Error-correcting pairs
and majority coset decoding
for and from algebraic geometry codes

Ruud Pellikaan
g.r.pellikaan@tue.nl
joint work with
Irene Márquez-Corbella

Valladolid, 10 July 2013
Introduction and content

- Error-correcting codes
- Codes on curves
- Error-correcting pairs for codes on curves
- Majority coset decoding
- Public-key cryptosystems
- Code-based cryptography
- Reverse engineering AG codes
- Error-correcting pairs from codes on curves
- Questions
Error-correcting codes

A linear block code: $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^n$

Parameters $[n, k, d]$:

- $n =$ length
- $k =$ dimension of $C$
- $d =$ minimum distance of $C$

$$d = \min \{|d(x, y) | x, y \in C, x \neq y \}$$

$t =$ error-correcting capacity of $C$

$$t = \lfloor \frac{d-1}{2} \rfloor$$
The **standard inner product** is defined by

\[ a \cdot b = a_1 b_1 + \cdots + a_n b_n \]

For two subsets \( A \) and \( B \) of \( \mathbb{F}_q^n \)
\( A \perp B \) if and only if \( a \cdot b = 0 \) for all \( a \in A \) and \( b \in B \)

Let \( a \) and \( b \) in \( \mathbb{F}_q^n \)
The **star product** is defined by coordinatewise multiplication:

\[ a \star b = (a_1 b_1, \ldots, a_n b_n) \]

For two subsets \( A \) and \( B \) of \( \mathbb{F}_q^n \)

\[ A \star B = \{ a \star b \mid a \in A \text{ and } b \in B \} \]
Let $C$ be a linear code in $\mathbb{F}_q^n$

The pair $(A, B)$ of linear subcodes of $\mathbb{F}_{q^m}^n$ is called a $t$-error correcting pair (ECP) over $\mathbb{F}_{q^m}$ for $C$ if

E.1 $(A \ast B) \perp C$
E.2 $k(A) > t$
E.3 $d(B^\perp) > t$
E.4 $d(A) + d(C) > n$
Let $A$ and $B$ be linear subspaces of $\mathbb{F}_q^n$

Let $r \in \mathbb{F}_q^n$ be a received word

Define the kernel

$$K(r) = \{ a \in A \mid (a \ast b) \cdot r = 0 \text{ for all } b \in B \}$$

Lemma

Let $C$ be an $\mathbb{F}_q$-linear code of length $n$

Let $r$ be a received word with error vector $e$

So $r = c + e$ for some $c \in C$

If $A \ast B \subseteq C^\perp$, then

$$K(r) = K(e)$$
Let \((A, B)\) be a \(t\)-ECP for \(C\)

Let \(J\) be a subset of \(\{1, \ldots, n\}\)

Define the subspace of \(A\)

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

Lemma

Let \((A \ast B) \perp C\)

Let \(e\) be an error vector of the received word \(r\)

If \(I = \text{supp}(e) = \{ i \mid e_i \neq 0 \}\), then

\[
A(I) \subseteq K(r)
\]

If moreover \(d(B^\perp) > \text{wt}(e)\), then \(A(I) = K(r)\)
Theorem

Let $C$ be an $\mathbb{F}_q$-linear code of length $n$
Let $(A, B)$ be a $t$-error-correcting pair over $\mathbb{F}_{q^m}$ for $C$

Then the basic algorithm corrects $t$ errors
for the code $C$ with complexity $\mathcal{O}((mn)^3)$
Let $X$ be an algebraic curve defined over $\mathbb{F}_q$ of genus $g$.

Let $\mathcal{P} = (P_1, \ldots, P_n)$ an $n$-tuple of mutual distinct points of $X(\mathbb{F}_q)$.

(If the support of $E$ is disjoint from $\mathcal{P}$), then the evaluation map

$$ev_{\mathcal{P}} : L(E) \to \mathbb{F}_q^n$$

where $ev_{\mathcal{P}}(f) = (f(P_1), \ldots, f(P_n))$, is well defined.

The algebraic geometry code $C_L(X, \mathcal{P}, E)$ is the image of $L(E)$ under the evaluation map $ev_{\mathcal{P}}$.

