On the security of Some Compact Keys for McEliece Scheme

Élise Barelli

INRIA Saclay and LIX, CNRS UMR 7161 École Polytechnique,
91120 Palaiseau Cedex

Journées Codage et Cryptographie 2017

Problem

-> Let $\mathcal{F}$ be any family of linear codes.

-> Let G be a **random looking** generator matrix of a code $\mathcal{C} \in \mathcal{F}$.

From G, can we recover the structure of the code $\mathcal{C}$?

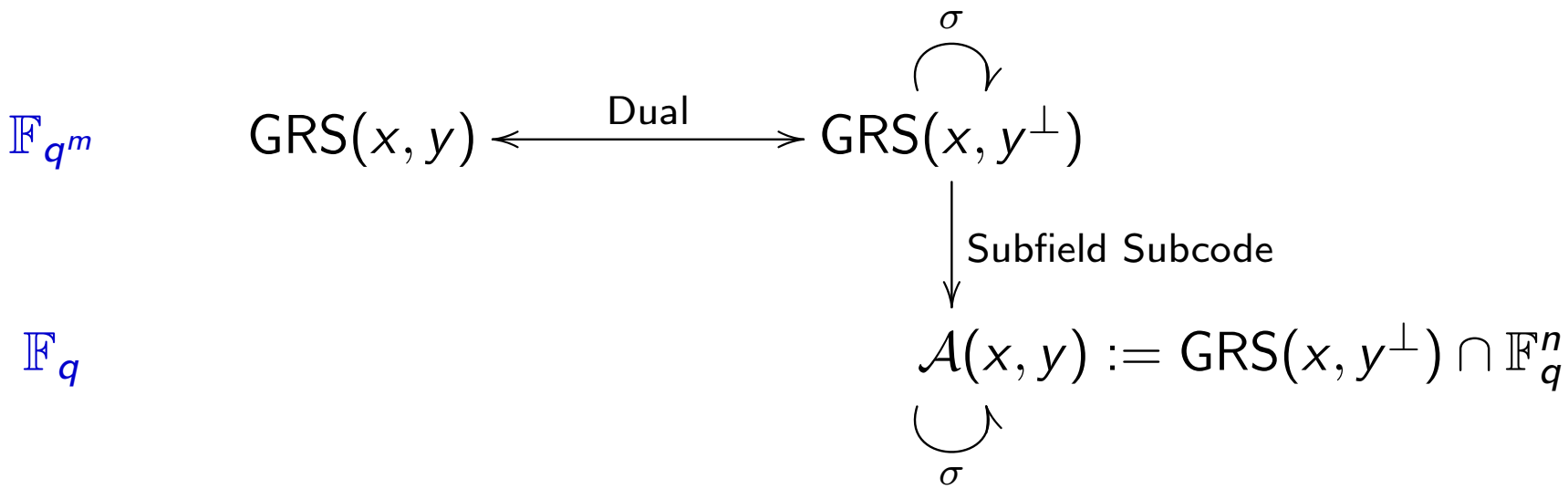
Here we consider the case where $\mathcal{F}$ is the family of **quasi-cyclic alternant codes**.

