On the Mollard code as a partially robust code

Darya Kovalevskaya

State University of Aerospace Instrumentation, Saint Petersburg, Russia
e-mail: dikovalevskaya@gmail.com

21 June 2016

Fifteenth International Workshop on Algebraic and Combinatorial Coding Theory, ACCT2016
Albena, Bulgaria, June 18-24, 2016
Outline

1. Definitions
2. The Mollard code construction
3. Memory protection architecture of the code $\tilde{M}^n$
Definitions

\( F^n \) – the \( n \)-dimensional metric space over the Galois field \( GF(2) \).

\( C^n \) – a perfect code of length \( n = 2^m - 1, \ m \geq 2, \ d = 3 \).
Definitions

\(F^n\) – the \(n\)-dimensional metric space over the Galois field \(GF(2)\).

\(C^n\) – a perfect code of length \(n = 2^m - 1, \ m \geq 2, \ d = 3\).

\(H^n\) – the linear binary perfect code of length \(n\), and code distance 3 (the Hamming code).
Definitions

$F^n$ – the $n$-dimensional metric space over the Galois field $GF(2)$.

$C^n$ – a perfect code of length $n = 2^m - 1$, $m \geq 2$, $d = 3$.

$H^n$ – the linear binary perfect code of length $n$, and code distance 3 (the Hamming code).
A detection kernel of $D \subset \mathbb{F}^n$:

$$K_{er_d}(D) = \{ e \in \mathbb{F}^n | e + d \in D, \forall d \in D \}.$$
A detection kernel of $D \subset \mathbb{F}^n$:
\[ \text{Ker}_d(D) = \{ e \in \mathbb{F}^n | e + d \in D, \forall d \in D \}. \]

A correction kernel of $D \subset \mathbb{F}^n$:
\[ \text{Ker}_c(D) = \{ e \in \mathbb{F}^n | e \notin D_{er}, d \in D, e' \in D_{er}, \text{Alg}_D(e, d) = \text{Alg}_D(e', d) \}. \]
Definitions

A detection kernel of $D \subset \mathbf{F}^n$:

$$\text{Ker}_d(D) = \{e \in \mathbf{F}^n | e + d \in D, \forall d \in D\}.$$ 

A correction kernel of $D \subset \mathbf{F}^n$:

$$\text{Ker}_c(D) = \{e \in \mathbf{F}^n | e \notin D_{er}, d \in D, e' \in D_{er}, \text{Alg}_D(e, d) = \text{Alg}_D(e', d)\}.$$ 

$\text{Alg}_D$ – an error correcting algorithm for $D$

$D_{er}$ – a set of errors which $\text{Alg}_D$ tries to correct
A detection kernel of $D \subset \mathbb{F}^n$:
$$Ker_d(D) = \{ e \in \mathbb{F}^n | e + d \in D, \forall d \in D \}.$$ 

A correction kernel of $D \subset \mathbb{F}^n$:
$$Ker_c(D) = \{ e \in \mathbb{F}^n | e \notin D_{er}, d \in D, e' \in D_{er}, Alg_D(e, d) = Alg_D(e', d) \}.$$ 

$Alg_D$ – an error correcting algorithm for $D$

$D_{er}$ – a set of errors which $Alg_D$ tries to correct
A code $D \subset \mathbb{F}^n$ is a **robust code** if $\text{Ker}_d(D) = 0$.

$$Q_D(x) = \frac{|d \in D : d+x \in D|}{|D|}$$ – the error masking probability of $x$. 
A code $D \subset \mathbb{F}^n$ is a robust code if $\text{Ker}_d(D) = 0$.

$$Q_D(x) = \frac{|\{d \in D : d+x \in D\}|}{|D|}$$ – the error masking probability of $x$.

For the robust code: $\max_{x \in \mathbb{F}^n \setminus \{0\}} Q_D(x) < 1$

A systematic $(n, 2^k, d)$-code $D$ is a partially robust code if $|\text{Ker}_d(D)| < 2^k$. 
A code $D \subset F^n$ is a robust code if $\text{Ker}_d(D) = 0$.

$$Q_D(x) = \frac{|d \in D : d + x \in D|}{|D|}$$ – the error masking probability of $x$.