If $m < n$, then $C_L(X, \mathcal{P}, E)$ is an $[n, k, d]$ code with

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

$n - m$ is called the designed minimum distance of $C_L(X, \mathcal{P}, E)$. 
Embedding of $X$ in linear system of $E$ of degree $m$

Let $f_1, f_2, \ldots, f_k$ be a basis of $L(E)$

$$\varphi_E : X \longrightarrow \mathbb{P}^{k-1}$$

$$P \mapsto (f_1(P) : f_2(P) : \ldots : f_k(P))$$

$Y = \varphi_E(X)$ is a curve of degree $m$ in $\mathbb{P}^{k-1}$

$Q = (\varphi_E(P_1), \ldots, \varphi_E(P_n))$ projective system

$$G_Q = \begin{pmatrix}
    f_1(P_1) & \cdots & f_1(P_j) & \cdots & f_1(P_n) \\
    f_2(P_1) & \cdots & f_2(P_j) & \cdots & f_2(P_n) \\
    \vdots & \cdots & \vdots & \cdots & \vdots \\
    f_k(P_1) & \cdots & f_k(P_j) & \cdots & f_k(P_n)
\end{pmatrix}$$ generator matrix

minimum distance $\geq n - m$
Let $\omega$ be a differential form with a simple pole at $P_j$ with residue 1 for all $j = 1, \ldots, n$.

Let $K$ be the canonical divisor of $\omega$. Let $m$ be the degree of the divisor $E$ on $X$ with disjoint support from $P$.

Let $E^\perp = D - E + K$ and $m^\perp = \deg(E^\perp)$. Then $m^\perp = 2g - 2 - m + n$ and

$$C_L(X, P, E)^\perp = C_L(X, P, E)$$
Let $F$ and $G$ be divisors.
Then there is a well defined linear map

$$L(F) \otimes L(G) \longrightarrow L(F + G)$$

given on generators by

$$f \otimes g \mapsto fg$$

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 \( C = C_L(\mathcal{X}, \mathcal{P}, E)^\perp \)

Choose a divisor \( F \) with support disjoint from \( \mathcal{P} \)
Let \( A = C_L(\mathcal{X}, \mathcal{P}, F) \)
Let \( B = C_L(\mathcal{X}, \mathcal{P}, E - F) \)

Then
- \( A \ast B \subseteq C^\perp \)
- If \( t + g \leq \deg(F) < n \), then \( k(A) > t \)
- If \( \deg(G - F) > t + 2g - 2 \), then \( d(B^\perp) > t \)
- If \( \deg(G - F) > 2g - 2 \), then \( d(A) + d(C) > n \)
Proposition

An algebraic geometry code of designed minimum distance $d$ from a curve over $\mathbb{F}_q$ of genus $g$ has a $t$-error-correcting pair over $\mathbb{F}_q$ where

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

An algebraic geometry code of designed minimum distance \( d \) from a curve over \( \mathbb{F}_q \) of genus \( g \) has a \( t \)-error-correcting pair over \( \mathbb{F}_{q^m} \) where

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

if

\[
m > \log_q \left( 2 \binom{n}{t} + 2 \binom{n}{t+1} + 1 \right)
\]

Not constructive!

Majority coset decoding gives a constructive and efficient approach
Proposition (Feng-Rao, Duursma)

Let $C$ be a code with a subcode $D$ of codimension one. Let $a_1, \ldots, a_w$ and $b_1, \ldots, b_w$ such that

\[
\begin{cases}
    a_i \ast b_j \in C^\perp & \text{if } i + j \leq w, \\
    a_i \ast b_j \in D^\perp \setminus C^\perp & \text{if } i + j = w + 1.
\end{cases}
\]

Then all words of $C \setminus D$ have weight at least $w$. 
Proof: Let $c \in C \setminus D$

Let $A$ be the $w \times n$ matrix with the $a_j$’s as rows

Let $B$ be the $w \times n$ matrix with the $b_j$’s as rows

Let $D(c)$ be the diagonal matrix with $c$ on the diagonal

Let $S(c)$ be the $w \times w$ matrix with entries $s_{i,j} = a_i \cdot b_j \cdot c$

Then

$$AD(c)B^T = S(c)$$

and

$$\begin{cases} 
  s_{i,j} = 0 & \text{if } i + j \leq w, \\
  s_{i,j} \neq 0 & \text{if } i + j = w + 1.
\end{cases}$$

