Is it hard to retrieve an error-correcting pair?

Ruud Pellikaan
and
Irene Márquez-Corbella

Third IMAC and Singacom Day Conference on Algebraic Applications to Information Theory
May 9th-10th, 2016
Instituto Universitario de Matemáticas y Aplicaciones de Castellón
Universidad Jaume I, Castellón, Spain
Content

- Decoding algorithm with an Error-Correcting Pair
- Existence of Error-Correcting Pairs
- Code Based Public Key Cryptosystem
- Possible attacks
Decoding algorithm with an Error-Correcting Pair
Error-correcting codes

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

**Parameters** \([n, k, d]:\)

- \( n = \text{length} \)
- \( k = \text{dimension of } C \)
- \( d = \text{minimum distance of } C \)

\[
d = \min \{|d(x, y)| \mid x, y \in C, x \neq y\}
\]

\( t = \text{error-correcting capacity of } C \)

\[
t = \left\lfloor \frac{d(C) - 1}{2} \right\rfloor
\]
Inner product

Let \( a \) and \( b \) in \( \mathbb{F}_q^n \)

The standard inner product is defined by

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

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

The dual code of \( C \) is defined by

\[
    C^\perp = \{ x | x \cdot c = 0 \text{ for all } c \in C \} 
\]
The **star product** is defined by coordinatewise multiplication:

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

Then

\[(a \ast b) \cdot c = \sum a_i b_i c_i = (a \ast c) \cdot b \]

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

\[ A \ast B = \langle a \ast b \mid a \in A \text{ and } b \in B \rangle \]
Efficient decoding algorithms

The following classes of codes:

- Generalized Reed-Solomon codes
- Cyclic codes
- Alternant codes
- Goppa codes
- Algebraic geometry codes

have efficient decoding algorithms:

- Arimoto, Peterson, Gorenstein, Zierler
- Berlekamp, Massey, Sakata
- Justesen et al., Vladut-Skorobogatov, ..........
- Error-correcting pairs
Notice that multiplying polynomials first and than evaluating gives the same answer as first evaluating and than multiplying. If \( f(X), g(X) \in \mathbb{F}_q[X] \) and \( h(X) = f(X)g(X) \) then

\[
h(a) = f(a)g(a) \text{ for all } a \in \mathbb{F}_q
\]

So

\[
\text{ev}(f(X)g(X)) = \text{ev}(f(X)) \star \text{ev}(g(X)) \quad \text{and}
\]

\[
\text{ev}_a(f(X)g(X)) = \text{ev}_a(f(X)) \star \text{ev}_a(g(X))
\]
Generalized Reed-Solomon codes

Let \( \mathbf{a} = (a_1, \ldots, a_n) \) be an \( n \)-tuple of distinct elements of \( \mathbb{F}_q \)

Let \( \mathbf{b} = (b_1, \ldots, b_n) \) be an \( n \)-tuple of nonzero elements of \( \mathbb{F}_q \)

Evaluation map:

\[
ev_{\mathbf{a}, \mathbf{b}}(f(X)) = (f(a_1)b_1, \ldots, f(a_n)b_n)
\]

\( \text{GRS}_k(\mathbf{a}, \mathbf{b}) = \{ \ev_{\mathbf{a}, \mathbf{b}}(f(X)) \mid f(X) \in \mathbb{F}_q[X], \deg(f(X)) < k \} \)

Parameters:

\[
[n, k, n - k + 1] \text{ if } k \leq n
\]

Since a polynomial of degree \( k - 1 \) has at most \( k - 1 \) zeros
PROPOSITION

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

and

\[ \text{RS}_k(n, b) \ast \text{RS}_l(n, c) = \text{RS}_{k+l-1}(n, b + c - 1) \text{ if } n = q - 1 \]
Now

\[ \text{GRS}_k(a, b) = \{ \text{ev}_a(f(X)) \ast b \mid f(X) \in \mathbb{F}_q[X], \deg f(X) < k \} \]

and similar statements hold for \( \text{GRS}_l(a, c) \) and \( \text{GRS}_{k+l-1}(a, b \ast c) \)

Furthermore

\[ (\text{ev}_a(f(X)) \ast b) \ast (\text{ev}_a(g(X)) \ast c) = \text{ev}_a(f(X)g(X)) \ast b \ast c \]

and \( \deg f(X)g(X) < k + l - 1 \) if \( \deg f(X) < k \) and \( \deg g(X) < l \)