Quasi-cyclic alternant codes

Definition 1

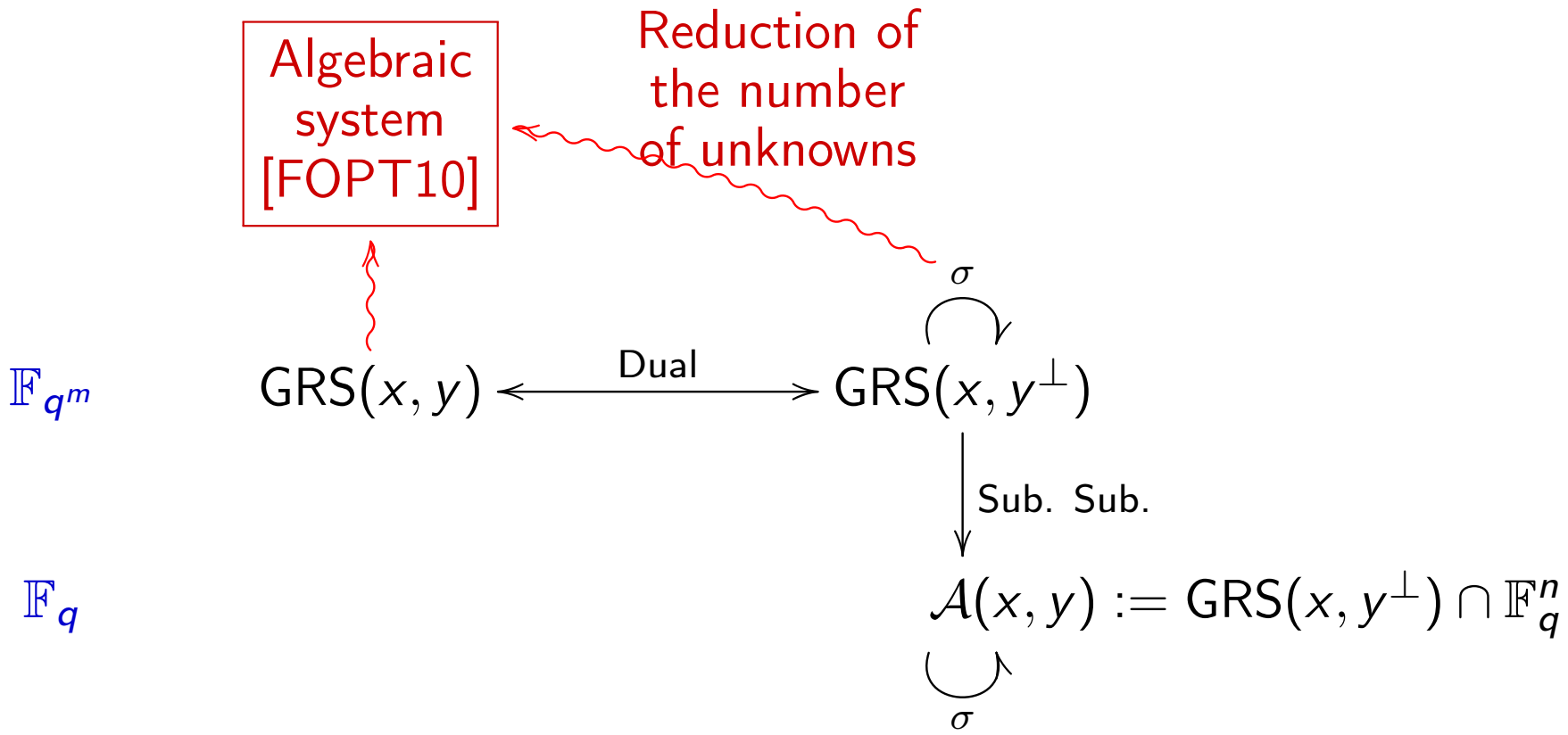
Let $x = (x_1, \ldots, x_n)$ be a n-tuple of distinct elements of $\mathbb{F}_{q^m}$, and $y = (y_1, \ldots, y_n)$ be an n-tuple of nonzero elements of $\mathbb{F}_{q^m}$,

$$\mathrm{GRS}_k(x, y) := \{(y_1 f(x_1), \ldots, y_n f(x_n)) \mid f \in \mathbb{F}_{q^m}[X]_{<k}\}.$$