Hence $\text{wt}(c) = \text{rk}(D(c)) \geq \text{rk}(S(c)) = w$
Let $w = 2t + 1$

$$
\begin{pmatrix}
0 & 0 & \ldots & 0 & 0 & \ldots & 0 & S_{1,w} \\
0 & 0 & \ldots & 0 & 0 & \ldots & S_{2,w-1} & S_{2,w-1} \\
\vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & \ldots & 0 & S_{t,t+1} & \ldots & S_{t,w-1} & S_{t,w} \\
0 & 0 & \ldots & S_{t+1,t} & S_{t+1,t+1} & \ldots & S_{t+1,w-1} & S_{t+1,w} \\
\vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & S_{w-1,2} & \ldots & S_{w-1,t} & S_{w-1,t+1} & \ldots & S_{w-1,w-1} & S_{w-1,w} \\
S_{w,1} & S_{w,2} & \ldots & S_{w,t} & S_{w,t+1} & \ldots & S_{w,w-1} & S_{w,w}
\end{pmatrix}
$$
Decoding: Let \( r \) be a received word
with \( r = c + e \) and \( c \in C \setminus D \) and error vector \( e \)
Let \( S(r) \) be the \( t \times t \) syndrome matrix with entries \( s_{i,j}(r) = a_i \ast b_j \cdot r \)
Then
\[
s_{i,j}(r) = s_{i,j}(e) \quad \text{if} \quad i + j \leq w
\]
are called the known syndromes
Now \( D \) has codimension one in \( C \), so there exists a \( d \in D^\perp \setminus C^\perp \)
and \( \lambda_{ij} \in \mathbb{F}_q^* \) for \( i + j = w + 1 \) such that
\[
a_i \ast b_j \equiv \lambda_{ij} d \pmod{C^\perp}
\]
Hence the unknown syndromes are related to \( d \cdot r \) by:
\[
s_{i,j}(r) = \lambda_{ij} d \cdot r \quad \text{if} \quad i + j = w + 1
\]
Let $w = 2t + 1$

$$
\begin{pmatrix}
  s_{1,1} & s_{1,2} & \cdots & s_{1,t} & s_{1,t+1} & \cdots & s_{1,w-1} & s_{1,w} \\
  s_{2,1} & s_{2,2} & \cdots & s_{2,t} & s_{2,t+1} & \cdots & s_{2,w-1} \\
  \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\
  s_{t,1} & s_{t,2} & \cdots & s_{t,t} & s_{t,t+1} & \cdots & \vdots & \vdots \\
  s_{t+1,1} & s_{t+1,2} & \cdots & s_{t+1,t} & \vdots & \vdots & \vdots & \vdots \\
  \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\
  s_{w-1,1} & s_{w-1,2} & \cdots & s_{w-1,1} & s_{w,1} \\
\end{pmatrix}
$$
At the heart of any public-key cryptosystem is a one-way function

\[ y = f(x) \]

that is easy to evaluate but for which it is computationally infeasible (one hopes) to find an inverse

\[ x \in f^{-1}(y) \]
PKC systems use **trapdoor one-way functions** by mathematical problems that are (supposedly) hard

- RSA, **factoring integers**
- Diffie-Hellman, **discrete-log problem** in finite field
- Elliptic curve PKC, **addition on elliptic curve**
- Lattice-based PKC systems **closest vector problem**
- Code-based PKC systems, **decoding of codes**
Code based PKC systems
Take a class of codes that have an efficient decoding algorithm:
Scramble a generator matrix such that it looks like a random code

– Goppa codes (McEliece)
– with parity check matrix instead of generator matrix (Niederreiter)
– Algebraic geometry codes (Janwa-Moreno)
– subcodes of GRS codes (Berger-Loidreau)
– subfield subcodes of algebraic geometry codes (Janwa-Moreno)
Generic attack – decoding algorithms:
- McEliece 1978
- Finiasz-Sendrier 2009
- Bernstein-Lange-Peters 2008-2011
- Becker-Joux-May-Meurer Eurocrypt 2012

Structural attack:
- GRS codes (Sidelnikov-Shestakov)
- subcodes of GRS codes (Wieschebrink, Márquez-Martínez-P)
- Alternant codes: open
- Goppa codes: open
- AG codeds: (Faure-Minder, $g \leq 2$)
- VSAG codes: (Márquez-Martínez-P-Ruano, arbitrary $g$)
Let \( \mathcal{X} \) be an absolutely irreducible and nonsingular curve of genus \( g \) over the perfect field \( \mathbb{F} \)

Let \( E \) be a divisor on \( \mathcal{X} \) of degree \( m \)

