Goppa–Like AG Codes from $C_{a,b}$ curves And the dimension of the square of their dual

Sabira El Khalfaoui, Mathieu Lhotel, **Jade Nardi**

CNRS, IRMAR, University of Rennes, France

AGC^2T 2023
9^{th} June 2023

arxiv.org/abs/2303.08687

Preliminaries: linear code

Let q be a prime power and $\mathbb{F}_q$ a finite field of size q.

Definition: Linear code

A **linear code** $\mathcal{C}$ of length n is a vector subspace of $\mathbb{F}_q^n$. It is said to be t–correcting if $\omega(\boldsymbol{c}) \geq 2t+1$ for every $\boldsymbol{c} = (c_1, \ldots, c_n) \in \mathcal{C}$, where $\omega(\boldsymbol{c}) = \#\{i \mid c_i \neq 0\}$ (Hamming weight).

A **generator matrix** of $\mathcal{C}$ is a matrix whose rows form a basis of $\mathcal{C}$.

The **dual code** of $\mathcal{C}$ is $\mathcal{C}^\perp = \left\{\boldsymbol{x} \in \mathbb{F}_q^n \mid \boldsymbol{c} \cdot \boldsymbol{x} = 0, \text{ for all } \boldsymbol{c} \in \mathcal{C}\right\}$. ($\cdot$ is the usual scalar product.)

Context and motivation: McEliece cryptosystem

→ First code-based public key encryption (1978).

Parameters: $n, t \in \mathbb{N}$ with $t \ll n$. A family $\mathcal{F}$ of efficiently decodable t–correcting codes $\mathcal{C} \subset \mathbb{F}_q^n$.

Key generation : $G^{\text{pub}} = SGP$ where

- G is a generator matrix of size $k \times n$ of a *random* code $\mathcal{C} \in \mathcal{F}$,
- S is a *random* invertible $k \times k$,
- P is a *random* permutation $n \times n$ matrix.

Public key: (G^{pub}, t).

Private key: $(S, D_{\mathcal{C}}, P)$ where $D_{\mathcal{C}}$ is an efficient decoding algorithm for $\mathcal{C}$.

Encryption of a cleartext $\boldsymbol{m} \in \mathbb{F}_q^k$**:** *randomly* pick $\boldsymbol{z} \in \mathbb{F}^n$ of weight t. → $\boldsymbol{y} = \boldsymbol{m}G^{\text{pub}} + \boldsymbol{z}$.

Decryption using the private key.

Its security is based on

1. the hardness of decoding random linear codes,
2. the indistinguishability of the chosen codes from random ones.

McEliece's original proposal, based on **binary Goppa codes**, has very large key size.

Goppa codes

Definition: Generalized Reed–Solomon (GRS)

Let $\boldsymbol{x} = (x_1, \cdots, x_n) \in \mathbb{F}_q^n$ with distinct entries (**support**) and **multiplier** $\boldsymbol{y} \in (\mathbb{F}_q^*)^n$.

$$\mathsf{GRS}_r(\boldsymbol{x}, \boldsymbol{y}) = \{(y_1 f(x_1), y_2 f(x_2), \ldots, y_n f(x_n)) \mid f \in \mathbb{F}_q[X] \text{ such that } \deg f < r\}.$$

Definition: Subfield subcode

Let $\mathcal{C}$ be a linear code over $\mathbb{F}_{q^m}$. Its **subfield subcode** $\mathcal{C}|_{\mathbb{F}_q}$ is defined by $\mathcal{C}|_{\mathbb{F}_q} = \mathcal{C} \cap \mathbb{F}_q^n$.

Definition: Goppa code of order r

Let $\boldsymbol{x} = (x_1, \cdots, x_n) \in \mathbb{F}_{q^m}^n$ with distinct entries and $g \in \mathbb{F}_{q^m}[x]$ be a polynomial of degree r such that $\forall i, g(x_i) \neq 0$. The **Goppa code** associated to $(\boldsymbol{x}, g)$ is defined as

$$\Gamma_r(\boldsymbol{x}, g) = \mathsf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})^{\perp}|_{\mathbb{F}_q},$$

where $\boldsymbol{y} = (g(x_1)^{-1}, \ldots, g(x_n)^{-1})$.

