ERROR-CORRECTING PAIRS AND ARRAYS FROM ALGEBRAIC GEOMETRY CODES

I. MÁRQUEZ-CORBELLA 1  R. PELLIKAAN 2

1 Department of Algebra, Geometry and Topology, University of Valladolid. Supported by a FPU grant AP2008-01598 by Spanish MEC.

2 Department of Mathematics and Computing Science, Eindhoven University of Technology.

Applications of Computer Algebra - ACA 2013
**Introduction to Coding Theory**

- An $[n, k]$ linear code $C$ over $\mathbb{F}_q$ is a $k$-dimensional subspace of $\mathbb{F}^n_q$.
  - Its size is $M = q^k$, the information rate is $R = \frac{k}{n}$ and the redundancy is $n - k$.
- The generator matrix of $C$ is a $k \times n$ matrix $G$ whose rows form a basis of $C$, i.e.
  \[
  C = \left\{ xG \mid x \in \mathbb{F}_q^k \right\}.
  \]
- The parity-check matrix of $C$ is an $(n - k) \times n$ matrix $H$ whose nullspace is generated by the codewords of $C$, i.e.
  \[
  C = \left\{ y \in \mathbb{F}_q^n \mid Hy^T = 0 \right\}.
  \]
- The hamming distance between $x, y \in \mathbb{F}^n_q$ is $d_H(x, y) = |\{i \mid x_i \neq y_i\}|$.
- The minimum distance of $C$ is
  \[
  d(C) = \min \left\{ d_H(c_1, c_2) \mid c_1, c_2 \in C \text{ and } c_1 \neq c_2 \right\}.
  \]
Public-Key Cryptosystems

Two keys:
- **Private Key**: Known only by the recipient.
- **Public Key**: Available to anyone.

Most PKC are based on number-theoretic problems

- Quantum computers will break the most popular PKCs: RSA, DSA, ECDSA, ECC, HECC, ...
- Can be attacked in polynomial time using Shor's algorithm.

Good news: Post-quantum cryptography

- Hash-based cryptography,
- Code-based cryptography,
- Lattice-based cryptography,
- Multivariate-quadratic-equation cryptography

**McEliece Cryptosystem**

**Key Generation**

1. Given:
   - \( C \) an \([n, k, d]\) linear code over \( \mathbb{F}_q \)
   - \( G \in \mathbb{F}_q^{k \times n} \) a generator matrix of \( C \)
   - \( S \in \mathbb{F}_q^{k \times k} \) a nonsingular matrix.
   - \( P \in \mathbb{F}_q^{n \times n} \) a permutation matrix.

2. McEliece Public Key: \((G' = SGP, t)\).

3. McEliece Private Key: \((G, S, P)\).

**Encryption**

Encrypt a message \( m \in \mathbb{F}_q^k \) as

\[
y' = mG' + e'
\]

where \( e \) and \( e' = eP \) in \( \mathbb{F}_q^n \) are random error vectors of weight \( t \).

**Decryption**

1. Compute \( y = y'P^{-1} = mG'P^{-1} + e'P^{-1} = mSG + e \).
2. Apply the decoding algorithm for \( C \) to find \( mS \).
3. \( m = mSS^{-1} \).

- McEliece introduced the first PKC based on Error-Correcting Codes in 1978.
- **Advantages:**
  1. Interesting candidate for post-quantum cryptography.
  2. Fast encryption (matrix-vector multiplication) and decryption functions.
- **Drawback:** Large key size.

R. J. McEliece.

*A public-key cryptosystem based on algebraic coding theory.*

Most effective attack against the McEliece cryptosystem is **Information Set Decoding**. Many variants:

1. McEliece (1978)
2. Leon (1988)
3. Lee and Brickell (1988)
5. van Tilburg (1990)

**A. Canteaut and H. Chabanne.**

*A further improvement of the work factor in an attempt at breaking McEliece’s cryptosystem.*


**A. Canteaut and F. Chabaud.**

*A new algorithm for finding minimum-weight words in a linear code: application to McEliece’s cryptosystem and to narrow-sense BCH codes of length 511.*

IEEE Transaction on Information Theory.

**A. Canteaut and N. Sendrier.**

*Cryptanalysis of the original McEliece cryptosystem.*

Advances in cryptology - ASIACRYPT’98.

**P. J. Lee and E. F. Brickell.**

*An observation on the security of McEliece’s public-key cryptosystem.*

Advances in cryptology - EUROCRYPT’98.