If \( m \geq 2g + 1 \)
then \( \varphi_E \) gives an embedding of \( \mathcal{X} \) onto \( Y = \varphi_E(\mathcal{X}) \)
which is a normal curve in the linear system \( |E| = \mathbb{P}^{m-g} \)

If \( m \geq 2g + 2 \), then \( Y \) is an intersection of quadrics
More precisely:
\( I(Y) \) is generated by \( I_2(Y) \)
the set of homogeneous elements of degree two in \( I(Y) \)
Let \( Y \) be a curve embedded in projective \( r \)-space of degree \( m \)

Let \( I(Y) \) be the vanishing ideal of \( Y \)

Let \( Q \) be a subset of \( Y \) of \( n \) points

Then

\[
I(Y) \subseteq I(Q)
\]

Hence

\[
I^2(Y) \subseteq I^2(Q)
\]

Suppose \( I(Y) \) is generated by \( I^2(Y) \)

If \( n > 2m \), then \( I^2(Y) = I^2(Q) \)

By Bézout’s Theorem
\( g_1, \ldots, g_k \) a basis of \( C \)

\( S^2(C) \) is the second symmetric power of \( C \)

\( S^2(C) \) has basis \( \{x_ix_j \mid 1 \leq i \leq j \leq n \} \) and dimension \( \binom{k+1}{2} \)

with \( x_i = g_i \)

\( C^{(2)} = \langle C \ast C \rangle \) the square of \( C \)

Consider the linear map

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

\[
x_i x_j \quad \mapsto \quad g_i \ast g_j
\]

\( K_2(C) \) is 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

\[
l_2(\mathcal{Q}) = K_2(C) := \{ \sum_{1 \leq i \leq j \leq k} a_{ij} X_i X_j \mid \sum_{1 \leq i \leq j \leq k} a_{ij} g_i \ast g_j = 0 \}
\]

**Proposition**

Let \( \mathcal{Q} \) be an \( n \)-tuple of points in \( \mathbb{P}^r \) over \( \mathbb{F} \) not in a hyperplane

Then the complexity of the computation of \( l_2(\mathcal{Q}) \) is at most \( \mathcal{O}(n^4) \)
C is called **very strong algebraic-geometric (VSAG)**

if \( C = C_L(\mathcal{X}, \mathcal{P}, E) \) and the curve \( \mathcal{X} \) has genus \( g \)
\( \mathcal{P} \) consists of \( n \) points and \( E \) has degree \( m \) such that

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

The dual of a VSAG code is again VSAG
Main Theorem

Let $C$ be a VSAG code

Then a VSAG representation of $C$ can be obtained efficiently from its generator matrix

Moreover all VSAG representations of $C$ are strict isomorphic
Shortcut via $t$-ECP pair $(A, B)$ in $\mathbb{F}_q^n$

Bypassing triple $(\mathcal{X}, \mathcal{P}, E)$ and Riemann–Roch spaces

<table>
<thead>
<tr>
<th>$\mathbb{F}_q^n$</th>
<th>$\mathbb{F}_q(\mathcal{X})$</th>
<th>$\mathbb{F}_q^n$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(\mathcal{X}, \mathcal{P}, E)$</td>
<td>$C = C_L(\mathcal{X}, \mathcal{P}, E)^\perp$</td>
<td>$\mathcal{L}(\mathcal{X}, \mathcal{P}, E)$</td>
</tr>
<tr>
<td>$(\mathcal{X}, \mathcal{P}, E - (t + g)P_1)$</td>
<td>$L(E)$</td>
<td>$A = C_L(\mathcal{X}, \mathcal{P}, E - (t + g)P_1)$</td>
</tr>
<tr>
<td>$(\mathcal{X}, \mathcal{P}, (t + g)P_1)$</td>
<td>$L((t + g)P_1)$</td>
<td>$B = C_L(\mathcal{X}, \mathcal{P}, (t + g)P_1)$</td>
</tr>
</tbody>
</table>
In fact, $A$ is the space of those code words in $C^\perp$ that are zero at the first position with multiplicity $m - t - g$. This multiplicity can be controlled since we computed $I_2(\mathcal{Q})$ efficiently.

Define $B_0 = \langle A \ast C \rangle^\perp$

Then $B_0^\perp = \langle A \ast C \rangle \subseteq B^\perp$

So $d(B_0^\perp) \geq d(B^\perp) > t$

Hence $(A, B_0)$ is a $t$-ECP for $C$

Similarly decode up to $\lfloor (d^* - 1)/2 \rfloor$ errors with majority coset decoding