Algebraic curves with many rational points over finite fields

Maria Montanucci

Technical University of Denmark (DTU)

Joint work with: Daniele Bartoli, Peter Beelen, Leonardo Landi, Vincenzo Pallozzi Lavorante, Luciane Quoos, Guilherme Tizziotti, Fernando Torres, Lara Vicino, Giovanni Zini

DTU Compute

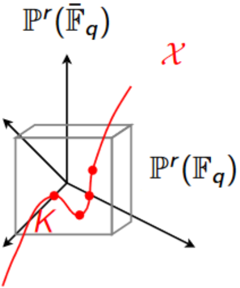
Department of Applied Mathematics and Computer Science

Outline

- Maximal curves over finite fields
  - Notation and terminology
  - Past, present and future research
- Classification and construction
  - The case of $\mathbb{F}_{p^2}$-maximal curves, p prime
  - The second generalized GK curve and its consequences
- Weierstrass semigroups and maximal curves
  - Weierstrass semigroups and the GK curve
  - Decoding AG codes from maximal curves
- Curves with many rational points in coding theory
  - LRC and MRD codes
  - What's next? The project **CREATE**

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 $d = \deg(\mathcal{X})$
- $Aut(\mathcal{X})$ automorphism group of $\mathcal{X}$ over $\overline{\mathbb{F}}_q$ (**Massimo's talk!**)
- $\mathcal{X}(\mathbb{F}_q) = \mathcal{X} \cap \mathbb{P}^r(\mathbb{F}_q)$



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

Necessary: q square or $g = 0$ (we change notation: $\mathbb{F}_q \to \mathbb{F}_{q^2}$)

Example: $\mathbb{F}_{q^2}$-maximal curve

Hermitian curve

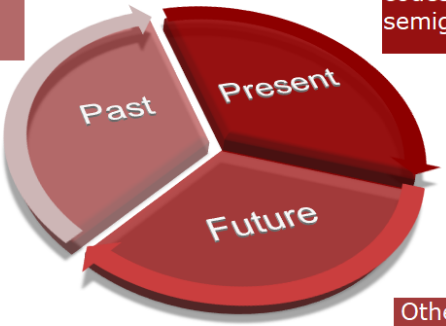
$$\mathcal{H}_q : Y^{q+1} = X^q + X, \quad q = p^h$$

$g = q(q-1)/2, \qquad |\mathcal{H}_q(\mathbb{F}_{q^2})| = q^3 + 1, \qquad Aut(\mathcal{H}_q) \cong PGU(3, q) \to \geq 16g^4$

My research on algebraic curves with many rational points

Classification and construction of maximal curves

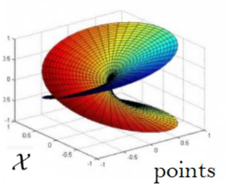
Applications to AG codes: Weierstrass semigroups

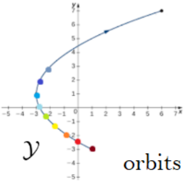


Other applications of curves with many points in coding theory

Coverings and Galois-coverings

- $\mathcal{X} \subseteq \mathbb{P}^r(\mathbb{F}_{q^2})$ and $\mathcal{Y} \subseteq \mathbb{P}^s(\mathbb{F}_{q^2})$
- Non-constant $\phi : \mathcal{X} \to \mathcal{Y} \implies \mathcal{Y}$ is covered by $\mathcal{X}$ (*subcover*)
- $\overline{\mathbb{F}}_{q^2}(\mathcal{X}) : \phi^*(\overline{\mathbb{F}}_{q^2}(\mathcal{Y}))$ is a finite field extension
- $\overline{\mathbb{F}}_{q^2}(\mathcal{X}) : \phi^*(\overline{\mathbb{F}}_{q^2}(\mathcal{Y}))$ Galois $\implies \mathcal{Y}$ is Galois-covered by $\mathcal{X}$ (*Galois-subcover*)





(Kleiman-Serre, 1987)

If $\mathcal{X}$ is $\mathbb{F}_{q^2}$-maximal and $\mathcal{Y}$ is $\mathbb{F}_{q^2}$-covered by $\mathcal{X}$ then $\mathcal{Y}$ is $\mathbb{F}_{q^2}$-maximal

Conjecture

Every $\mathbb{F}_{q^2}$-maximal curve is (Galois-)covered by the Hermitian curve $\mathcal{H}_q$

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 $\mathbb{P}^r(\overline{\mathbb{F}}_{q^2})$:
  $\mathcal{H}_{r,q} : X_2^{q+1} + X_3^{q+1} + \ldots + X_r^{q+1} = X_1^q X_0 + X_1 X_0^q$