**A. Becker, J. S. Coron and A. Joux**

*Improved generic algorithms for hard knapsacks.*

Advances in cryptology - EUROCRYPT 2011.
Niederreiter Cryptosystem

Niederreiter presents a dual version of McEliece cryptosystem in 1986 which is equivalent in terms of security, with the same Goppa codes.

**Key Generation**

1. **Given:**
   - \( C \) an \([n, k, d]\) linear code over \( \mathbb{F}_q \)
   - \( H \in \mathbb{F}_q^{(n-k) \times n} \) a parity check matrix of \( C \).
   - \( S \in \mathbb{F}_q^{(n-k) \times (n-k)} \) a nonsingular matrix.
   - \( P \in \mathbb{F}_q^{n \times n} \) a permutation matrix.

2. **Niederreiter Public Key:**
   \( (H' = SHP, t) \).

3. **Niederreiter Private Key:** \( (H, S, P) \)

**Encryption**

Encrypt a message \( m \in \mathbb{F}_q^k \) as

\[
y' = mH'^T.
\]

**Decryption**

1. Compute \( y = y' = (S^{-1})^T = mP^T H^T = m'H^T \). Syndrome of \( m' \) by \( H \).

2. Apply decoding algorithm for \( C \) to find \( m' = mP^T \) and thereby \( m \).

In its original paper Niederreiter proposed the class of GRS codes over \( \mathbb{F}_{2^m} \).

---

**References**

H. Niederreiter.
Knapsack-type crypto system and algebraic coding theory.
Problems of Control and Information Theory, 1986.

Y. Xing Li, R. H. Deng and X. Mei Wang.
On the equivalence of McEliece’s and Niederreiter public-key cryptosystems.
For all $a, b \in F_q^n$ we define:

- **Star Multiplication**: $a \ast b = (a_1 b_1, \ldots, a_n b_n) \in F_q^n$.
- **Standard Inner Multiplication**: $a \cdot b = \sum_{i=1}^{n} a_i b_i$.

For all subsets $A, B \subseteq F_q^n$ we define:

- $A \ast B = \{a \ast b \mid a \in A \text{ and } b \in B\}$.
- $A \perp B \iff a \cdot b = 0 \quad \forall a \in A \text{ and } b \in B$. 
Let $C$ be an $\mathbb{F}_q$ linear code of length $n$. The pair $(A, B)$ of $\mathbb{F}_{q^m}$-linear codes of length $n$ is a $t$-ECP for $C$ over $\mathbb{F}_{q^m}$ if the following properties hold:

1. $(A \ast B) \perp C$.
2. $k(A) > t$.
3. $d(B^\perp) > t$.
4. $d(A) + d(C) > n$.

An $[n, k]$ code which has a $t$-ECP over $\mathbb{F}_{q^m}$ has a decoding algorithm with complexity $\mathcal{O}((nm)^3)$.

R. Pellikaan

*On decoding by error location and dependent sets of error positions.*

R. Kötter.

*A unified description of an error locating procedure for linear codes.*
Motivation

“At the heart of any public-key cryptosystem is a one-way function - a function \( y = f(x) \) that is easy to evaluate but for which is computationally infeasible (one hopes) to find the inverse \( x = f^{-1}(y) \).”

N. Koblitz, A. Menezes.  
*The brave new world of bodacious assumptions in cryptography.*  

Let \( C_t \) the class of linear codes over \( \mathbb{F}_q \) that have a \( t \)-ECP over an extension of \( \mathbb{F}_q \).

- This family have an **efficient decoding algorithm** \( \Rightarrow \) they are appropriate for code-based cryptography.
- Most families of codes used in code-based cryptography belongs to \( C_t \). (Like GRS codes, Goppa codes, AG codes ...
- We proposed to use the subclass of \( C_t \) formed by those linear codes \( C \) whose error correcting pair is not easily reconstructed from \( C \), i.e. we consider the following one way function:

\[
\mathbf{x} = (A, B) \quad \mapsto \quad \mathbf{y} = A \ast B,
\]

where \((A, B)\) is a \( t \)-ECP.
Let

- $C$ be an $\mathbb{F}_q$-linear code of length $n$.
- $A$ and $B$ be linear subspaces of $\mathbb{F}_q^n$.
- $y \in \mathbb{F}_q^n$ be the received word with error vector $e \rightarrow y = c + e$ for some $c \in C$.

