+1}} = Y^{q^2} - Y. \end{cases} \quad \mapsto \tilde{\varphi}(\mathcal{C}) := \mathcal{X}_3 : \begin{cases} Y^{q+1} = X^{q+1} - 1, \\ Z^{\frac{q^3+1}{q+1}} = Y\frac{X^{q^2}-X}{X^{q+1}-1}. \end{cases}$$

- Generalization (as for the GGS): $\mathcal{X}_n : \begin{cases} Y^{q+1} = X^{q+1} - 1, \\ Z^{\frac{q^n+1}{q+1}} = Y\frac{X^{q^2}-X}{X^{q+1}-1}. \end{cases}$

The idea behind the construction of $\{\mathcal{X}_n\}_n$, n odd

Theorem (Beelen-M., Journal of the London Math. Soc., 2018)

1. $\mathcal{X}_3$ is isomorphic to the GK curve $\mathcal{C}$,
2. $\mathcal{X}_n$ is $\mathbb{F}_{q^{2n}}$-maximal for every q and $n \geq 3$ odd,
3. For every $n \geq 5$ and $q \geq 3$ $\mathcal{X}_n$ is not Galois-covered by $\mathcal{H}_{q^n}$,
4. For every $n \geq 5$, $Aut(\mathcal{X}_n)/C_{(q^n+1)/(q+1)} \cong PGU(3,q)_\ell$, ℓ line at infinity,
5. Even though $g(\mathcal{X}_n) = g(\mathcal{C}_n)$ for every q and n, the curves $\mathcal{X}_n$ and $\mathcal{C}_n$ are isomorphic if and only if $n = 3$

- (Beelen-M., FFA, 2020) New other maximal curves as Galois-subcovers of $\mathcal{X}_n$
- (M.- Pallozzi Lavorante, Discrete Math., 2020) Weierstrass semigroups and codes

Questions

- What about other maximal subgroups?
- Can we use the Natural Embedding Theorem for $r = 4$?

A method to deal with the Galois covering problem

- Question: How can we decide in general whether a given $\mathbb{F}_{q^2}$-maximal curve is *new*, namely e.g. not Galois-covered by $\mathcal{H}_q$?

(M.-Zini, FFA, 2016)

A method to study Galois subcovers of $\mathcal{H}_q$ can be given in a purely geometric language (using Mitchell and Hartley results on $PGU(3,q)$)

- (M.-Zini, FFA, 2016) Suzuki and Ree curves $\mathcal{S}_8$ and $\mathcal{R}_3$ $\rightarrow$ proof of a conjecture by Rains and Zieve!
- (Giulietti-M.-Zini, FFA, 2016) Generalized GS curves
- (Giulietti-Kawakita-Lia-M., Advances in Geom., 2018) Wiman's sextics
- (Bartoli-Giulietti-Kawakita-M., FFA, 2020) New curves of genus 4 and 5 constructed using Kani-Rosen Theorem
- (Bartoli-M.-Torres, Advances in Geom., 2020) Fricke-MacBeath curve
- (Giulietti-M.-Quoos-Zini, J. Number Theory, 2020) Skabelund's curve

Further applications of the method

- (Hurwitz genus formula) If $G \leq Aut(\mathcal{H}_q) \cong PGU(3,q)$ then

$$2g(\mathcal{H}_q) - 2 = q^2 - q - 2 = 2|G|(g(\mathcal{H}_q/G) - 1) + \sum_{\sigma \in G} i(\sigma)$$

- (Mitchell 1918- Hartley 1925) The geometry and action of G can be predicted according to a maximal subgroup of $PGU(3,q)$ containing it.

(M.-Zini, FFA, 2016)

The contribution $i(\sigma)$ can be computed exactly for all $\sigma \in PGU(3,q)$ depinding on the order of σ and the geometry of the given group G containing it.

- IDEA: We can use the method to compute the genera of Galois-subcovers of $\mathcal{H}_q$

Spectrum of genera of maximal curves

Open problem (Garcia-Stichtenoth-Xing, Composition Math., 2000)

Compute the genera of all Galois-subcovers of the Hermitian curve $\mathcal{H}_q$

- **Complication:** A complete list of $G \leq PGU(3,q)$ is not known
- General idea: Case-by-Case analysis of subgroups of a given maximal subgroup of $PGU(3,q)$
  - G fixes an $\mathbb{F}_{q^2}$-rational point of $\mathcal{H}_q$ (Garcia-Stichtenoth-Xing 2000, Abdón-Quoos 2004, Bassa-Ma-Xing-Yeo 2013)
  - G fixes a self-polar triangle in $\mathbb{P}^2(\mathbb{F}_{q^2})$ (Giulietti-Hirschfeld-Korchmáros-Torres 2006, Dalla Volta- M. Zini, Communications in Alg., 2019)
  - G fixes a $(q+1)$-secant line to $\mathcal{H}_q$ (M.-Zini, Communications in Alg., 2018)
  - G is contained in the normalizer of a Singer cycle (Cossidente-Korchm'aros-Torres 1999-2000))
  - G has no fixed points or triangles (M.-Zini, J. Algebr. Comb., 2019)