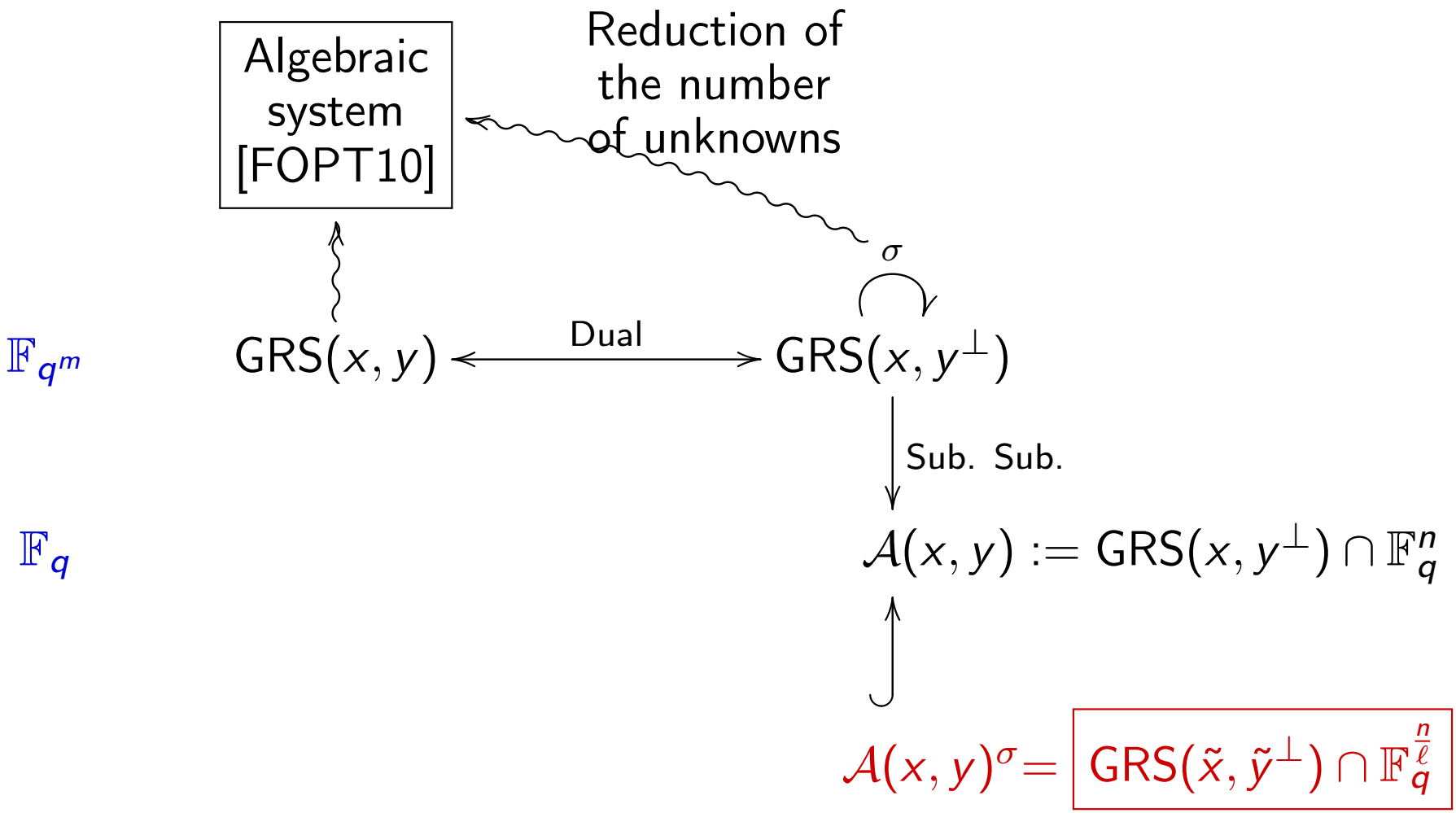


$\sigma \in Aut(\mathrm{GRS}(x, y^\perp))$

Algebraic attack



Contribution



1. Introduction

2. Quasi-cyclic Alternant Codes
   - Representation of $\mathcal{A}_k(x, y)$ as a subfield subcode of an AG code
   - Induced permutations of Alternant Codes

3. Invariant and Folded Codes
   - Definitions and properties
   - The Invariant Code of $\mathcal{A}_r(x, y)$

Functions on $\mathbb{P}^1$

We consider $\mathbb{P}^1$ the projective line over $\mathbb{F}_{q^m}$.

The function field over $\mathbb{F}_{q^m}$ of $\mathbb{P}^1$ is:

$$\mathbb{F}_{q^m}(\mathbb{P}^1) := \left\{ \frac{F(X,Y)}{G(X,Y)} \mid F, G \in \mathbb{F}_{q^m}[X,Y] \text{ homogeneous of same degree} \right\}.$$

Functions on $\mathbb{P}^1$

We consider $\mathbb{P}^1$ the projective line over $\mathbb{F}_{q^m}$.

The function field over $\mathbb{F}_{q^m}$ of $\mathbb{P}^1$ is:

$$\mathbb{F}_{q^m}(\mathbb{P}^1) := \left\{ \frac{F(X,Y)}{G(X,Y)} \mid F, G \in \mathbb{F}_{q^m}[X,Y] \text{ homogeneous of same degree} \right\}.$$

A divisor of $\mathbb{P}^1$ is a formal sum, with integers coefficients, of points of $\mathbb{P}^1$.

For $f \in \mathbb{F}_{q^m}(\mathbb{P}^1)$, the principal divisor of f, denoted by (f), is defined as the formal sum of zeros and poles of f, counted with multiplicity.

Functions on $\mathbb{P}^1$

We consider $\mathbb{P}^1$ the projective line over $\mathbb{F}_{q^m}$.

The function field over $\mathbb{F}_{q^m}$ of $\mathbb{P}^1$ is:

$$\mathbb{F}_{q^m}(\mathbb{P}^1) := \left\{ \frac{F(X,Y)}{G(X,Y)} \mid F, G \in \mathbb{F}_{q^m}[X,Y] \text{ homogeneous of same degree} \right\}.$$

A divisor of $\mathbb{P}^1$ is a formal sum, with integers coefficients, of points of $\mathbb{P}^1$.