Even if Generalized Reed–Solomon are heavily structured, Goppa codes *look like* random codes.

Schur Product and Square code Distinguisher

Many attemps to replace Goppa codes have been broken by using an operation that endows $\mathbb{F}_q^n$ with an algebra structure, the Schur product.

In $\mathbb{F}_q^n$ we denote by $\star$ the **Schur product** $\boldsymbol{c} \star \boldsymbol{d} = (c_1 d_1, \cdots, c_n d_n)$.

The Schur product of two codes $\mathcal{C}, \mathcal{D} \subseteq \mathbb{F}_q^n$ is $\mathcal{C} \star \mathcal{D} = \mathrm{Span}\{\boldsymbol{c} \star \boldsymbol{d} \mid \mathbf{c} \in \mathcal{C}, \mathbf{d} \in \mathcal{D}\}$.

If $\mathcal{C} = \mathcal{D}$, then we denote by $\mathcal{C}^{\star \mathbf{2}} = \mathcal{C} \star \mathcal{C}$.

Schur Product and Square code Distinguisher

Many attemps to replace Goppa codes have been broken by using an operation that endows $\mathbb{F}_q^n$ with an algebra structure, the Schur product.

In $\mathbb{F}_q^n$ we denote by $\star$ the **Schur product** $\boldsymbol{c} \star \boldsymbol{d} = (c_1 d_1, \cdots, c_n d_n)$.
The Schur product of two codes $\mathcal{C}, \mathcal{D} \subseteq \mathbb{F}_q^n$ is $\mathcal{C} \star \mathcal{D} = \mathrm{Span}\{\boldsymbol{c} \star \boldsymbol{d} \mid \mathbf{c} \in \mathcal{C}, \mathbf{d} \in \mathcal{D}\}$.
If $\mathcal{C} = \mathcal{D}$, then we denote by $\mathcal{C}^{\star \mathbf{2}} = \mathcal{C} \star \mathcal{C}$.

Dimension of the square of a linear code

Let $\mathcal{C} = \mathrm{Span}\{\boldsymbol{c}_1, \ldots, \boldsymbol{c}_k\} \subseteq \mathbb{F}_q^n$. Then $\mathcal{C}^{\star 2} = \mathrm{Span}\{\boldsymbol{c}_i \star \boldsymbol{c}_j \mid 1 \leq i \leq j \leq k\}$, so

$$\dim(\mathcal{C}^{\star 2}) \leq \min\left(n, \binom{k+1}{2}\right).$$

If $\mathcal{C}$ is random, we expect to have equality.

We can use this property as a **distinguisher**, *i.e.* to identify certain codes from random ones.

- If $r \leq \frac{n+1}{2}$: then $\dim(\mathrm{GRS}_r(\boldsymbol{x}, \boldsymbol{y})^{\star 2}) = \dim(\mathrm{GRS}_{2r-1}(\boldsymbol{x}, \boldsymbol{y} \star \boldsymbol{y})) = 2r - 1 < \binom{r+1}{2}$.
- AG codes have a similar behaviour (Mumford, 1970): if $\mathcal{C}$ is an AG code over a curve of genus $\mathfrak{g}$, then $\dim \mathcal{C}^{\star 2} \simeq 2 \dim \mathcal{C} - \mathfrak{g} - 1$.

Some attemps to reduce the key size in McEliece cryptosystem

- **Generalized Reed-Solomon codes** by Niederreiter (1986)
  🔨 Sidelnikov & Shestakov (1992): recover the support and the multiplier by linear algebra.
- **Subcodes of Generalized Reed-Solomon codes** by Berger & Loidreau (2005)
  🔨 Wieschebrink (2010): use the previous attack on the square of the code.
- **Algebraic geometry codes** and their **subfield subcodes** by Janwa & Moreno (1996)
  🔨 Faure & Minder (2008): use the group structure of curves of genus $g \leq 2$.
  🔨 Couvreur, Márquez-Corbella & Pellikaan (2014): filtration attack using the Schur product.
  These attacks do not apply to **subfield subcodes of AG codes**.