Natural Embedding Theorem (Korchmáros-Torres, 2001)

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

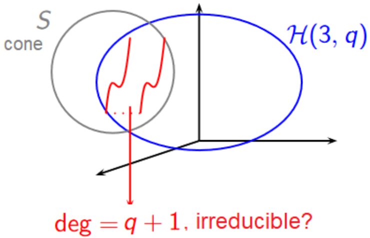
- contained in some $\mathcal{H}_{r,q}$ for some $r \geq 2$
- irreducible of degree $q+1$
- not contained in any hyperplane of $\mathbb{P}^r(\overline{\mathbb{F}}_q)$

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) $\rightarrow$ $r \geq 3$?

The conjecture is false: 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 $\mathcal{H}_p$

Note: Known $\mathbb{F}_{p^2}$-maximal curves are Galois-covered by $\mathcal{H}_p$ and have many automorphisms

Theorem (Bartoli-M.-Torres, 2020)

Let $\mathcal{X}$ be an $\mathbb{F}_{p^2}$-maximal curves of genus $g \geq 2$, $p \geq 7$. 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!
- Example: $\mathbb{F}_{71^2}$-maximal Fricke-MacBeath curve

Question (open)

Are there other examples? Is a similar result true for $\mathbb{F}_{p^{2n}}$-maximal curves?

A generalization of the GK-curve

(Garcia-Güneri-Stichtenoth, 2010)

Let q be a prime power, $n \geq 3$ 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)

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

Theorem (Giulietti-M.-Zini, 2016)

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

- 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 $\mathrm{PGU}(3, 2^n)$ and their action on $\mathcal{H}_{2^n}$

A new 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)

$n \geq 5$, $Aut(\mathcal{C}_n)/C_{(q^n+1)/(q+1)} \cong PGU(3,q)_{P_\infty}$ **maximal subgroup** of $Aut(\mathcal{H}_q)$

- (Mitchell 1911, Hartley 1925) Maximal subgroups of $Aut(\mathcal{H}_q)$
- (M.-Zini, 2018) $PGU(3,q)_\ell$ **second largest maximal subgroup** of $Aut(\mathcal{H}_q) \cong PGU(3,q)$

Idea

Find another family $\{\mathcal{X}_n\}_n$ with $\mathcal{X}_3 \cong \mathcal{C}$ such that $Aut(\mathcal{X}_n)/C_{(q^n+1)/(q+1)} \cong PGU(3,q)_\ell$

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

Intuition: $Aut(\mathcal{C}_n)/C_{(q^n+1)/(q+1)} \cong PGU(3,q)_{P_\infty}$

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

Observation 1

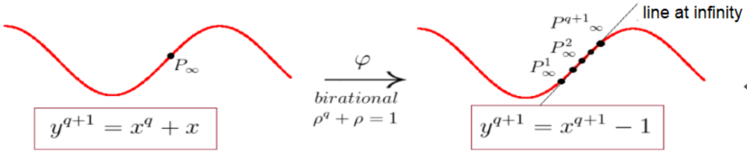
$\alpha(Y^{q^2} - Y) = a(Y^{q^2} - Y)$ for some constant a.

Observation 2

Any such α can be lifted in $Aut(\mathcal{C}_n)$ just by defining $\alpha(Z) = \lambda Z$, $\lambda^{(q^n+1)/(q+1)} = a$

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

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



$$\begin{cases} \varphi(x) = \frac{x+1}{(1-\rho)x-\rho}, \\ \varphi(y) = \frac{y}{(1-\rho)x-\rho}. \end{cases}$$

- $\tilde{\varphi}(X,Y,Z) = (\varphi(X), \varphi(Y), -Z/(1-\rho)X-\rho)$ defines 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 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. $g(\mathcal{X}_n) = g(\mathcal{C}_n)$ but $\mathcal{X}_n$ and $\mathcal{C}_n$ are isomorphic if and only if $n = 3$

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

Questions

- Can we use the Natural Embedding Theorem for $r = 4$?
- What about other properties? (New PhD: Jonathan Tilling Niemann)

From the generalized GK curves

(Tafazolian-Teherán-Herrera-Torres, 2016)

Galois-subcovers of the GGS curve, $m = \frac{q^n+1}{q+1}$, s divisor of m, $q = p^a$, $\bar{q} = p^b$ with $b \mid a$, $c^{q-1} = -1$