For $f \in \mathbb{F}_{q^m}(\mathbb{P}^1)$, the principal divisor of f, denoted by (f), is defined as the formal sum of zeros and poles of f, counted with multiplicity.

We denote by $\mathcal{L}(G) := \{f \in \mathbb{F}_{q^m}(\mathbb{P}^1) \mid (f) \geq -G\} \cup \{0\}$ the Riemann-Roch space associated to a divisor G.

AG codes on $\mathbb{P}^1$

Let $\mathcal{P} = \{P_1, \ldots, P_n\}$ be a set of n distinct points of $\mathbb{P}^1_{\mathbb{F}_{q^m}}$ and G be a divisor, then the AG code $C_{\mathcal{L}}(\mathbb{P}^1, \mathcal{P}, G)$ is defined by:

$$C_{\mathcal{L}}(\mathbb{P}^1, \mathcal{P}, G) := \{\mathrm{Ev}_{\mathcal{P}}(f) \mid f \in \mathcal{L}(G)\}.$$

AG codes on $\mathbb{P}^1$

Let $\mathcal{P} = \{P_1, \ldots, P_n\}$ be a set of n distinct points of $\mathbb{P}^1_{\mathbb{F}_{q^m}}$ and G be a divisor, then the AG code $C_{\mathcal{L}}(\mathbb{P}^1, \mathcal{P}, G)$ is defined by:

$$C_{\mathcal{L}}(\mathbb{P}^1, \mathcal{P}, G) := \{\mathrm{Ev}_{\mathcal{P}}(f) \mid f \in \mathcal{L}(G)\}.$$

Let x and y be as previously, we define:

- $\mathcal{P} := \{(x_i : 1) |\ i \in \{1, \ldots, n\}\}$,
- $G := (k-1)P_\infty - (f)$,

with $f \in \mathbb{F}_{q^m}(\mathbb{P}^1)$ the function associated to the interpolation polynomial of $y_1, \ldots, y_n$ through the points $x_1, \ldots, x_n$.

Proposition 2

Then $GRS_k(x, y)$ is the AG code $C_{\mathcal{L}}(\mathbb{P}^1, \mathcal{P}, G)$ and:

$$\mathcal{A}_k(x, y) := C_{\mathcal{L}}(\mathbb{P}^1, \mathcal{P}, G)^{\perp} \cap \mathbb{F}_q^n.$$

Automorphim group of $\mathbb{P}^1$

$\mathrm{PGL}_2(\mathbb{F}_{q^m})$ is the automorphism group of the projective line $\mathbb{P}^1$ defined by:

$$\mathrm{PGL}_2(\mathbb{F}_{q^m}) := \left\{ \begin{array}{ccc} \mathbb{P}^1_{\mathbb{F}_{q^m}} & \to & \mathbb{P}^1_{\mathbb{F}_{q^m}} \\ (x:y) & \mapsto & (ax+by : cx+dy) \end{array} \middle| \begin{cases} a,b,c,d \in \mathbb{F}_{q^m}, \\ ad-bc \neq 0 \end{cases} \right\}.$$

Automorphim group of $\mathbb{P}^1$

$\mathrm{PGL}_2(\mathbb{F}_{q^m})$ is the automorphism group of the projective line $\mathbb{P}^1$ defined by:

$$\mathrm{PGL}_2(\mathbb{F}_{q^m}) := \left\{ \begin{array}{ccc} \mathbb{P}^1_{\mathbb{F}_{q^m}} & \to & \mathbb{P}^1_{\mathbb{F}_{q^m}} \\ (x:y) & \mapsto & (ax+by : cx+dy) \end{array} \middle| \begin{cases} a,b,c,d \in \mathbb{F}_{q^m}, \\ ad-bc \neq 0 \end{cases} \right\}.$$

Remark

The permutations of $\mathrm{PGL}_2(\mathbb{F}_{q^m})$ *have also a matrix representation, ie:*

$$\forall \sigma \in \mathrm{PGL}_2(\mathbb{F}_{q^m}), \text{ we write } \sigma := \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \text{ with } ad-bc \neq 0.$$

Where the elements a, b, c *and* d *are defined up to a multiplication by a nonzero scalar.*

Support and divisor σ-invariant

Let σ be an automorphism of $\mathbb{P}^1_{\mathbb{F}_{q^m}}$.

For a point $Q \in \mathbb{P}^1$, we denote $Orb_\sigma(Q) := \{\sigma^j(Q) \mid j \in \{1..\ell\}\}$.
We define the **support**:

$$\mathcal{P} := \coprod_{i=1}^{n/\ell} Orb_\sigma(Q_i), \tag{1}$$

where the points $Q_i \in \mathbb{P}^1_{\mathbb{F}_{q^m}}$ are pairwise distinct with trivial stabilizer subgroup.