Define:

$$K_y = \{ a \in A \mid \langle y, a \rangle = 0, \text{ for all } b \in B \}$$

**Lemma 1:**

If $A \ast B \subseteq C^\perp \implies K_y = K_e$

Let $J$ be a subset of $\{1, \ldots, n\}$, define:

$$A(J) = \{ a \in A \mid a_j = 0, \text{ for all } j \in J \}$$

**Lemma 2:**

If $(A \ast B) \perp C$ and $I = \text{supp}(e) \implies A(I) \subseteq K_y$.

Moreover, if $d(B^\perp) > w_H(e) \implies A(I) = K_y$.

**Lemma 3:**

If $k(A) > t \geq w_H(e)$ and $I = \text{supp}(e) \implies \exists a \in A(I) \setminus \{0\}$.
Algorithm to find the error positions II

**Lemma 4:**

If $d(A) + d(C) > n \implies \forall a \in A : |J| = n - |\text{supp}(a)| \leq d(C) - 1$

Moreover, if $d(B^\perp) > t \geq w_H(e) \implies l = \text{supp}(e) \subseteq J$

1. Compute:
   
   $$K_y = \{a \in A \mid \langle y, a \ast b \rangle = 0, \text{ for all } b \in B\}$$

   Find the zero space of a set of linear equations over $\mathbb{F}_{q^m}$

2. If $K_y = 0 \implies$ The received word has more than $t$ errors
   
   Else take a nonzero $a \in K_y \subseteq A(l)$ and define $J = \{j \mid a_j = 0\}$

3. Find $e \in \mathbb{F}_q^n$ by solving the following linear equation (which has a unique solution):
   
   $$Hx^T = Hy^T \text{ such that } x_j = 0 \text{ for } j \in J$$

   Solve linear equations over $\mathbb{F}_q$

**Complexity:** $\sim \mathcal{O}((nm)^3)$
Let
\begin{itemize}
  \item \( \mathbf{a} = (a_1, \ldots, a_n) \) be an \( n \)-tuple of mutually distinct elements of \( \mathbb{F}_q \).
  \item \( \mathbf{b} = (b_1, \ldots, b_n) \) be an \( n \)-tuple of nonzero elements of \( \mathbb{F}_q \).
\end{itemize}

The GRS code \( \text{GRS}_k(\mathbf{a}, \mathbf{b}) \) is defined by:
\[
\text{GRS}_k(\mathbf{a}, \mathbf{b}) = \{ \text{ev}_{\mathbf{a}, \mathbf{b}}(f(X)) = (f(a_1)b_1, \ldots, f(a_n)b_n) \mid f \in \mathbb{F}_q[X] \text{ and } \deg(f) < k \}
\]

**Parameters of \( \text{GRS}_k(\mathbf{a}, \mathbf{b}) \)**

The \( \text{GRS}_k(\mathbf{a}, \mathbf{b}) \) is an MDS code with parameters \([n, k, n - k + 1]\).

\( \rightarrow \) A generator matrix of \( \text{GRS}_k(\mathbf{a}, \mathbf{b}) \) is given by

\[
G_{\mathbf{a}, \mathbf{b}} = \begin{pmatrix}
  b_1 & \cdots & b_n \\
  b_1 a_1 & \cdots & b_n a_n \\
  \vdots & \ddots & \vdots \\
  b_1 a_1^{k-1} & \cdots & b_n a_n^{k-1}
\end{pmatrix} \in \mathbb{F}_q^{k \times n}
\]
\textbf{t-ECP for GRS}

Note that: \( \text{ev}_{a,b} (f(X)) \ast \text{ev}_{a,c} (g(X)) = \text{ev}_{a,b} (f(X)g(X)) \ast c \). Therefore:

\[ \text{GRS}_k(a, b) \ast \text{GRS}_l(a, c) = \text{GRS}_{k+l-1}(a, b \ast c) \]

Let

\[ A = \text{GRS}_{t+1}(a, b_1), \quad B = \text{GRS}_t(a, b_2) \quad \text{and} \quad C = \text{GRS}_{2t}(a, b_1 \ast b_2)^\bot \]

then \( (A, B) \) is a \( t \)-ECP for \( C \).