(M.-Zini, J. Algebra, 2020)

Complete answer to the open problem when $q \equiv 1 \pmod 4$

Frobenius dimension and Weierstrass semigroups

Let $\mathcal{X}$ be a curve and let $P \in \mathcal{X}$

Definition: Weierstrass semigroup at P

$H(P) = \{\rho \in \mathbb{Z}_{\geq 0} \mid$ there exists a rat. func. f with $(f)_\infty = \rho P\}$

Weierstrass gap Theorem

$G(P) = \mathbb{N}_0 \setminus H(P)$ contains exactly $g(\mathcal{X})$ elements called gaps

Theorem

If $\mathcal{X}$ is $\mathbb{F}_{q^2}$-maximal and $P \in \mathcal{X}(\mathbb{F}_{q^2})$ then $q, q+1 \in H(P)$ and $r \leq$ number of non-gaps less than $q+1$

- The structure of $H(P)$ is almost always the same: Weierstrass points
- Independent interest (e.g. Stöhr-Voloch Theory) and main ingredient to construct AG codes!
- Hermitian curve: $r = 2 \rightarrow$ (Garcia-Viana, 1986)
- GK curve: $r = 3$ (smallest possible) $\rightarrow$?

Weierstrass semigroups on the GK curve $\mathcal{C}$

- (Giulietti-Korchmáros, 2009) $H(P) = \langle q^3 - q^2 + q, q^3, q^3 + 1 \rangle$, $P \in \mathcal{C}(\mathbb{F}_{q^2})$
- (Fanali-Giulietti, 2010) $H(P)$, $P \in \mathcal{C}(\mathbb{F}_{q^6}) \setminus \mathcal{C}(\mathbb{F}_{q^2})$ and $q \leq 3$
- (Duursma, 2011) $H(P)$, $P \in \mathcal{C}(\mathbb{F}_{q^6}) \setminus \mathcal{C}(\mathbb{F}_{q^2})$ and $q \leq 9$

Conjecture (Duursma 2011, IEEE Trans. Inf. Theory)

Let $P \in \mathcal{C}(\mathbb{F}_{q^6}) \setminus \mathcal{C}(\mathbb{F}_{q^2})$. Then

$$H(P) = \langle q^3 - q + 1, q^3 + 1, q^3 + i(q^4 - q^3 - q^2 + q - 1) \mid i = 0, \dots, q - 1 \rangle$$

- Nothing is known for $P \notin \mathcal{C}(\mathbb{F}_{q^6})$
- **Main questions:**
  1. Which points of $\mathcal{C}$ are Weierstrass points?
  2. Is it possible to determine $H(P)$ for all $P \in \mathcal{C}$? (in particular, to prove the conjecture)?

Weierstrass semigroups on the GK curve $\mathcal{C}$

(Theorem, Beelen-M., FFA, 2018)

Let $P \in \mathcal{C}$. Then

- $H(P) = \langle q^3 - q^2 + q, q^3, q^3 + 1 \rangle$, if $P \in \mathcal{C}(\mathbb{F}_{q^2})$;
- $H(P) = \langle q^3 - q + 1, q^3 + 1, q^3 + i(q^4 - q^3 - q^2 + q - 1) \mid i = 0, \ldots, q-1 \rangle$, if $P \in \mathcal{C}(\mathbb{F}_{q^6}) \setminus \mathcal{C}(\mathbb{F}_{q^2})$ $\rightarrow$ proof of Duursma's conjecture;
- $H(P) = \mathbb{N} \setminus G$, if $P \notin \mathcal{C}(\mathbb{F}_{q^6})$, where $G = \{iq^3 + kq + m(q^2+1) + \sum_{s=1}^{q-2} n_s((s+1)q^2) + j + 1 \mid i, j, k, m, n_1, \ldots, n_{q-2} \in \mathbb{Z}_{\geq 0}, j \leq q-1$ and $i + j + k + mq + \sum_s n_s((s+1)q - s) \leq q^2 - 2\}$.

(Corollary, Beelen-M., FFA, 2018)

The set of Weierstrass points of the GK curve is $W = \mathcal{C}(\mathbb{F}_{q^6})$

$\rightarrow$ One of the very few curves in which all Weierstrass semigroups and points are known!