Support and divisor σ-invariant

Let σ be an automorphism of $\mathbb{P}^1_{\mathbb{F}_{q^m}}$.

For a point $Q \in \mathbb{P}^1$, we denote $Orb_\sigma(Q) := \{\sigma^j(Q) \mid j \in \{1..\ell\}\}$.
We define the **support**:

$$\mathcal{P} := \coprod_{i=1}^{n/\ell} Orb_\sigma(Q_i), \tag{1}$$

where the points $Q_i \in \mathbb{P}^1_{\mathbb{F}_{q^m}}$ are pairwise distinct with trivial stabilizer subgroup.
We define the **divisor**:

$$G := t \sum_{j=1}^{\ell} \sigma^j(R), \tag{2}$$

with R a point of $\mathbb{P}^1_{\mathbb{F}_{q^m}}$, $t \in \mathbb{Z}$ and $\deg(G) = \ell t$.

Permutations of $\mathcal{A}_k(x, y)$

The automorphism σ of $\mathbb{P}^1$ induces a permutation $\tilde{\sigma}$ of $\mathcal{C} = \mathcal{C}_{\mathcal{L}}(\mathbb{P}^1, \mathcal{P}, G)$ defined by:

$$\begin{array}{rccc} \tilde{\sigma}: & \mathcal{C} & \longrightarrow & \mathcal{C} \\ & (f(P_1), \ldots, f(P_n)) & \longmapsto & (f(\sigma(P_1)), \ldots, f(\sigma(P_n))). \end{array}$$

Then $\tilde{\sigma}$ is also a permutation of $\mathcal{A} := \mathcal{C}^{\perp} \cap \mathbb{F}_q^n$.

Equivalence classes of $\mathrm{PGL}_2(\mathbb{F}_{q^m})$

Lemma 3

Let $\rho \in \mathrm{PGL}_2(\mathbb{F}_{q^m})$ be an automorphism on $\mathbb{P}^1$. Then $\sigma' := \rho \circ \sigma \circ \rho^{-1}$ induces the same permutation on $\mathcal{C}$ as σ.

Equivalence classes of $\mathrm{PGL}_2(\mathbb{F}_{q^m})$

Lemma 3

Let $\rho \in \mathrm{PGL}_2(\mathbb{F}_{q^m})$ be an automorphism on $\mathbb{P}^1$. Then $\sigma' := \rho \circ \sigma \circ \rho^{-1}$ induces the same permutation on $\mathcal{C}$ as σ.

Three cases are possible, depending on the eigenvalues of the matrix $M := Mat(\sigma)$:

1. $M \sim \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$, with $a \in \mathbb{F}_{q^m}$,
2. $M \sim \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$, with $b \in \mathbb{F}_{q^m}$,
3. $M \sim \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$, with $a \in \mathbb{F}_{q^{2m}}$.

Let $\mathcal{C}$ be a linear code and $\sigma \in \mathit{Perm}(\mathcal{C})$ of order ℓ. Consider:

$$\varphi : \mathcal{C} \to \mathcal{C}$$

$$c \mapsto \sum_{i=0}^{\ell-1} \sigma^i(c).$$

The *folded* code of $\mathcal{C}$ is defined by

$$\mathsf{Fold}_\sigma(\mathcal{C}) := \mathsf{Im}(\varphi)$$

and the *invariant* code of $\mathcal{C}$ is defined by

$$\mathcal{C}^\sigma := \ker(\sigma - \mathsf{Id}).$$

Let $\mathcal{C}$ be a linear code and $\sigma \in Perm(\mathcal{C})$ of order ℓ. Consider:

$$\varphi : \mathcal{C} \to \mathcal{C}$$

$$c \mapsto \sum_{i=0}^{\ell-1} \sigma^i(c).$$

The *folded* code of $\mathcal{C}$ is defined by

$$\mathrm{Fold}_\sigma(\mathcal{C}) := \mathrm{Im}(\varphi)$$

and the *invariant* code of $\mathcal{C}$ is defined by

$$\mathcal{C}^\sigma := \ker(\sigma - \mathrm{Id}).$$

Proposition 4

The codes $\mathrm{Fold}_\sigma(\mathcal{C})$ *and* $\mathcal{C}^\sigma$ *are subcodes of* $\mathcal{C}$ *and:*

$$\mathrm{Fold}_\sigma(\mathcal{C}) \subseteq \mathcal{C}^\sigma.$$

If Char $(\mathbb{F}_{q^m}) \nmid \ell$ *then* $\mathrm{Fold}_\sigma(\mathcal{C}) = \mathcal{C}^\sigma$.