Hence

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

Equality holds since on both sides the vector spaces are generated by the elements

\((ev_a(X^i) \ast b) \ast (ev_a(X^j) \ast c) = ev_a(X^{i+j}) \ast b \ast c\)

where \(0 \leq i < k\) and \(0 \leq j < l\)
Let \( n = q - 1 \)
Let \( \alpha \) be a primitive element of \( \mathbb{F}_q^* \)
Define \( a_j = \alpha^{j-1} \) and \( b_j = a_j^{n-b+1} \) for \( j = 1, \ldots, n \)

Then

\[
RS_k(n, b) = GRS_k(a, b)
\]

Similar statements hold for \( RS_l(n, c) \) and \( RS_{k+l-1}(n, b + c - 1) \)

The statement concerning the star product of \( RS \) codes is now a consequence of the corresponding statement on the GRS codes.
Kernel of a received word

Let $A$ and $B$ be linear subspaces of $\mathbb{F}_{q}^{m}$ and $r \in \mathbb{F}_{q}^{n}$ a received word.

Define the kernel

$$K(r) = \{ a \in A \mid (a \ast b) \cdot r = 0 \text{ for all } b \in B \}$$
Let $B^\vee$ be the space of all linear functions $\beta : B \to \mathbb{F}_q$

Now $K(r)$ is a subspace of $A$ and it is the kernel of the linear map

$$S_r : A \to B^\vee$$

defined by $a \mapsto \beta_a$, where

$$\beta_a(b) = (a \ast b) \cdot r$$

Let $a_1, \ldots, a_l$ and $b_1, \ldots, b_m$ be bases of $A$ and $B$

Then the map $S_r$ has the $m \times l$ syndrome matrix

$$((b_i \ast a_j) \cdot r | 1 \leq j \leq l, 1 \leq i \leq m)$$

with respect to these bases
Kernel for a GRS code

Let $A = \text{GRS}_{t+1}(a, 1)$ and $B = \text{GRS}_t(a, 1)$ and $C = \langle A \ast B \rangle^\perp$

Let
\[
\begin{align*}
    a_i &= \text{ev}_{a,1}(X^{i-1}) \text{ for } i = 1, \ldots, t + 1 \\
    b_j &= \text{ev}_{a,1}(X^j) \text{ for } j = 1, \ldots, t \\
    h_l &= \text{ev}_{a,1}(X^l) \text{ for } l = 1, \ldots, 2t
\end{align*}
\]

Then
\[
\begin{align*}
    a_1, \ldots, a_{t+1} \text{ is a basis of } A \\
    b_1, \ldots, b_t \text{ is a basis of } B \\
    h_1, \ldots, h_{2t} \text{ is a basis of } C^\perp
\end{align*}
\]

Furthermore
\[
a_i \ast b_j = \text{ev}_{a,1}(X^{i+j-1}) = h_{i+j-1}
\]
Matrix of syndromes for a GRS code

Let $r$ be a received word and its syndrome

$$(s_1, \ldots, s_{2t}) = rH^T$$

Then

$$(b_j \ast a_i) \cdot r = s_{i+j-1}$$

To compute the kernel $K(r)$ we have to compute the null space of the matrix of syndromes

$$
\begin{pmatrix}
  s_1 & s_2 & \cdots & s_t & s_{t+1} \\
  s_2 & s_3 & \cdots & s_{t+1} & s_{t+2} \\
  \vdots & \vdots & \ddots & \vdots & \vdots \\
  s_t & s_{t+1} & \cdots & s_{2t-1} & s_{2t}
\end{pmatrix}
$$
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

$$K(r) = K(e)$$
We have that $r = c + e$ for some codeword $c \in C$

Now $a \ast b$ is a parity check for $C$, since $A \ast B \subseteq C^\perp$

So $(a \ast b) \cdot c = 0$, and hence

$$(a \ast b) \cdot r = (a \ast b) \cdot e$$

for all $a \in A$ and $b \in B$
Let $J$ be a subset of $\{1, \ldots, n\}$

We defined before the subspace $A(J)$ of $A$ by

$$A(J) = \{ a \in A \mid a_j = 0 \text{ for all } j \in J \}$$
LEMMA - 2

Let $e$ be an error vector of the received word $r$

If \[(A * B) \subseteq C^\perp\]
and
\[l = \text{supp}(e) = \{ i \mid e_i \neq 0 \}\]
then
\[A(I) \subseteq K(r)\]
PROOF