Conversely, let \( C = \text{GRS}_{n-2t}(a, b) \) then

\[ A = \text{GRS}_{t+1}(a, b') \quad \text{and} \quad B = \text{GRS}_t(a, 1) \]

is a \( t \)-ECP for \( C \) where \( b' \in (\mathbb{F}_q \setminus \{0\})^n \) verifies that

\[ C^\bot = \text{GRS}_{n-2t}(a, b)^\bot = \text{GRS}_{2t}(a, b'). \]

Moreover an \([n, n - 2t, 2t + 1]\) code that has a \( t \)-ECP is a GRS code.
The class of GRS codes was proposed by Niederreiter for code-based PKC.

Sidelnikov and Shestakov introduced an algorithm that breaks the original Niederreiter cryptosystem in polynomial time.

V. M. Sidelnikov and S. O. Shestakov.

On insecurity of cryptosystems based on generalized Reed-Solomon codes.

Discrete mathematics and Applications.
**Subcodes**

Let:

- $\mathcal{D}$ be a code that has $(A, B)$ as $t$-ECP.
- $\mathcal{C}$ be a subcode of $\mathcal{D}$

Then $(A, B)$ is also a $t$-ECP for $\mathcal{C}$.

The class of subcodes of GRS codes was proposed by Berger-Loidreau for code-based PKC to resist Sidelnikov-Shestakov attack.

For certain parameters, this proposal is not secure.

T. Berger and P. Loidreau.
*How to mask the structure of codes for a cryptographic use.*

I. Márquez-Corbella, E. Martínez-Moro and R. Pellikaan.
The non-gap sequence of a subcode of a generalized Reed-Solomon code.

C. Wieschebrink.
*An attack on the modified Niederreiter encryption scheme.*

C. Wieschebrink.
*Cryptoanalysis of the Niederreiter public key scheme based on GRS subcodes.*
Let:
- \( \mathcal{X} \) be an algebraic curve of genus \( g \) defined over the finite field \( \mathbb{F}_q \),
- \( P = (P_1, \ldots, P_n) \) be an \( n \)-tuple of distinct \( \mathbb{F}_q \)-rational points on \( \mathcal{X} \),
- \( E \) be a divisor of \( \mathcal{X} \) with \( \text{supp}(E) \cap P = \emptyset \) and \( \deg(E) = m \).

### Space of Rational Functions Associated to \( E \)

The space of rational functions associated to \( E \) is

\[
L(E) = \{ f \in \mathbb{F}_q(\mathcal{X}) \mid f = 0 \text{ or } (f) + E \geq 0 \}
\]

Since \( \text{supp}(E) \cap P = \emptyset \) the following evaluation map is well defined:

\[
\text{ev}_P : \quad L(E) \quad \longrightarrow \quad \mathbb{F}_q^n
\]

\[
f \quad \longmapsto \quad \text{ev}_P(f) = (f(P_1), \ldots, f(P_n))
\]

### Riemman-Roch Theorem

\[
\dim L(E) \geq m + 1 - g.
\]

Furthermore if \( m > 2g - 2 \) then \( \dim L(E) = m + 1 - g \).
Algebraic geometry codes

Algebraic Geometry codes (AG codes)

The AG code associated to $\mathcal{X}, P = (P_1, \ldots, P_n)$ and $E$ is

$$C_L(\mathcal{X}, P, E) = \{ev_P(f) \mid f \in L(E)\}$$

Theorem: Parameters of an AG code

If $n > m$ then $C_L(\mathcal{X}, P, E)$ is an $[n, k, d]$ code over $\mathbb{F}_q$ where

$$k \geq m + 1 - g \quad \text{and} \quad d \geq n - m$$

Moreover, if $m > 2g - 2$ then $k = m + 1 - g$.

\[ G = \begin{pmatrix}
  f_1(P_1) & \ldots & f_1(P_n) \\
  \vdots & \ddots & \vdots \\
  f_k(P_1) & \ldots & f_k(P_n)
\end{pmatrix} \in \mathbb{F}_q^{k \times n} \]

is a generator matrix of the code $C_L(\mathcal{X}, P, E)$
Let $F$ and $G$ be divisors of $\mathcal{X}$. Then there is a well defined linear map:

$$L(E) \otimes L(G) \rightarrow L(F + G)$$

$$f \otimes g \mapsto fg$$

Hence:

$$C_L(\mathcal{X}, \mathcal{P}, F) \ast C_L(\mathcal{X}, \mathcal{P}, G) \subseteq C_L(\mathcal{X}, \mathcal{P}, F + G)$$