If $\mathcal{C}$ is a linear code over $\mathbb{F}_{q^m}$, σ-invariant then:

$$(\mathcal{C} \cap \mathbb{F}_q^n)^\sigma = \{c \in \mathcal{C} \mid c \in \mathbb{F}_q^n \text{ and } \sigma(c) = c\} = \mathcal{C}^\sigma \cap \mathbb{F}_q^n.$$

If $\mathcal{C}$ is a linear code over $\mathbb{F}_{q^m}$, σ-invariant then:

$$(\mathcal{C} \cap \mathbb{F}_q^n)^\sigma = \{c \in \mathcal{C} \mid c \in \mathbb{F}_q^n \text{ and } \sigma(c) = c\} = \mathcal{C}^\sigma \cap \mathbb{F}_q^n.$$

Theorem 5

Let $\mathsf{GRS}(x, y) := \mathcal{C}_{\mathcal{L}}(\mathbb{P}^1, \mathcal{P}, G) \subseteq \mathbb{F}_{q^m}^n$ *be a* σ*-invariant AG code, with* $\sigma \in \mathsf{PGL}_2(\mathbb{P}^1_{\mathbb{F}_{q^m}})$ *of order* ℓ *and* $\mathcal{P}$ *and* G *defined as (1) and (2). Then the invariant code* $\mathsf{GRS}(x, y)^\sigma$ *is a GRS code of length* n/ℓ.

Corollary 6

The invariant code $\mathcal{A}(x, y)^\sigma$ *is an alternant code of length* n/ℓ.

Lemma 7

Let $c := Ev_{\mathcal{P}}(f) \in \mathcal{C}_{\mathcal{L}}(\mathbb{P}^1, \mathcal{P}, G)$ *such that* $\sigma(c) = c$, *then* f *is* σ*-invariant, ie:* $f \circ \sigma = f$.

Lemma 7

Let $c := Ev_{\mathcal{P}}(f) \in \mathcal{C}_{\mathcal{L}}(\mathbb{P}^1, \mathcal{P}, G)$ such that $\sigma(c) = c$, then f is σ-invariant, ie: $f \circ \sigma = f$.

Let $G := t \sum_{j=1}^{\ell} \sigma^j(R)$, with R a rational point of $\mathbb{P}^1_{\mathbb{F}_{q^m}}$ and $t \in \mathbb{Z}$. We denote:

$$\sigma^j(R) := (\gamma_j : \delta_j), \text{ for } j \in \{0, \ldots, \ell - 1\}.$$

Lemma 8

With the previous notation, any $f \in \mathcal{L}(G)$ can be written as:

$$f(X, Y) = \frac{F(X, Y)}{\prod_{j=0}^{\ell-1} (\delta_j X - \gamma_j Y)^t},$$

with $F \in \mathbb{F}_{q^m}[X, Y]$ a homogeneous polynomial of degree $t\ell$.

Case σ diagonalizable over $\mathbb{F}_{q^m}$:

$$\begin{array}{rccc} \sigma: & \mathbb{P}^1 & \to & \mathbb{P}^1 \\ & (X:Y) & \mapsto & (aX:Y), \end{array}$$

with $a \in \mathbb{F}_{q^m}$.

Case σ trigonalizable over $\mathbb{F}_{q^m}$:

$$\begin{array}{rccc} \sigma: & \mathbb{P}^1 & \to & \mathbb{P}^1 \\ & (X:Y) & \mapsto & (X+bY:Y) \end{array}$$

with $b \in \mathbb{F}_{q^m}^*$.

Case σ diagonalizable over $\mathbb{F}_{q^{2m}} \setminus \mathbb{F}_{q^m}$:

$$\begin{array}{rccc} \sigma: & \mathbb{P}^1 & \to & \mathbb{P}^1 \\ & (X:Y) & \mapsto & (aX:Y), \end{array}$$

with $a \in \mathbb{F}_{q^{2m}} \setminus \mathbb{F}_{q^m}$.

Case σ diagonalizable over $\mathbb{F}_{q^m}$

Proposition 9

If $F(aX, Y) = F(X, Y)$, then

$$F(X, Y) = R(X^\ell, Y^\ell)$$

with $R \in \mathbb{F}_{q^m}[X, Y]$ an homogeneous polynomial of degree t.