Let $a \in A(I)$
Then $a_i = 0$ for all $i$ such that $e_i \neq 0$
Therefore

$$(a \ast b) \cdot e = \sum_{i=1}^{n} a_i b_i e_i = \sum_{e_i \neq 0} a_i b_i e_i = 0$$

for all $b \in B$
So $a \in K(e)$

But $K(e) = K(r)$ by Lemma (1) hence $a \in K(r)$

Therefore $A(I) \subseteq K(r)$
Let $e$ be an error vector of the received word $r$

If

$$(A \ast B) \subseteq C^\perp$$

and

$$I = \text{supp}(e) = \{ i \mid e_i \neq 0 \}$$

and

$$d(B^\perp) > \text{wt}(e) = t$$

then

$$A(I) = K(r)$$
Suppose that \( d(B^\perp) > \text{wt}(e) \)
Let \( a \in K(r) \) then \( a \in K(e) \) by Lemma (1)
Hence
\[
(e \ast a) \cdot b = e \cdot (a \ast b) = 0
\]
for all \( b \in B \), giving \( e \ast a \in B^\perp \)
Now
\[
\text{wt}(e \ast a) \leq \text{wt}(e) < d(B^\perp)
\]
So \( e \ast a = 0 \) meaning that \( e_i a_i = 0 \) for all \( i \)
Hence \( a_i = 0 \) for all \( i \) such that \( e_i \neq 0 \)
that is for all \( i \in I = \text{supp}(e) \)

Hence \( a \in A(I) \)
Therefore \( K(r) \subseteq A(I) \) and equality holds by Lemma (2)
COROLLARY

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

\[
(A \ast B) \subseteq C^\perp
\]

and

\[
l = \text{supp}(e) = \{ i \mid e_i \neq 0 \}
\]

and

\[
d(B^\perp) > \text{wt}(e) = t
\]

and \( a \) an element of \( K(r) \) with

\[
J = \{ j \mid a_j = 0 \}
\]

Then

\[
l \subseteq J
\]
The Lemmas imply

\[ K(r) = K(e) = A(I) \]

Let \( a \) be an element of \( K(r) \) then \( a \in A(I) \)

Then

\[ a_j = 0 \text{ for all } j \in I \]

Hence

\[ I \subseteq \{ j \mid a_j = 0 \} = J \]
Let \( I = \text{supp}(e) \) be the set of error positions. The set of zero coordinates of \( a \in A(I) \) contains the set of error positions by the Corollary.

The elements of \( A(I) \) are called \textit{error-locator} vectors or functions.

The space \( A(I) \) is not known to the receiver. The space \( K(r) \) can be computed after receiving the word \( r \). The equality \( A(I) = K(r) \) implies that all elements of \( K(r) \) are error-locator functions.
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 $\langle A \ast B \rangle \perp C$
E.2 $k(A) > t$
E.3 $d(B^\perp) > t$
E.4 $d(A) + d(C) > n$
Let $A \ast B \subseteq C^\perp$

Let $(A, B)$ be a $t$-ECP for $C$ with $d(C) \geq 2t + 1$

Suppose that $c \in C$ is the code word sent and $r = c + e$ is the received word for some error vector $e$ with $\text{wt}(e) \leq t$

The basic algorithm for the code $C$:
- Compute the kernel $K(r)$
  This kernel is nonzero since $k(A) > t$
- Take a nonzero element $a$ of $K(r)$
  $K(r) = K(e)$ since $(A \ast B) \perp C$
- Determine the set $J$ of zero positions of $a$
  $\text{supp}(e) \subseteq J$ since $d(B^\perp) > t$
- Compute the error values by erasure decoding
  $|J| < d(C)$ since $n - d(A) < d(C)$
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 $\mathcal{O}((mn)^3)$
The pair \((A, B)\) is a \(t\)-error-correcting for \(C\) so \(A \ast B \subseteq C^\perp\) and the basic algorithm can be applied to decode \(C\).