Let $C = C_L(\mathcal{X}, \mathcal{P}, E)^\perp$ and choose a divisor $F$ with disjoint support from $\mathcal{P}$, then:

$$A = C_L(\mathcal{X}, \mathcal{P}, E) \quad \text{and} \quad B = C_L(\mathcal{X}, \mathcal{P}, E - F)$$

is a $t$-ECP for $C$. 
**t-ECP for AG codes II**

**Proposition: [Pellikaan (1989)]**

An AG code on a curve of genus $g$ with designed minimum distance $d$ has a $t$-ECP over $\mathbb{F}_q$ with

$$t = \left\lfloor \frac{d - 1 - g}{2} \right\rfloor$$

**Proposition: [Pellikaan (1996)]**

If $m$ is sufficiently large then an AG code with designed minimum distance $d$ has a $t$-ECP over $\mathbb{F}_{q^m}$ where

$$t = \left\lfloor \frac{d - 1}{2} \right\rfloor$$

- With **ECPs** we do not have a constructive decoding scheme
- **BUT** an **Error-correcting array** gives a decoding algorithm that decodes up to

$$\left\lfloor \frac{d^* - 1}{2} \right\rfloor$$

where $d^* = $ Feng-Rao designed minimum distance

with complexity $\mathcal{O}(n^3) \implies$ **Majority coset decoding**
In 1996 Janwa and Moreno propose to use AG codes for the McEliece cryptosystem.

This system was broken for:

1. Codes on curves of genus $g = 0$ by the Sidelnikov-Shestakov attack.

   GRS codes are Algebraic Geometry codes on the projective line.

2. Codes on curves of genus $g \leq 2$ by Faure and Minder.

3. VSAG are not secure for McEliece cryptosystem by M-Martínez-Pellikaan-Ruano

Very Strong Algebraic-Geometric (VSAG) codes

A code $C$ has a VSAG representation if $C = C_{\mathcal{X}}(P, E)$ where the curve $\mathcal{X}$ has genus $g$, $P$ consists of $n$ points and $E$ has degree $m$ such that

$$2g + 2 < m < \frac{1}{2}n \quad \text{or} \quad \frac{1}{2}n + 2g - 2 < m < n - 4$$

C. Faure and L. Minder.

Cryptanalysis of the McEliece cryptosystem over hyperelliptic codes.

H. Janwa and O. Moreno.

McEliece public crypto system using algebraic-geometric codes.
Designs, Codes and Cryptography, 1996.

I. Márquez-Corbella, E. Martínez-Moro and R. Pellikaan.

On the unique representation of very strong algebraic geometry codes.
Designs, Codes and Cryptography, 2013.

I. Márquez-Corbella, E. Martínez-Moro, R. Pellikaan and D. Ruano.

Computational aspects of retrieving a representation of an algebraic geometry code.
Submitted to Designs, Codes and Cryptography.
Let

- \( \mathbf{a} = (a_1, \ldots, a_n) \) be an \( n \)-tuple of **mutually distinct** elements of \( \mathbb{F}_{q^m} \).
- \( \mathbf{b} = (b_1, \ldots, b_n) \) be an \( n \)-tuple of **nonzero** elements of \( \mathbb{F}_{q^m} \).

\( \rightarrow \) \( \text{GRS}_k(\mathbf{a}, \mathbf{b}) \) be the GRS code over \( \mathbb{F}_{q^m} \) of dimension \( k \).

**The alternant code** \( \text{Alt}_r(\mathbf{a}, \mathbf{b}) \) is the \( F_q \)-linear restriction:

\[
\text{Alt}_r(\mathbf{a}, \mathbf{b}) = \mathbb{F}_q^n \cap (\text{GRS}_r(\mathbf{a}, \mathbf{b}))^\perp
\]

**Parameters of** \( \text{Alt}_r(\mathbf{a}, \mathbf{b}) \)

The \( \text{Alt}_r(\mathbf{a}, \mathbf{b}) \) has parameters \([n, k, d]_q\) with:

\[
k \geq n - mr \quad \text{and} \quad d \geq r + 1
\]

Every \([n, k, d]\) linear code with \( d \geq 2 \) is an **alternant code**!
**t-ECP for Alternant codes**

Let $C = \text{Alt}_{2t}(a, b)$. Then:

$$d(C) \geq 2t + 1 \quad \text{and} \quad C \subseteq (\text{GRS}_{2t+1}(a, b))^\perp$$

Let

$$A = \text{GRS}_{t+1}(a, 1), \quad \text{and} \quad B = \text{GRS}_t(a, b)$$

then $(A, B)$ is a $t$-ECP over $\mathbb{F}_{q^m}$ for $C$.