Some attemps to reduce the key size in McEliece cryptosystem

- **Generalized Reed-Solomon codes** by Niederreiter (1986)
  🔨 Sidelnikov & Shestakov (1992): recover the support and the multiplier by linear algebra.
- **Subcodes of Generalized Reed-Solomon codes** by Berger & Loidreau (2005)
  🔨 Wieschebrink (2010): use the previous attack on the square of the code.
- **Algebraic geometry codes** and their **subfield subcodes** by Janwa & Moreno (1996)
  🔨 Faure & Minder (2008): use the group structure of curves of genus $g \leq 2$.
  🔨 Couvreur, Márquez-Corbella & Pellikaan (2014): filtration attack using the Schur product.
  These attacks do not apply to **subfield subcodes of AG codes**.

Let us try to replace Goppa codes by subfield subcodes of AG codes in McEliece cryptosystem!

Classical Goppa code vs. Goppa-like AG codes on $C_{a,b}$ curves

Let a, b be coprime positive integers.

For polynomials in $\mathbb{F}_{q^m}[x, y]$, we defined a **weighted degree** by $\deg_{a,b}\left(x^i y^j\right) = ai + bj$.

$$\deg_{a,b}(f) = \max\left\{\deg_{a,b}\left(x^i y^j\right) \mid a_{i,j} \neq 0\right\} \text{ for } f = \sum a_{i,j} x^i y^j.$$

A $C_{a,b}$ curve is a plane curve $\mathcal{X}_{a,b}$ with affine equation $f_{a,b}(x, y) = \alpha y^a + \beta x^b + f'$ with $\alpha, \beta \neq 0$ and $\deg_{a,b}(f') < ab$. (elliptic curves, Hermitian curve...)

Classical Goppa code vs. Goppa-like AG codes on $C_{a,b}$ curves

Let a, b be coprime positive integers.
For polynomials in $\mathbb{F}_{q^m}[x,y]$, we defined a **weighted degree** by $\deg_{a,b}\left(x^i y^j\right) = ai + bj$.

$\deg_{a,b}(f) = \max\left\{\deg_{a,b}\left(x^i y^j\right) \mid a_{i,j} \neq 0\right\}$ for $f = \sum a_{i,j} x^i y^j$.

A $C_{a,b}$ curve is a plane curve $\mathcal{X}_{a,b}$ with affine equation $f_{a,b}(x,y) = \alpha y^a + \beta x^b + f'$ with $\alpha, \beta \neq 0$ and $\deg_{a,b}(f') < ab$. (elliptic curves, Hermitian curve...)

	Classical Goppa codes	One–point **Goppa–like AG codes** on $C_{a,b}$ curves
Context	A degree r	A weighted degree r
We evaluate $f \in$	$\mathbb{F}_{q^m}[x]_{<r}$	$\mathbb{F}_{q^m}[x,y]$ with $\deg_{a,b}(f) < r$
at...	$\boldsymbol{x} = (x_1, \cdots, x_n)$	$\mathcal{P} = (P_1, \ldots, P_n) \subset \mathcal{X}_{a,b}(\mathbb{F}_{q^m})$ $\quad P_i = (x_i, y_i)$
divided by...	$g \in \mathbb{F}_{q^m}[x]$, $\deg(g) = r$	$g \in \mathbb{F}_{q^m}[x,y]$ with $\deg_{a,b}(g) = r$
	$g(x_i) \neq 0$	$g(x_i, y_i) \neq 0$
Codewords in $\mathcal{C}$	$\left(\frac{f}{g}(x_1), \ldots, \frac{f}{g}(x_n)\right)$	$\left(\frac{f}{g}(P_1), \ldots, \frac{f}{g}(P_n)\right)$
Goppa code $\mathcal{C}^{\perp}\vert_{\mathbb{F}_q}$	$\Gamma_r(\boldsymbol{x}, g)$	$\Gamma_r(\mathcal{P}, g)$
Family for McEliece	$\mathcal{F} = \{\Gamma_r(\begin{matrix}\boldsymbol{x}\\ \mathcal{P}\end{matrix}, g) \mid$ squarefree g, $\begin{matrix}\deg\\ \deg_{a,b}\end{matrix}(g) = r\}$	

Using Goppa–like AG codes can reduce the key size.