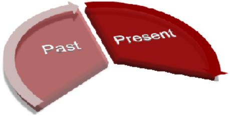
$$\mathcal{Y}_{n,s} : \begin{cases} Z^{m/s} = Y^{q^2} - Y \\ Y^{q+1} = X^q + X \end{cases} \qquad \mathcal{X}_{a,b,n,s} : \begin{cases} Z^{m/s} = Y^{q^2} - Y \\ cY^{q+1} = X + X^{\bar{q}} + \cdots + X^{q/\bar{q}} \end{cases}$$

- for some values of the parameters $\mathcal{X}_{a,b,n,s}$ and $\mathcal{Y}_{n,s}$ are not covered by $\mathcal{H}_{q^n}$
- **Reason**: values of $g(\mathcal{Y}_{n,s})$ and $g(\tilde{\mathcal{X}}_{a,b,n,s})$
- **Observation:** the groups inducing $\mathcal{X}_{a,b,n,s}$ and $\mathcal{Y}_{n,s}$ exist also in $Aut(\mathcal{X}_n)$ and $g(\mathcal{X}_n) = g(\mathcal{C}_n)$

Idea

Create the anologue curves $\tilde{\mathcal{X}}_{a,b,n,s}$ and $\tilde{\mathcal{Y}}_{n,s}$ as subcovers of $\mathcal{X}_n$

The curves $\tilde{\mathcal{Y}}_{n,s}$ and $\tilde{\mathcal{X}}_{a,b,n,s}$



$n \geq 3$ odd, $m = \frac{q^n+1}{q+1}$, $s \mid m$, $\quad q = p^a$, $\bar{q} = p^b$, $b \mid a$

$$\tilde{\mathcal{Y}}_{n,s} : \begin{cases} Z^{m/s} = Y \frac{X^{q^2} - X}{X^{q+1} - 1} \\ Y^{q+1} = X^{q+1} - 1 \end{cases} \qquad \tilde{\mathcal{X}}_{a,b,n,s} := \tilde{\mathcal{Y}}_{n,s}/E_{\bar{q}}$$

where $E_{\bar{q}} \leq \mathrm{Aut}(\tilde{\mathcal{Y}}_{n,s})$ is the lift to $\tilde{\mathcal{Y}}_{n,s}$ of the stabilizer of $P \in \tilde{\mathcal{H}}_q(\mathbb{F}_{q^2})$,
$\tilde{\mathcal{H}}_q : \; y^{q+1} = x^{q+1} - 1$

(M.-Tizziotti-Zini, 2023)

$g(\tilde{\mathcal{Y}}_{n,s}) = g(\mathcal{Y}_{n,s})$ but $\tilde{\mathcal{Y}}_{n,s} \not\cong \mathcal{Y}_{n,s}$

$g(\tilde{\mathcal{X}}_{a,b,n,s}) = g(\mathcal{X}_{a,b,n,s})$, $\tilde{\mathcal{X}}_{a,b,n,s} \not\cong \mathcal{X}_{a,b,n,s}$

$\Longrightarrow$ new $\mathbb{F}_{q^{2n}}$-maximal curves not covered by $\mathcal{H}_{q^n}$

More info: Giovanni's Talk!

Weierstrass semigroups and maximal curves

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

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 $r \leq$ number of elements in $H(P)$ less than $q+1$

- The structure of $H(P)$ is almost always the same: Weierstrass points
- Main ingredient to construct AG codes!
- Hermitian curve: $r = 2 \rightarrow$ (Garcia-Viana, 1986)
- GK curve: $r = 3 \rightarrow$?

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

Present

- (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

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

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

- Nothing known for $P \notin \mathcal{C}(\mathbb{F}_{q^6})$

(Beelen-M., 2018)

- $H(P)$ for all $P \in \mathcal{C}$ $\rightarrow$ conjecture proven!
- The set of Weierstrass points of the GK curve is $\mathcal{C}(\mathbb{F}_{q^6})$

Why was it a conjecture?