Case σ diagonalizable over $\mathbb{F}_{q^m}$

Proposition 9

If $F(aX, Y) = F(X, Y)$, then

$$F(X, Y) = R(X^\ell, Y^\ell)$$

with $R \in \mathbb{F}_{q^m}[X, Y]$ an homogeneous polynomial of degree t.

We denote $\sigma^j(P_i) := (\alpha_{i\ell+j} : \beta_{i\ell+j})$, for $i \in \{0, \ldots, \frac{n}{\ell} - 1\}$, $j \in \{0, \ldots, \ell - 1\}$.

Proposition 10

The code $(\mathcal{C}_{\mathcal{L}}(\mathbb{P}^1, \mathcal{P}, G))^\sigma$ is the GRS code $\mathcal{C}_{\mathcal{L}}(\mathbb{P}^1, \tilde{\mathcal{P}}, \tilde{G})$, with

- $\tilde{P}_i = (\alpha_i^\ell : \beta_i^\ell)$,
- $\tilde{G} = t\tilde{R}$, *where* $\tilde{R} = \left((-1)^{\ell-1} \prod_{j=0}^{\ell-1} \gamma_j : \prod_{j=0}^{\ell-1} \delta_j\right)$.

Case σ trigonalizable over $\mathbb{F}_{q^m}$

Proposition 11

If $F(X + bY, Y) = F(X, Y)$, *then*

$$F(X, Y) = R(X^p - b^{p-1}XY^{p-1}, Y^p)$$

with $R \in \mathbb{F}_q[X, Y]$ *a homogeneous polynomial of degree* t.

Proposition 12

The code $(\mathcal{C}_{\mathcal{L}}(\mathbb{P}^1, \mathcal{P}, G))^\sigma$ *is the GRS code* $\mathcal{C}_{\mathcal{L}}(\mathbb{P}^1, \tilde{\mathcal{P}}, \tilde{G})$, *with:*

- $\tilde{P}_i = (\alpha_i^p - b^{p-1}\alpha_i\beta_i^{p-1} : \beta_i^p)$,
- $\tilde{G} = t(\tilde{R})$, *where* $\tilde{R} = \left(\prod_{j=0}^{p-1} \gamma_j : \prod_{j=0}^{p-1} \delta_j\right)$.

Case σ diagonalizable over $\mathbb{F}_{q^{2m}} \backslash \mathbb{F}_{q^m}$

Idea

We extend the code $\mathcal{C}$ defined on $\mathbb{F}_{q^m}$ to the field $\mathbb{F}_{q^{2m}}$. We consider $\mathcal{C} \otimes \mathbb{F}_{q^{2m}} := \mathrm{Span}_{\mathbb{F}_{q^{2m}}} < \mathcal{C} >$, we have:

$$\mathcal{C} \otimes \mathbb{F}_{q^{2m}} = \{\mathrm{Ev}_{\mathcal{P}}(f) \mid f \in \mathcal{L}_{\mathbb{F}_{q^{2m}}}(G)\}.$$

Case σ diagonalizable over $\mathbb{F}_{q^{2m}} \backslash \mathbb{F}_{q^m}$

Idea

We extend the code $\mathcal{C}$ defined on $\mathbb{F}_{q^m}$ to the field $\mathbb{F}_{q^{2m}}$. We consider $\mathcal{C} \otimes \mathbb{F}_{q^{2m}} := \mathrm{Span}_{\mathbb{F}_{q^{2m}}} < \mathcal{C} >$, we have:

$$\mathcal{C} \otimes \mathbb{F}_{q^{2m}} = \{\mathrm{Ev}_{\mathcal{P}}(f) \mid f \in \mathcal{L}_{\mathbb{F}_{q^{2m}}}(G)\}.$$

$$\begin{array}{lccc} \mathbb{F}_{q^{2m}} & \mathcal{C} \otimes \mathbb{F}_{q^{2m}} & \xrightarrow{\mathrm{Inv}_\sigma} & (\mathcal{C} \otimes \mathbb{F}_{q^{2m}})^\sigma \\ & \mathrm{Sub.} \uparrow \quad \mathrm{Sub.} \uparrow & & \uparrow \\ \mathbb{F}_{q^m} & \mathcal{C} & \xrightarrow{\mathrm{Inv}_\sigma} & \mathcal{C}^\sigma \end{array}$$