No known structural attacks against code-base PKC using Alternant codes
Let
- \( \mathbf{a} = (a_1, \ldots, a_n) \) be an \( n \)-tuple of \textbf{mutually distinct} elements of \( \mathbb{F}_{q^m} \).
- \( g \) be a polynomial \textbf{with coefficients} in \( \mathbb{F}_{q^m} \) such that
  \[ g(a_j) \neq 0 \text{ for all } j = 1, \ldots, n \]

The **Goppa code** \( \Gamma(\mathbf{a}, g) \) is the \( \mathbb{F}_q \)-linear code defined by:

\[
\Gamma(\mathbf{a}, g) = \left\{ \mathbf{c} \in \mathbb{F}_q^n \mid \sum_{j=1}^{n} \frac{c_j}{X-a_j} \equiv 0 \pmod{g(X)} \right\}
\]

**Goppa Codes are Alternant Codes**

Let
- \( \mathbf{a} = (a_1, \ldots, a_n) \) be an \( n \)-tuple of \textbf{mutually distinct} elements of \( \mathbb{F}_{q^m} \).
- \( g \) be a **Goppa polynomial** of degree \( r \).
- \( \mathbf{b} = (b_1, \ldots, b_n) \) be an \( n \)-tuple of \textbf{nonzero} elements of \( \mathbb{F}_{q^m} \) such that
  \[ b_j = \frac{1}{g(a_j)} \]

Then: \( \Gamma(\mathbf{a}, g) = \text{Alt}_r(\mathbf{a}, \mathbf{b}) \implies \text{it has an } \left\lfloor \frac{r}{2} \right\rfloor \text{-ECP} \)
Let:
- \( a = (a_1, \ldots, a_n) \) be an \( n \)-tuple of \textbf{mutually distinct} elements of \( \mathbb{F}_{2m} \).
- \( g \) be a Goppa polynomial with coefficients in \( \mathbb{F}_{2m} \) of \textbf{degree} \( r \).
- \( \rightarrow \) And suppose moreover that \( g \) has \textbf{no square factor}.

Then:
1. \( \Gamma(a, g) = \Gamma(a, g^2) \).
2. \( \Gamma(a, g) \) has parameters \([n, k, d]\) with
   \[
   k \geq n - mr \quad \text{and} \quad d \geq 2r + 1
   \]
   \( \Gamma(a, g) \) has an \( r \)-ECP
Let

- \( n = q^m - 1 \)
- \( \alpha \) be a primitive element of \( \mathbb{F}^*_m \)
- \( m_i(X) \) be the minimal polynomial of \( \alpha^i \)

The **primitive narrow-sense BCH code** over \( \mathbb{F}_q \) of length \( n \) and distance at least \( d \) is the **cyclic code** with generator polynomial:

\[
g(X) = \text{lcm}(m_1(X), \ldots, m_{d-1}(X))
\]

### BCH Codes are Alternant Codes

Let

- \( \mathbf{a} = (a_1, \ldots, a_n) \) with \( a_i = \alpha^{i-1} \) for \( i = 1, \ldots, n \).
- \( \mathbf{b} = 1 \in \mathbb{F}^n_{qm} \).

Then the BCH code with defining zeros \( \mathcal{Z} = \{0, 1, \ldots, \delta - 2\} \) is: \( \text{Alt}_{\delta-1}(\mathbf{a}, \mathbf{b}) \).

→ ECP for cyclic codes were found **beyond half the BCH bound** by Duursma and Kötter.

---

I. Duursma

*Decoding codes from curves and cyclic codes.*


---

R. Kötter.

*On algebraic decoding of algebraic-geometric and cyclic codes.*


---

I. Duursma, R. Kötter.

*Error-locating pairs for cyclic codes.*

**GRS codes**

V. M. Sidelnikov and S. O. Shestakov.

On insecurity of cryptosystems based on generalized Reed-Solomon codes.
Discrete mathematics and Applications.