Level of security	n	k	$t = r$	Security bits	Key–Size(bit)
Category 1	3 488	2 720	64	143	2 088 960
Category 3	4 608	3 360	96	185	4 193 280
Category 5	6 688	5 024	128	263	8 359 936
	8 192	6 528	128	300	10 862 592

Table: McEliece cryptosystem based on **binary Goppa codes**

q	r	n	k	t	Security bits	Key–Size(bit)
11	266	1 320	898	77	153	1 136 868
13	313	2 188	1 718	77	198	2 422 380
16	355	4 078	3 608	56	199	6 783 040
13	491	2 189	1 363	166	270	3 377 514
16	461	4 080	3 398	109	313	9 269 744

Table: **Goppa–Like Hermitian codes** parameters $\Gamma_r(\mathcal{P}, g)$ over $\mathbb{F}_{q^2}$.

Hermitian curve $(a, b) = (q^{m/2}, q^{m/2} + 1)$**:** $y^{q^{m/2}} + y = x^{q^{m/2}+1}$. ($m$ even)

High–rate Goppa codes do not look so random...

High–rate Goppa codes do not look so random...

Dimension of the square of the dual of Goppa codes for $r \geq g-1$ (Morra & Tillich, 2021)

$$\dim(\Gamma_r(\boldsymbol{x},g)^{\perp})^{\star 2} \leq \underbrace{\binom{rm+1}{2}}_{\text{random code}} - \frac{m}{2} r\left((2e_\Gamma+1)r - 2(q-1)q^{e_\Gamma-1} - 1\right) \text{ with } e_\Gamma = \left\lfloor \log_q\left(\tfrac{r}{(q-1)^2}\right)+1 \right\rfloor.$$

The smallest distinguishable codes are very big compared to the ones used in Classic McEliece.

n	m	r	R	Largest distinguishable r	Corresponding R
3488	12	64	0.77982	12	0.95872
4608	13	96	0.72917	12	0.96615
6688	13	128	0.75120	15	0.97084
6960	13	119	0.77773	16	0.97011
8192	13	128	0.79688	19	0.96985

High–rate Goppa codes do not look so random...

Dimension of the square of the dual of Goppa codes for $r \geq q-1$ (Morra & Tillich, 2021)

$$\dim(\Gamma_r(\boldsymbol{x},g)^{\perp})^{\star 2} \leq \underbrace{\binom{rm+1}{2}}_{\text{random code}} - \frac{m}{2} r\left((2e_\Gamma+1)r - 2(q-1)q^{e_\Gamma-1} - 1\right) \text{ with } e_\Gamma = \left\lceil \log_q\left(\tfrac{r}{(q-1)^2}\right)+1 \right\rceil.$$

The smallest distinguishable codes are very big compared to the ones used in Classic McEliece.

n	m	r	R	Largest distinguishable r	Corresponding R
3488	12	64	0.77982	12	0.95872
4608	13	96	0.72917	12	0.96615
6688	13	128	0.75120	15	0.97084
6960	13	119	0.77773	16	0.97011
8192	13	128	0.79688	19	0.96985

Trace operator on $\mathbb{F}_{q^m}$

$$\mathrm{Tr}: \begin{cases} \mathbb{F}_{q^m} & \to & \mathbb{F}_q \\ x & \mapsto & \mathrm{Tr}(x) = x + x^q + \ldots + x^{q^{m-1}} \end{cases}$$

It extends to $\mathbb{F}_{q^m}^n$ by $\mathrm{Tr}(\boldsymbol{x}) = (\mathrm{Tr}(x_1), \ldots, \mathrm{Tr}(x_n))$.