If a received word \(r\) has at most \(t\) errors then the error vector \(e\) with support \(I\) has size at most \(t\). 
\(A(I)\) is not zero, since \(I\) imposes at most \(t\) linear conditions on \(A\) and the dimension of \(A\) is at least \(t + 1\).
Let \(a\) be a nonzero element of \(K(r)\).
Let $a$ be a nonzero element of $K(r)$
Let $J = \{ j \mid a_j = 0 \}$

We assumed that $d(B^\perp) > t$
So $K(r) = A(I)$ by the Lemmas
So $a$ is an error-locator vector and $J$ contains $I$

The weight of the vector $a$ is at least $d(A)$
so $a$ has at most $n - d(A) < d(C)$ zeros by (4)
Hence $|J| < d(C)$ and erasure decoding gives the error values

The complexity is that of solving systems of linear equations
that is $O(n^3)$ in case $m = 1$ and $O((mn)^3)$ in general
Existence of Error-Correcting Pairs
Let $C^\perp = \text{GRS}_{2t}(a, 1)$
Then $C = \text{GRS}_{n-2t}(a, b)$ for some $b$
has parameters: $[n, n - 2t, 2t + 1]$

Let $A = \text{GRS}_{t+1}(a, 1)$ and $B = \text{GRS}_t(a, 1)$
Then $(A \ast B) \subseteq C^\perp$

$A$ has parameters $[n, t + 1, n - t]$
$B$ has parameters $[n, t, n - t + 1]$
So $B^\perp$ has parameters $[n, n - t, t + 1]$

Hence $(A, B)$ is a $t$-error-correcting pair for $C$
The converse is also true

**Theorem**

Let $C$ be an $[n, n - 2t, 2t + 1]$ code that has a $t$-ECP. Then $C$ is a GRS code.
Let $\mathbf{x} \in \mathbb{F}_q^n$ and $J$ be a subset of $\{1, \ldots, n\}$ consisting of $m$ integers

$$J = \{i_1, \ldots, i_m\} \quad \text{with} \quad 1 \leq i_1 < \cdots < i_m \leq n$$

Define

$$\mathbf{x}_J = (x_{i_1}, \ldots, x_{i_m}) = (x_j \mid j \in J) \in \mathbb{F}_q^m$$

the restriction of $\mathbf{x}$ to the coordinates indexed by $J$
Puncturing is the process of deleting columns from a generator matrix of a given linear code $C$ or equivalently deleting the same set of coordinates in each codeword of $C$.

Consider a subset $J \subseteq \{1, \ldots, n\}$ with $m$ elements.

Let $\overline{J}$ be the relative complement of $J$ in $\{1, \ldots, n\}$.

$C_J$ is punctured code of $C$ at $J$, is defined by

$$C_J = \{ c_{\overline{J}} \mid c \in C \}$$

So $C_J$ is the set of codewords of $C$ restricted to the positions of $\overline{J}$. 
$C^J$ is shortened code of $C$ at $J$

it is obtained by puncturing at $J$ the set of codewords that have a zero in the $J$-locations:

$$C^J = \{c^J_j \mid c \in C \text{ and } c_J = 0\}$$
Duality between puncturing and shortening

\[(C_j)^\perp = (C^\perp)^\prime\]

and

\[(C')^\perp = (C^\perp)^\prime,\]
Suppose that $C$ is a code that has $(A, B)$ as $t$-ECP and $A$ has parameters $[n, t + 1, n - t]$ and $B$ has parameters $[n, t, n - t + 1]$. Let $C_1$ be the code obtained from $C$ by puncturing on the two right-most coordinates. Define

$$A_1 = \{a' = (a_1, \ldots, a_{n-2}) \in \mathbb{F}_q^{n-2} \mid (a', 0, a_n) \in A \text{ for some } a_n \in \mathbb{F}_q \}$$

$$B_1 = \{b' = (b_1, \ldots, b_{n-2}) \in \mathbb{F}_q^{n-2} \mid (b', b_{n-1}, 0) \in B \text{ for some } b_{n-1} \in \mathbb{F}_q \}$$

Then $(A_1, B_1)$ is a $(t - 1)$-ECP for $C_1$ and $A_1$ has parameters $[n - 2, t, n - t - 1]$ and $B_1$ has parameters $[n - 2, t - 1, n - t]$.
Existence of ECPs

Error-Correcting Pairs exist for:

- Generalized Reed-Solomon codes
- Cyclic codes
- Alternant codes
- Goppa codes
- Algebraic geometry codes
Code Based Public Key Cryptosystems
Code based PKC systems - 1

McEliece:
Let $C$ be a class of codes that have efficient decoding algorithms correcting $t$ errors with $t \leq (d - 1)/2$

Secret key: $(S, G, P)$

- $S$ an invertible $k \times k$ matrix
- $G$ a $k \times n$ generator matrix of a code $C$ in $C$.
- $P$ an $n \times n$ permutation matrix

Public key: $G' = SGP$
McEliece:

Encryption with public key $G' = SGP$ and message $m$ in $\mathbb{F}_q^k$:

$$y = mG' + e$$

with random chosen $e$ in $\mathbb{F}_q^n$ of weight $t$

Decryption with secret key $(S, G, P)$:

$$yp^{-1} = (mG' + e)p^{-1} = mSG + ep^{-1}$$

$SG$ and $G$ are generator matrices of the same code $C$
e$P^{-1}$ has weight $t$
Decoder gives $c = mSG$ as closest codeword
Minimum distance decoding is NP-hard
(Berlekamp-McEliece-Van Tilborg)

It is assumed that:

1. $P \neq NP$
2. Decoding up to half the minimum distance is hard
3. One cannot distinguish nor retrieve the original code by disguising it with $S$ and $P$
Possible attacks
Generic attack – decoding algorithms:

– McEliece 1978
– Brickell, Lee 1988
– Leon 1988
– van Tilburg 1988
– Stern 1989
– Canteaut, Chabaud, Sendrier 1998
– Finiasz-Sendrier 2009
– Bernstein-Lange-Peters 2008-2011
– Becker-Joux-May-Meurer Eurocrypt 2012
Structural attacks:

- GRS codes (Sidelnikov-Shestakov)
- subcodes of GRS codes (Wieschebrink, Márquez-Martínez-P)
- Alternant codes: open
- Goppa codes: open
- Algebraic geometry codes: (Faure-Minder, genus $g \leq 2$)
- VSAG codes: (Márquez-Martínez-P-Ruano, arbitrary $g$)
- Polynomial attack on AG codes and certain subcodes (Couvreur-Márquez-P, using ECP’s)
Let $C$ be a linear code in $\mathbb{F}_q^n$
Let $(A, B)$ be a pair of $\mathbb{F}_{q^m}$-linear subcodes of $\mathbb{F}_{q^m}^n$
Consider the following conditions

E.1 $(A \ast B) \perp C$
E.2 $k(A) > t$
E.3 $d(B^\perp) > t$
E.4 $d(A) + d(C) > n$
E.5 $d(A^\perp) > 1$, that means $A$ is a non-degenerated code
E.6 $d(A) + 2t > n$
Let $\mathcal{P}(n, t, q)$ be the collection of pairs $(A, B)$ such that there exist a positive integer $m$ and a pair $(A, B)$ of $\mathbb{F}_{q^m}$-linear codes of length $n$ that satisfy the conditions E.2, E.3, E.5 and E.6.

Let $C$ be the $\mathbb{F}_q$-linear code of length $n$ that is the subfield subcode that has the elements of $A \ast B$ as parity checks:

$$C = \mathbb{F}_q^n \cap (A \ast B)^\perp$$

Then the minimum distance of $C$ is at least $2t + 1$ and $(A, B)$ is a $t$-ECP for $C$. 
Let $\mathcal{F}(n, t, q)$ be the collection of $\mathbb{F}_q$-linear codes of length $n$ and minimum distance $d \geq 2t + 1$

Consider the following map

$$\varphi(n,t,q) : \mathcal{P}(n, t, q) \rightarrow \mathcal{F}(n, t, q)$$

$$(A, B) \mapsto C$$

The question is whether this map is a one-way function
One step is finding a pair of codes \((A, B)\) such that \((A \ast B) \perp C\) for a given code \(C\)

Let \(G\) be a generator matrix of \(C\) with entries \(g_{ij}, 1 \leq i \leq k, 1 \leq j \leq n\)

Generator matrix for \(A\) with variables \(X_{ij}\) with \(1 \leq i \leq t + 1, 1 \leq j \leq n\)

and similarly for \(B\) by \(Y_{ij}\), \(1 \leq i \leq t, 1 \leq j \leq n\)

Finding a pair of codes \((A, B)\) such that \((A \ast B) \perp C\) is equivalent to finding a solution of the following system of \(kt(t + 1)\) quadratic equations in \(n(2t + 1)\) variables:

\[
\sum_{j=1}^{n} g_{wj} X_{uj} Y_{vj} = 0, \text{ for all } 1 \leq u \leq t + 1, 1 \leq v \leq t, 1 \leq w \leq k.
\]
This is a bilinear homogeneous system of equations. Such systems are studied by Faugère et al. using Groebner bases theory and Buchberger's algorithm and have improved complexity. Use Puncturing/shortening to reduce the number of variables.
Thanks for your attention!