For the robust code: $\max_{x \in F^n \setminus \{0\}} Q_D(x) < 1$

A systematic $(n, 2^k, d)$-code $D$ is a partially robust code if $|\text{Ker}_d(D)| < 2^k$.

The error masking probability of $D$:

$$Q_{mc}(D) = \max_{e \notin \text{Ker}_d(D)} Q_D(e).$$
A code $D \subseteq \mathbb{F}^n$ is a robust code if $\text{Ker}_d(D) = 0$.

$$Q_D(x) = \frac{|d \in D : d + x \in D|}{|D|}$$

- the error masking probability of $x$.

For the robust code: $\max_{x \in \mathbb{F}^n \setminus \{0\}} Q_D(x) < 1$

A systematic $(n, 2^k, d)$-code $D$ is a partially robust code if $|\text{Ker}_d(D)| < 2^k$.

The error masking probability of $D$:

$$Q_{mc}(D) = \max_{e \notin \text{Ker}_d(D)} Q_D(e).$$
Definitions

Derivative of the function $f : \mathbb{F}^k \rightarrow \mathbb{F}^s$:

$$D_v f(x) = f(x + v) + f(x), \quad v \in \mathbb{F}^k.$$  

Measure of the function $f$ nonlinearity:

$$P_f = \max_{v \in \mathbb{F}^k \setminus \{0\}} \max_{b \in \mathbb{F}^s} \Pr(D_v f(x) = b).$$
Definitions

**Derivative** of the function $f : \mathbb{F}^k \to \mathbb{F}^s$:

$$D_v f(x) = f(x + v) + f(x), \ v \in \mathbb{F}^k.$$ 

**Measure of the function $f$ nonlinearity:**

$$P_f = \max_{v \in \mathbb{F}^k \setminus \{0\}} \max_{b \in \mathbb{F}^s} \Pr(D_v f(x) = b).$$

$Pr(E)$ – the probability of the event $E$ occurrence.
Definitions

Derivative of the function $f : \mathbb{F}^k \rightarrow \mathbb{F}^s$:

$$D_v f(x) = f(x + v) + f(x), \quad v \in \mathbb{F}^k.$$ 

Measure of the function $f$ nonlinearity:

$$P_f = \max_{v \in \mathbb{F}^k \setminus \{0\}} \max_{b \in \mathbb{F}^s} \Pr(D_v f(x) = b).$$

$\Pr(E)$ – the probability of the event $E$ occurrence.
Definitions

The Mollard code construction
Memory protection architecture of the code $\mathcal{M}^n$

Nonlinear perfect codes constructions

Switching constructions

Vasiliev code

Mollard code

Method of ijk-components

Solov'eva-Phelps code

Cascade codes

Zinoviev code

Krotov combined construction

Darya Kovalevskaya

On the Mollard code as a partially robust code
The Vasiliev code construction:

\[ C^s \text{ – any perfect binary code of length } s \]
\[ f : C^s \rightarrow \{0, 1\} \text{ – some boolean function} \]

The Vasiliev code:

\[ V^{2s+1} = \{(x + c, |x| + f(c), x) : x \in F^s, c \in C^s\} \]

M. Karpovsky, K. Kulikowski and Z. Wang:

\[ V^{2s+1} \text{ – a partially robust code} \]
\[ |\text{Ker}_d(V^{2s+1})| = 2^s \]
\[ Q_{mc}(V^{2s+1}) = P_f \]
The classic Mollard code construction.