Delsarte's theorem

$$\left(\mathcal{C}|_{\mathbb{F}_q}\right)^{\perp} = \mathrm{Tr}\,\mathcal{C}^{\perp}.$$

Dimension of trace code

$$\dim_{\mathbb{F}_q} \mathrm{Tr}\,(\mathcal{C}) \leq \min\{m \dim_{\mathbb{F}_q^m} \mathcal{C}, n\}.$$

$$\Gamma_r(\boldsymbol{x},g)^{\perp} = (\mathsf{GRS}_r(\boldsymbol{x}, g(\boldsymbol{x})^{-1})^{\perp}|_{\mathbb{F}_q})^{\perp} = \mathrm{Tr}\,\mathsf{GRS}_r(\boldsymbol{x}, g(x)^{-1}).$$

Gist: As GRS codes have a small square, so have their trace... **AG codes have the same issue.**

For any code $\mathcal{C}$ over $\mathbb{F}_{q^m}$, we have $\mathrm{Tr}(\mathcal{C})^{*2} \subseteq \sum_{i=0}^{\lfloor m/2 \rfloor} \mathrm{Tr}\left(\mathcal{C} \star \mathcal{C}^{q^i}\right)$ where $\mathcal{C}^{q^i} = \left\{(c_1^{q^i}, \ldots, c_n^{q^i}) \,|\, \boldsymbol{c} \in \mathcal{C}\right\}$.

For any code $\mathcal{C}$ over $\mathbb{F}_{q^m}$, we have $\mathrm{Tr}(\mathcal{C})^{*2} \subseteq \sum_{i=0}^{\lfloor m/2 \rfloor} \mathrm{Tr}\left(\mathcal{C} \star \mathcal{C}^{q^i}\right)$ where $\mathcal{C}^{q^i} = \left\{(c_1^{q^i}, \ldots, c_n^{q^i}) \,|\, \boldsymbol{c} \in \mathcal{C}\right\}$.

	Morra & Tillich's case	**Our case**
$\mathcal{C}$	$\mathsf{GRS}_r(\boldsymbol{x}, \boldsymbol{y}) = \left\{\left(\frac{f}{g}(x_i)\right) \mid \deg(f) < r\right\}$	$\mathcal{C}_r(\mathcal{P}, g) = \left\{\left(\frac{f}{g}(P_i)\right), \deg_{a,b}(f) < r\right\}$
$\mathcal{C} \star \mathcal{C}^{q^i}$ $\sim \mathrm{Span}\left\{\frac{f_1}{g}(\frac{f_2}{g})^{q^i}\right\}$	$\subseteq \mathsf{GRS}_{(r-1)(q^i+1)+1}(\boldsymbol{x}, \boldsymbol{y}^{q^i+1})$ $= \text{if } i \leq e = \lfloor \log_q(r) \rfloor$	
$\mathrm{Tr}\left(\mathcal{C} \star \mathcal{C}^{q^i}\right)$	$\mathrm{Tr}\left(\frac{f}{g^{q^i+1}}\right) = \mathrm{Tr}\left(\frac{f'}{g^{q^i+1}}\right)$ by *division* by $g^{q^i - q^{i-1}+1}$ $\deg f' < r(q^i - q^{i-1}+1) < (r-1)(q^i+1)+1$	
	$= T_i = \mathrm{Tr}\,\mathsf{GRS}_{r(q^i-q^{i-1}+1)}(\boldsymbol{x}, \boldsymbol{y}^{q^i+1})$ $T_0 \subseteq T_1 \subseteq \cdots \subseteq T_{\lfloor m/2 \rfloor}$	

For any code $\mathcal{C}$ over $\mathbb{F}_{q^m}$, we have $\mathrm{Tr}(\mathcal{C})^{*2} \subseteq \sum_{i=0}^{\lfloor m/2 \rfloor} \mathrm{Tr}\left(\mathcal{C} \star \mathcal{C}^{q^i}\right)$ where $\mathcal{C}^{q^i} = \left\{(c_1^{q^i}, \ldots, c_n^{q^i}) \,|\, \boldsymbol{c} \in \mathcal{C}\right\}$.