Why is it a conjecture? Main difficulties

Let $P = P_{(a,b,c)} \in \mathcal{C}(\mathbb{F}_{q^6}) \setminus \mathcal{C}(\mathbb{F}_{q^2})$ and

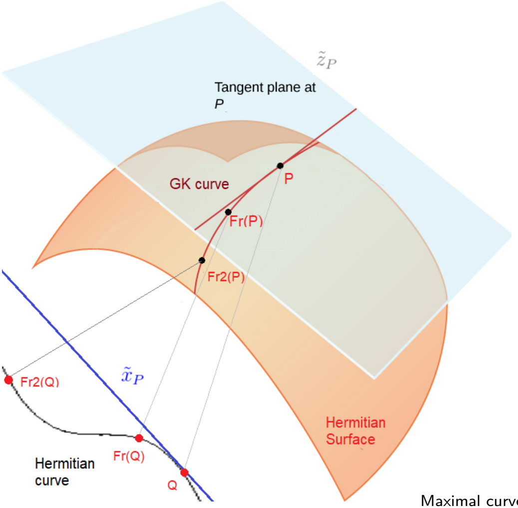
$$T := \langle q^3 - q + 1, q^3 + 1, q^3 + i(q^4 - q^3 - q^2 + q - 1) \mid i = 0, \dots, q-1 \rangle$$

- Two aims
  1. $T \subseteq H(P)$
  2. $|\mathbb{N} \setminus T| = g(\mathcal{C})$
- We need functions $f_\rho \in \mathbb{F}_{q^6}(\mathcal{C})$ with $(f_\rho)_\infty = \rho P$, ρ generator of T
- An explicit description of $f_\rho(x, y, z)$ can be really complicated
- Example $q = 3$: $f_{q^4-q^2+q-1} = f_{74}$ is

$$(2x^3b^{72} + 2x^3b^{64} + 2x^3b^{56} + 2x^3b^{48} + 2x^3b^{40} + 2x^3b^{32} + 2x^3b^{24} + 2x^3b^{16} + 2x^3b^8 + 2x^3 + 2x^2yb^{27} + x^2yb^3 + x^2b^{36}$$
$$+2x^2b^{12} + xy^2b^{54} + 2xy^2b^6 + xya^3b^{27} + 2xya^3b^3 + xyb^{63} + 2xyb^{39} + 2xa^3b^{36} + xa^3b^{12} + xb^{72} + xb^{48} + xb^{24} + y^3b^{73} + y^3b^{65}$$
$$+y^3b^{49} + y^3b^{41} + 2y^3b^{33} + y^3b^{25} + y^3b^{17} + 2y^3b^9 + y^2a^3b^{54} + 2y^2a^3b^6 + 2y^2b^{66} + y^2b^{18} + 2ya^6b^{27} + ya^6b^3 + ya^3b^{63}$$
$$+2a^9b^{72} + 2a^9b^{64} + 2a^9b^{56} + 2a^9b^{48} + 2a^9b^{40} + 2a^9b^{32} + 2a^9b^{24} + 2a^9b^{16} + 2a^9b^8 + 2a^9 + a^6b^{36} + 2a^6b^{12} + a^3b^{72} + a^3b^{48}$$
$$+2ya^3b^{39} + 2yb^{75} + 2yb^{51} + 2yb^{27} + a^3b^{24} + b^{84} + 2b^{12})/(-a^{27} - x + b^{27}y + c^{27}z)^3$$

Our proof of the Conjecture: $T \subseteq H(P)$

- There exists $\tilde{z}_P$ with $(\tilde{z}_P) = (q^3+1)P - (q^3+1)P_\infty$ (Natural Emb. Theorem)
- $\tilde{x}_P = -a^q - x + b^q y$ (tangent line at $P|Q$ on the Hermitian curve)
- $P \notin \mathcal{C}(\mathbb{F}_{q^2})$: $k = 1, 2$, k-Frobenius twist of $\tilde{x}_P$: $\tilde{x}_P^{(k)} = -a^{q^{2k+1}} - x + b^{q^{2k+1}} y$



Our proof of the Conjecture: $T \subseteq H(P)$

(Lemma, Beelen-M., FFA, 2018)

Let

$$f_i = \frac{\tilde{x}_P^{qi} \cdot \tilde{x}_P^{(2)}}{(\tilde{x}_P^{(1)})^i \cdot \tilde{z}_P^{q-i+1}}, \qquad i = 1, \ldots, q-1.$$

Then

$$(f_i)_\infty = q^3 + i(q^4 - q^3 - q^2 + q - 1)P$$

while $1/\tilde{z}_P$, $(y-b)/\tilde{z}_P$ and $\tilde{x}_P/\tilde{z}_P$ give $\langle q^3 - q + 1, q^3, q^3 + 1 \rangle \subseteq H(P)$. So $T \subseteq H(P)$

- (M.- Pallozzi Lavorante, Discrete Math., 2020) $H(P)$ where $P \in \mathcal{X}_n(\mathbb{F}_{q^2})$
- (Bartoli-M.-Zini, Acta Arith., 2020) $H(P)$ at every P and W: Suzuki curve $\mathcal{S}_q$
- (Beelen-Landi-M., 2020) $H(P)$ at every P and W: Skabelund curve

Maria Montanucci
Department of Applied Mathematics and Computer Science
Technical University of Denmark (DTU)

Building 303B, Room 150
2800 Kgs. Lyngby, Denmark

marimo@dtu.dk.
+45 50106435