Case σ diagonalizable over $\mathbb{F}_{q^{2m}} \setminus \mathbb{F}_{q^m}$

Idea

We extend the code $\mathcal{C}$ defined on $\mathbb{F}_{q^m}$ to the field $\mathbb{F}_{q^{2m}}$. We consider $\mathcal{C} \otimes \mathbb{F}_{q^{2m}} := \mathrm{Span}_{\mathbb{F}_{q^{2m}}} < \mathcal{C} >$, we have:

$$\mathcal{C} \otimes \mathbb{F}_{q^{2m}} = \{\mathrm{Ev}_{\mathcal{P}}(f) \mid f \in \mathcal{L}_{\mathbb{F}_{q^{2m}}}(G)\}.$$

$$\begin{array}{lccc} \mathbb{F}_{q^{2m}} & \mathcal{C} \otimes \mathbb{F}_{q^{2m}} & \xrightarrow{\mathrm{Inv}_\sigma} & (\mathcal{C} \otimes \mathbb{F}_{q^{2m}})^\sigma = \mathcal{C}_{\mathcal{L}}(\mathbb{P}^1, \tilde{\mathcal{P}}, \tilde{G})_{\mathbb{F}_{q^{2m}}} \\ & \text{Sub. Sub.} \uparrow & & \uparrow \\ \mathbb{F}_{q^m} & \mathcal{C} & \xrightarrow{\mathrm{Inv}_\sigma} & \mathcal{C}^\sigma \end{array}$$

Case σ diagonalizable over $\mathbb{F}_{q^{2m}} \setminus \mathbb{F}_{q^m}$

-> $\mathcal{C} \otimes \mathbb{F}_{q^{2m}}$ has a base in $\mathbb{F}_{q^m}^n$.

-> Here $p \nmid \ell$ then $\mathrm{Fold}_\sigma(\mathcal{C}) = \mathcal{C}^\sigma$. So $(\mathcal{C} \otimes \mathbb{F}_{q^{2m}})^\sigma$ has also a base in $\mathbb{F}_{q^m}^n$.

$$\begin{array}{lccc} \mathbb{F}_{q^{2m}} & \mathcal{C} \otimes \mathbb{F}_{q^{2m}} & \xrightarrow{\mathrm{Inv}_\sigma} & (\mathcal{C} \otimes \mathbb{F}_{q^{2m}})^\sigma = \mathcal{C}_{\mathcal{L}}(\mathbb{P}^1, \tilde{\mathcal{P}}, \tilde{G})_{\mathbb{F}_{q^{2m}}} \\ & \text{Sub.} \uparrow \quad \text{Sub.} & & \uparrow \\ \mathbb{F}_{q^m} & \mathcal{C} & \xrightarrow{\mathrm{Inv}_\sigma} & \mathcal{C}^\sigma \end{array}$$

Case σ diagonalizable over $\mathbb{F}_{q^{2m}} \setminus \mathbb{F}_{q^m}$

-> $\mathcal{C} \otimes \mathbb{F}_{q^{2m}}$ has a base in $\mathbb{F}_{q^m}^n$.

-> Here $p \nmid \ell$ then $\mathrm{Fold}_\sigma(\mathcal{C}) = \mathcal{C}^\sigma$. So $(\mathcal{C} \otimes \mathbb{F}_{q^{2m}})^\sigma$ has also a base in $\mathbb{F}_{q^m}^n$.

$$\begin{array}{lccc} \mathbb{F}_{q^{2m}} & \mathcal{C} \otimes \mathbb{F}_{q^{2m}} & \xrightarrow{\mathrm{Inv}_\sigma} & (\mathcal{C} \otimes \mathbb{F}_{q^{2m}})^\sigma = \mathcal{C}_{\mathcal{L}}(\mathbb{P}^1, \tilde{\mathcal{P}}, \tilde{G})_{\mathbb{F}_{q^{2m}}} \\ & \text{Sub. } \uparrow \text{ Sub.} & & \uparrow \text{ Sub.} \\ \mathbb{F}_{q^m} & \mathcal{C} & \xrightarrow{\mathrm{Inv}_\sigma} & \mathcal{C}^\sigma = \mathcal{C}_{\mathcal{L}}(\mathbb{P}^1, \tilde{\mathcal{P}}, \tilde{G}) \end{array}$$

Conclusion

Results:

- The invariant code of a quasi-cyclic GRS code is a GRS code.
- The security of alternant codes with induced permutation from the projective linear group, is reduced to the security of the invariant code which is an alternant code.

Conclusion

Results:

- The invariant code of a quasi-cyclic GRS code is a GRS code.
- The security of alternant codes with induced permutation from the projective linear group, is reduced to the security of the invariant code which is an alternant code.

Works in progress:

- Security of AG codes on cyclic cover of the projective line.
- Security of AG codes on cyclic covers of plane curves of genus > 0.

Thank you!