	Morra & Tillich's case	**Our case**
$\mathcal{C}$	$\mathrm{GRS}_r(\boldsymbol{x}, \boldsymbol{y}) = \left\{\left(\frac{f}{g}(x_i)\right) \mid \deg(f) < r\right\}$	$\mathcal{C}_r(\mathcal{P}, g) = \left\{\left(\frac{f}{g}(P_i)\right), \deg_{a,b}(f) < r\right\}$
$\mathcal{C} \star \mathcal{C}^{q^i}$ $\sim \mathrm{Span}\left\{\frac{f_1}{g}(\frac{f_2}{g})^{q^i}\right\}$	$\subseteq \mathrm{GRS}_{(r-1)(q^i+1)+1}(\boldsymbol{x}, \boldsymbol{y}^{q^i+1})$ $= \text{if } i \le e = \lfloor \log_q(r) \rfloor$	
$\mathrm{Tr}\left(\mathcal{C} \star \mathcal{C}^{q^i}\right)$	$\mathrm{Tr}\left(\frac{f}{g^{q^i+1}}\right) = \mathrm{Tr}\left(\frac{f'}{g^{q^i+1}}\right)$ by *division* by $g^{q^i - q^{i-1}+1}$ $\deg f' < r(q^i - q^{i-1}+1) < (r-1)(q^i+1)+1$	
	$= T_i = \mathrm{Tr}\,\mathrm{GRS}_{r(q^i-q^{i-1}+1)}(\boldsymbol{x}, \boldsymbol{y}^{q^i+1})$ $T_0 \subseteq T_1 \subseteq \cdots \subseteq T_{\lfloor m/2 \rfloor}$	

$$\dim\left(\mathrm{Tr}(\mathcal{C})^{*2}\right) \le \dim \sum_{i=0}^{\lfloor m/2 \rfloor} \mathrm{Tr}\left(\mathcal{C} \star \mathcal{C}^{q^i}\right) \le \dim T_e + \sum_{i=e+1}^{\lfloor m/2 \rfloor} \dim \mathrm{Tr}\left(\mathcal{C} \star \mathcal{C}^{q^i}\right) \text{ for any } e$$

$$\le mr(q^e - q^{e-1}+1) + \left(\frac{m-2}{2} - e\right) m(\dim \mathcal{C})^2$$

Minimizing with respect to e gives Mora–Tillich's bound.

For any code $\mathcal{C}$ over $\mathbb{F}_{q^m}$, we have $\mathrm{Tr}(\mathcal{C})^{*2} \subseteq \sum_{i=0}^{\lfloor m/2 \rfloor} \mathrm{Tr}\left(\mathcal{C} \star \mathcal{C}^{q^i}\right)$ where $\mathcal{C}^{q^i} = \left\{(c_1^{q^i}, \ldots, c_n^{q^i}) \,|\, \boldsymbol{c} \in \mathcal{C}\right\}$.

	Morra & Tillich's case	**Our case**
$\mathcal{C}$	$\mathrm{GRS}_r(\boldsymbol{x}, \boldsymbol{y}) = \left\{\left(\frac{f}{g}(x_i)\right) \mid \deg(f) < r\right\}$	$\mathcal{C}_r(\mathcal{P}, g) = \left\{\left(\frac{f}{g}(P_i)\right), \deg_{a,b}(f) < r\right\}$
$\mathcal{C} \star \mathcal{C}^{q^i}$ $\sim \mathrm{Span}\left\{\frac{f_1}{g}(\frac{f_2}{g})^{q^i}\right\}$	$\subseteq \mathrm{GRS}_{(r-1)(q^i+1)+1}(\boldsymbol{x}, \boldsymbol{y}^{q^i+1})$ $=$ if $i \le e = \lfloor \log_q(r) \rfloor$	$\subseteq \mathcal{C}_{(r-1)(q^i+1)+1}(\mathcal{P}, g)$ equality case hard to handle!
$\mathrm{Tr}\left(\mathcal{C} \star \mathcal{C}^{q^i}\right)$	$\mathrm{Tr}\left(\frac{f}{g^{q^i+1}}\right) = \mathrm{Tr}\left(\frac{f'}{g^{q^i+1}}\right)$ by *division* by $g^{q^i - q^{i-1}+1}$	
	$\deg f' < r(q^i - q^{i-1} + 1) < (r-1)(q^i+1)+1$	f' not so nice...(using Groebner basis)
	$= T_i = \mathrm{Tr}\,\mathrm{GRS}_{r(q^i - q^{i-1}+1)}(\boldsymbol{x}, \boldsymbol{y}^{q^i+1})$ $T_0 \subseteq T_1 \subseteq \cdots \subseteq T_{\lfloor m/2 \rfloor}$	Trickier!