---

**Subcodes of GRS codes**

I. Márquez-Corbella, E. Martínez-Moro and R. Pellikaan.

*The non-gap sequence of a subcode of a generalized Reed-Solomon code.*

C. Wieschebrink.

*An attack on the modified Niederreiter encryption scheme.*

C. Wieschebrink.

*Cryptoanalysis of the Niederreiter public key scheme based on GRS subcodes.*
Structural attacks against code-based PKC II

Error-correcting pairs and arrays from algebraic geometry codes

Introduction to Coding Theory

Code based cryptography

McEliece Cryptosystem

Generic attacks on the McEliece PKC

Niederreiter Cryptosystem

Error Correcting Pairs

Examples of the existence of ECP

GRS codes

Subcodes

AG codes

Alternant codes

Goppa codes

BCH codes

Conclusions

Reverse engineering AG codes

AG codes

C. Faure and L. Minder.
Cryptanalysis of the McEliece cryptosystem over hyperelliptic codes.

I. Márquez-Corbella, E. Martínez-Moro and R. Pellikaan.
On the unique representation of very strong algebraic geometry codes.
Designs, Codes and Cryptography, 2013.

I. Márquez-Corbella, E. Martínez-Moro, R. Pellikaan and D. Ruano.
Computational aspects of retrieving a representation of an algebraic geometry code.
Submitted to Designs, Codes and Cryptography.

Subfield subcodes of GRS codes = Alternant codes:
OPEN
QUESTION:

→ If a code has a $t$-ECP how difficult / easy is to retrieve such a pair?
Let

- \( \mathcal{X} \) be an algebraic curve over \( \mathbb{F}_q \) of genus \( g \).
- \( E \) be a divisor of \( \mathcal{X} \) with \( \deg(E) = m \) and \( \{ f_0, \ldots, f_r \} \) be a basis of \( L(E) \).

We consider the following map:

\[
\varphi_E : \mathcal{X} \longrightarrow \mathbb{P}^r(\mathbb{F}_q) \\
P \longmapsto \varphi_E(P) = (f_0(P), \ldots, f_r(P))
\]

### Curves defined by quadratic equations

1. If \( m \geq 2g + 2 \) then \( \varphi_E(\mathcal{X}) = \mathcal{Y} \) is a normal curve in \( \mathbb{P}^{m-g} \) which is the intersection of quadrics.

   - In particular \( I(\mathcal{Y}) \) is generated by \( I_2(\mathcal{Y}) \).

2. If \( m \geq 2g + 1 \) then \( \varphi_E(\mathcal{X}) = \mathcal{Y} \) is a normal curve in \( \mathbb{P}^{m-g} \) which is the intersection of quadrics and cubics.

   - In particular \( I(\mathcal{Y}) \) is generated by \( I_2(\mathcal{Y}) \) and \( I_3(\mathcal{Y}) \).

---

D. Mumford.  
*Varieties defined by quadratic equations.*  

B. Saint-Donat.  
*Sur les équations définissant une courbe algébrique.*  

\( I_d(\mathcal{Y}) \)

\( I_d(\mathcal{Y}) \) is the ideal generated by the homogeneous elements of degree \( d \) in \( I(\mathcal{Y}) \).
Let

- $\mathcal{Y}$ be an algebraic curve in $\mathbb{P}^r$ of degree $m$ such that $I(\mathcal{Y}) = l_2(\mathcal{Y})$.
- $Q$ be an $n$-tuples of points that lies on the curve $\mathcal{Y}$ (i.e. $I(\mathcal{Y}) \subseteq I(Q)$)

**Proposition: due to Bezout-Theorem**

If $n > 2m$ then,

$$l_2(Q) = l_2(\mathcal{Y})$$
Let \( C \) be a \( k \)-dimensional subspace of \( \mathbb{F}^n \) with basis \( \{g_1, \ldots, g_k\} \).

We denote:

1. **The second symmetric power of** \( C \) **by** \( S^2(C) \)
   - \( S^2(C) \) has basis \( \{X_iX_j \mid 1 \leq i \leq j \leq n\} \) and dimension \( \binom{k+1}{2} \)

2. **The square code of** \( C \) **by** \( \langle C \ast C \rangle \) **or by** \( C^{(2)} \).
   - \( C^{(2)} \) is the linear subspace in \( \mathbb{F}^n \) generated by \( \{a \ast b \mid a, b \in C\} \).

We consider the linear map:

\[
\sigma : S^2(C) \longrightarrow C^{(2)}
\]

\[
X_iX_j \longmapsto g_i \ast g_j
\]

We denote by \( K_2(C) \) the kernel of this map, then

\[
0 \longrightarrow K_2(C) \longrightarrow S^2(C) \longrightarrow C^{(2)} \longrightarrow 0
\]

is an **exact sequence**.