- $A^t$ – an arbitrary binary code of length $t$, $d_A \geq 3$, $0 \in A^t$.
- $B^m$ – an arbitrary binary code of length $m$, $d_B \geq 3$, $0 \in B^m$.
- $f : A^t \rightarrow F^m$ – any function.
- An arbitrary vector $x \in F^{tm}$:
  \[ x = (x_{11}, x_{12}, \ldots, x_{1m}, x_{21}, x_{22}, \ldots, x_{2m}, \ldots, x_{t1}, x_{t2}, \ldots, x_{tm}) \]
- The generalized parity check functions:
  \[ p_1(x) = (v_1, v_2, \ldots, v_t) \in F^t, v_i = \sum_{j=1}^{m} x_{ij}, \]
  \[ p_2(x) = (w_1, w_2, \ldots, w_m) \in F^m, w_i = \sum_{i=1}^{t} x_{ij}. \]
The classic Mollard code construction.

**Theorem 1 (Mollard M.).**

A set
\[ M^n = \{(x, a + p_1(x), b + p_2(x) + f(a)) | x \in \mathbb{F}^{tm}, a \in A^t, b \in B^m\} \]

is a binary code of length \( n = tm + t + m \) which minimal distance equals to 3.

- \( A^t = 2^{t_1} - 1 \), \( B^m = 2^{m_1} - 1 \) – perfect binary codes

\[ \downarrow \]

\[ M^n \] is a perfect binary code.

- \( m = 1, t = 2^{t_1} - 1 \)

\[ \downarrow \]

The Mollard code = the Vasiliev code
The classic Mollard code construction.

**Theorem 1 (Mollard M.).**

A set
\[ M^n = \{(x, a + p_1(x), b + p_2(x) + f(a)) | x \in F^{tm}, a \in A^t, b \in B^m\} \]

is a binary code of length \( n = tm + t + m \) which minimal distance equals to 3.

\[ A^t = 2^{t_1} - 1, \quad B^m = 2^{m_1} - 1 \]

\( \downarrow \)

\( M^n \) is a perfect binary code.

\[ m = 1, \quad t = 2^{t_1} - 1 \]

\( \downarrow \)

The Mollard code = the Vasiliev code.
Lemma 1.

If $A^t$ and $B^m$ are systematic codes, the Mollard code $M^n = \{(x, a + p_1(x), b + p_2(x) + f(a)) | x \in F^{tm}, a \in A^t, b \in B^m\}$ is a systematic one.
The classic Mollard code construction

- $A^t$: $(t = 2^{t_1} - 1, \frac{2^t}{t+1}, 3)$-systematic perfect code with $t - t_1$ information bits and $t_1$ redundant bits
- $B^m$: $(m = 2^{m_1} - 1, \frac{2^m}{m+1}, 3)$-systematic perfect code with $m - m_1$ information bits and $m_1$ redundant bits
- $P_1 : \mathbb{F}^{tm} \rightarrow \mathbb{F}^t$ and $P_2 : \mathbb{F}^{tm} \rightarrow \mathbb{F}^m$ – such mappings that the code distance of $(x, P_1(x), P_2(x))$ equals to 2

**Theorem 2.**

The Mollard code

$M^{tm+t+m} = \{(x, a + P_1 x, b + P_2 x + f(a)) | x \in \mathbb{F}^{tm}, a \in A^t, b \in B^m\}$

with parameters $(tm + t + m, \frac{2^{tm+t+m}}{tm+t+m+1}, 3)$ is a partially robust code with $|\text{Ker}_d(M^{tm+t+m})| = \frac{2^{tm+m}}{m+1}$ and $Q_{mc}(M^{tm+t+m}) = P_f$. 

Darya Kovalevskaya

On the Mollard code as a partially robust code
The classic Mollard code construction

- \( A^t: (t = 2^{t_1} - 1, \frac{2^t}{t+1}, 3) \)-systematic perfect code with \( t - t_1 \) information bits and \( t_1 \) redundant bits
- \( B^m: (m = 2^{m_1} - 1, \frac{2^m}{m+1}, 3) \)-systematic perfect code with \( m - m_1 \) information bits and \( m_1 \) redundant bits
- \( P_1: \mathbb{F}^{tm} \to \mathbb{F}^t \) and \( P_2: \mathbb{F}^{tm} \to \mathbb{F}^m \) – such mappings that the code distance of \((x, P_1(x), P_2(x))\) equals to 2

Theorem 2.