$$\dim\left(\mathrm{Tr}(\mathcal{C})^{*2}\right) \le \dim \sum_{i=0}^{\lfloor m/2 \rfloor} \mathrm{Tr}\left(\mathcal{C} \star \mathcal{C}^{q^i}\right) \le \dim T_e + \sum_{i=e+1}^{\lfloor m/2 \rfloor} \dim \mathrm{Tr}\left(\mathcal{C} \star \mathcal{C}^{q^i}\right) \text{ for any } e$$

$$\le mr(q^e - q^{e-1} + 1) + \left(\frac{m-2}{2} - e\right) m(\dim \mathcal{C})^2$$

Minimizing with respect to e gives Mora–Tillich's bound.

Our results for one–point Goppa–like AG codes on $C_{a,b}$ curves

Theorem [El Khalfaoui, Lhotel, N., 2023]

Let $r \geq q+(a-1)(b-1)-1$ and $e^* := \min\left(\left\lfloor \frac{m}{2} \right\rfloor, \left\lceil \log_q\left(\frac{k^2}{r(q-1)^2}\right)\right\rceil + 1\right)$. Writing $k = \dim \mathcal{C}$, we have

$$\dim(\Gamma_r(\mathcal{P},g)^{\perp})^{\star 2} \leq \binom{mk+1}{2} - \frac{m}{2}(k^2(2e^*+1)+k-2r(q^{e^*}-q^{e^*-1}+1)).$$

Proposition [El Khalfaoui, Lhotel, N., 2023]

If $r \geq q+q^{m/2}(q^{m/2}-1)-1$, 1–point Goppa–like Hermitian codes $\Gamma_r(\mathcal{P},g)$ resist the distinguisher.

Our results for one–point Goppa–like AG codes on $C_{a,b}$ curves

Theorem [El Khalfaoui, Lhotel, N., 2023]

Let $r \geq q+(a-1)(b-1)-1$ and $e^* := \min\left(\left\lfloor \frac{m}{2} \right\rfloor, \left\lceil \log_q\left(\frac{k^2}{r(q-1)^2}\right)\right\rceil + 1\right)$. Writing $k = \dim \mathcal{C}$, we have

$$\dim(\Gamma_r(\mathcal{P},g)^{\perp})^{\star 2} \leq \binom{mk+1}{2} - \frac{m}{2}(k^2(2e^*+1)+k-2r(q^{e^*}-q^{e^*-1}+1)).$$

Proposition [El Khalfaoui, Lhotel, N., 2023]

If $r \geq q+q^{m/2}(q^{m/2}-1)-1$, 1–point Goppa–like Hermitian codes $\Gamma_r(\mathcal{P},g)$ resist the distinguisher.

Goppa–like AG codes appear to be **good candidates** to replace classical Goppa codes in order to reduce key size. Working on higher genus curves does not make these codes more likely to be distinguished by their Schur square or it of their dual.

We do not provide specifications for use in McEliece cryptosystem but our work indicates a *safe* area in which you can choose them if you want to work on the *large class of $C_{a,b}$ curves*.

Interesting research direction: Cartier codes.

Thank you for your attention!

Many thanks to the organizers and to all of the speakers for this great conference!