And

\[
l_2(Q) = \left\{ \sum_{1 \leq i \leq j \leq k} a_{ij}X_iX_j \mid \sum_{1 \leq i \leq j \leq k} a_{ij} (g_i \ast g_j) = 0 \right\} = K_2(C)
\]

**Proposition**

Let \( Q \) be an \( n \)-tuple of points in \( \mathbb{P}^r \) over \( \mathbb{F} \) not in a hyperplane. Then the complexity of the computation of \( l_2(Q) \) is at most \( O \left( n^2 \binom{r}{2} \right) \).
A code $C$ has a VSAG representation if $C = C_L(\mathcal{X}, P, E)$ where the curve $\mathcal{X}$ has genus $g$, $P$ consists of $n$ points and $E$ has degree $m$ such that

$$2g + 2 < m < \frac{1}{2}n \quad \text{or} \quad \frac{1}{2}n + 2g - 2 < m < n - 4$$

The dual of a VSAG code is again VSAG

→ The dimension of such a code is $k = m + 1 - g$. Thus the dimension satisfies the following bound:

$$g + 3 < k < \frac{1}{2}n - g + 1 \quad \text{or} \quad \frac{1}{2}n + g - 1 < k < n - g - 2$$

Theorem

Let $C$ be a VSAG code then a VSAG representation can be obtained from its generator matrix.

→ Moreover all VSAG representations of $C$ are strict isomorphic.
Let \( C = C_L(\mathcal{X}, P, E)^\perp \) be an AG code where

- the curve \( \mathcal{X} \) has genus \( g \).
- the divisor \( E \) has degree \( m \) such that \( 2g + 2 \leq m < \frac{1}{2} n \)

\( \rightarrow \) \( C \) is a VSAG code with \( d^* = m - 2g + 1 \)

**Our goal:** Construct ECP’S eluding the use of Riemann-Roch spaces!!

The attackers will use an equivalent representation \((\mathcal{Y}, Q, F)\) of the same code \( C^\perp \), which is also VSAG.
Recall that: Let \( C = C_L(\mathcal{Y}, Q, F)^\perp \) be an AG code of genus \( g \) and designed minimum distance \( d^* \) such that

\[
m = \deg(F) > 2g - 2.
\]

Then \( C \) has parameters \([n, \geq n + g - m - 1, \geq m - 2g + 2] \).

Define \( A = C_L(\mathcal{Y}, Q, F - D) \) and \( B = C_L(\mathcal{Y}, Q, D) \)

Then \( < A \ast B > \subseteq C^\perp \). Moreover if

\[
t = \left\lfloor \frac{d^* - 1 - g}{2} \right\rfloor \quad \text{and} \quad \deg(D) = t + g
\]

then \((A, B)\) is a \( t\)-ECP for \( C \).

In particular we take \( D = (t + g)Q_1 \) where \( Q_1 \) is the first rational point of \( Q \).
Define:

- $A_0 = C_L(\mathcal{Y}, Q, F - (m - t - g)Q_1)$.
  - Note that $L(F - (m - t - g)Q_1) \subseteq L(F)$, thus $A_0 \subseteq C_{\perp} = C_L(\mathcal{Y}, Q, F)$
  - $A_0$ is the space of those codewords in $C_{\perp}$ that are zero at the first position of multiplicity $m - t - g$. This multiplicity can be controlled!!!

- $B_0 = \langle A \ast C \rangle_{\perp}$
  - Note that $B_0_{\perp} \subseteq B_{\perp}$ so $d(B_0_{\perp}) \geq d(B_{\perp}) > t$

Thus $(A_0, B_0)$ is a $t$-ECP for $C$. 

---

**Reverse engineering AG codes VI**

**Error-correcting pairs and arrays from algebraic geometry codes**

**Introduction to Coding Theory**

**Code based cryptography**

**McEliece Cryptosystem**

**Generic Attacks on the McEliece PKC**

**Niederreiter Cryptosystem**

**Error Correcting Pairs**

**Examples of the existence of ECP**

- GRS codes
- Subcodes
- AG codes
- Alternant codes
- Goppa codes
- BCH codes

**Conclusions**

**Reverse engineering AG codes**
THANK YOU FOR YOUR ATTENTION!