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

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

- 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

$$(2x^3b^{72} + 2x^3b^{64} + 2x^3b^{56} + 2x^3b^{48} + 2x^3b^{40} + 2x^3b^{32} + 2x^3b^{24} + 2x^3b^{16} + 2x^3b^{8} + 2x^3 + 2x^2yb^{27} + x^2yb^3 + x^2b^{36}$$

$$+2x^2b^{12} + xy^2b^{54} + 2xy^2b^6 + xya^3b^{27} + 2xya^3b^3 + xyb^{63} + 2xyb^{39} + 2xa^3b^{36} + xa^3b^{12} + xb^{72} + xb^{48} + xb^{24} + y^3b^{73} + y^3b^{65}$$

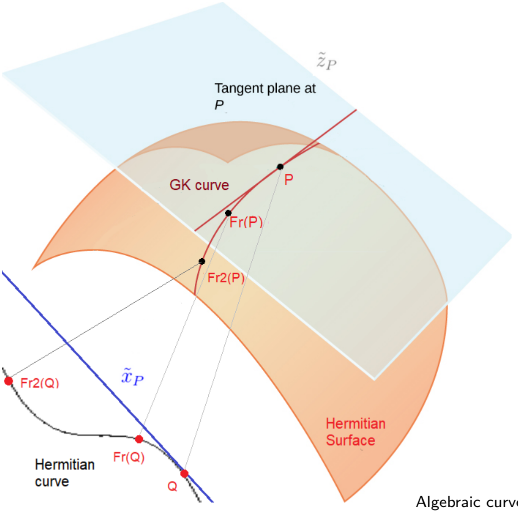
$$+y^3b^{49} + y^3b^{41} + 2y^3b^{33} + y^3b^{25} + y^3b^{17} + 2y^3b^9 + y^2a^3b^{54} + 2y^2a^3b^6 + 2y^2b^{66} + y^2b^{18} + 2ya^6b^{27} + ya^6b^3 + ya^3b^{63}$$

$$+2a^9b^{72} + 2a^9b^{64} + 2a^9b^{56} + 2a^9b^{48} + 2a^9b^{40} + 2a^9b^{32} + 2a^9b^{24} + 2a^9b^{16} + 2a^9b^8 + 2a^9 + a^6b^{36} + 2a^6b^{12} + a^3b^{72} + a^3b^{48}$$

$$+2ya^3b^{39} + 2yb^{75} + 2yb^{51} + 2yb^{27} + a^3b^{24} + b^{84} + 2b^{12})/(-a^{27} - x + b^{27}y + c^{27}z)^3$$

Proving the conjecture: $T \subseteq H(P)$

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



Proving the conjecture: $T \subseteq H(P)$

Present

DTU

(Lemma, Beelen-M., 2018)

Let

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

Then $1/\tilde{z}_P$, $(y-b)/\tilde{z}_P$, $\tilde{x}_P/\tilde{z}_P$ and f_i give $T \subseteq H(P)$

- (M.- Pallozzi Lavorante, 2020) $H(P)$ where $P \in \mathcal{X}_n(\mathbb{F}_{q^2})$
- (Bartoli-M.-Zini, 2020) $H(P)$ at every P: Suzuki curve
- (Beelen-Landi-M., 2021) $H(P)$ at every P: Skabelund curve
- (Beelen-M.-Vicino, 2023) $H(P)$ at every P: third largest genus (**Lara's talk!**)

Question

Can this method also work for the Ree curve?

The Fundamental Equality: list decoding

- List decoding: the decoder gives a short list of messages that might have been encoded
- Guruswami-Sudan list decoding: $c = (f(P_1), \ldots, f(P_n))$ find a polynomial Q such that $Q(f) = 0$
- **Main steps**: Interpolation step+root finding (optimize?)
- **Theoretically**: find a set of conditions that ensure Q exists and has an nice form

(Beelen-M., 202?)

Efficient Guruswami-Sudan list decoding algorithm for AG codes from maximal curves using the fundamental equation

$$Q(z) = Q_{q+1} z_{q+1} + Q_q z^q + Q_1 z + Q_0$$

- We are still working on the algorithmic complexity/optimization!

Algebraic curves in Coding Theory

DTU

(Bartoli-M.-Quoos, 2021)

LRC codes from automorphisms of curves of genus $g \geq 1$ (maximal/p-rank zero curves have special automorphism groups **Massimo's talk**)

(Bartoli-M.-Zini, 2022)

Quantum codes from "Swiss curves"

(Bartoli-Csajbók-M., Marino-M.-Zullo, Bartoli-M., Zanella-M., 2021/2022)

Algebraic curves methods to construct/classify asymptotically **MRD codes** (maximum/exceptional scattered polynomials)

- **Dream:** find a big picture for all these ad-hoc constructions
- With some extra help: develop the right algebraic curves theory/construct the right curves

Algebraic curves in Information Theory: a treasure yet to discover 2023/2028

CREATE
ALGEBRAIC CURVES IN INFORMATION THEORY

2023: Postdoc (MRD codes)

2024: PhD (Algebraic curves)

2026: Postdoc (LRC codes)

THE VELUX FOUNDATIONS

VILLUM FONDEN VELUX FONDEN

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