The Mollard code
\[
M^{tm+t+m} = \{(x, a+P_1x, b+P_2x+f(a)) | x \in \mathbb{F}^{tm}, a \in A^t, b \in B^m\}
\]
with parameters \((tm + t + m, \frac{2^{tm+t+m}}{tm+t+m+1}, 3)\) is a partially robust code with \(|Ker_d(M^{tm+t+m})| = \frac{2^{tm+m}}{m+1}\) and \(Q_{mc}(M^{tm+t+m}) = P_f\).
The generalized Mollard code construction

\( f : A^t \rightarrow F^m \) – an arbitrary nonlinear function, \( f(0) = 0 \)

**Theorem 3.**

The code

\[ \tilde{M}^n = \{(x, a + p_1(x, 0), b + p_2(x, 0) + f(a)) | x \in F^z, 0 \in F^{tm-z}, 0 < z \leq tm, a \in A^t, b \in B^m\} \]

is a partially robust code with parameters

\[ (n = z + t + m, \frac{2^z + t + m}{tm + t + m + 1}, 3), \]

where \( |Ker_d(\tilde{M}^n)| = \frac{2^z + m}{m + 1} \), and \( Q_{mc}(\tilde{M}^n) = P_f \).

Adding one linear parity check bit to \( \tilde{M}^n \), we get a partially robust code \( \bar{M}^n \) with the code distance 4, and power of detection kernel and \( \max(e \in Ker_d(D)) Q_D(e) \) like that of the code \( \tilde{M}^n \).
Definitions
The Mollard code construction
Memory protection architecture of the code $\tilde{M}^n$

$k_A = t - \log_2(t + 1), \ k_B = m - \log_2(m + 1)$

Theorem 4.
Let $\tilde{M}^n$ be the extended generalized Mollard code with parameters $(z + m + t + 1, \ \frac{2^{z+m+t}}{tm+t+m+1}, 4)$.

There are $|\text{Ker}_d| = \frac{2^{z+m}}{m+1}$ undetectable errors and $2^z \left( \frac{2^t}{t+1} - 1 \right)$ errors which are conditionally detectable.

If only errors occurred to the information part of the code are corrected, the number of miscorrected errors is $k_A(2^{z+k_A+m} - 1) + k_B2^{z+k_B} - z$ and the number of conditionally miscorrected errors is $k_Ak_B \cdot 2^{z+k_A}(2^{k_B} - 1)$.

The conditionally detectable error masking probability and the conditionally miscorrected errors miscorrection probability are limited by nonlinearity $P_f$ of function $f$. 
Table: Capabilities of Hamming, Vasiliev and Mollard codes (length 37), their detection and correction kernels

\( n = z + t + m + 1 - \text{length of } \tilde{M}^n, t - \text{length of } A^t, m - \text{length of } B^m \)

<table>
<thead>
<tr>
<th>n</th>
<th>t, m, z</th>
<th>Set</th>
<th>((H)^n)</th>
<th>(M^n)</th>
<th>(V^n)</th>
</tr>
</thead>
<tbody>
<tr>
<td>37</td>
<td>15, 7, 14</td>
<td>(C) 230</td>
<td>229 23</td>
<td>8 230 + 22 24 - 30</td>
<td></td>
</tr>
<tr>
<td>37</td>
<td>15, 3, 18</td>
<td>(C) 230</td>
<td>229 218</td>
<td>8 230 + 22 24 - 30</td>
<td></td>
</tr>
<tr>
<td>37</td>
<td>7, 15, 14</td>
<td>(C) 230</td>
<td>229 225</td>
<td>8 230 + 22 24 - 30</td>
<td></td>
</tr>
<tr>
<td>37</td>
<td>7, 7, 22</td>
<td>(C) 230</td>
<td>230 226</td>
<td>8 230 + 22 24 - 30</td>
<td></td>
</tr>
</tbody>
</table>
The Mollard code construction

Memory protection architecture of the code $\tilde{M}^n$

Table: Capabilities of Hamming, Vasiliev and Mollard codes (length 62), their detection and correction kernels

\( n = z + t + m + 1 - \text{length of } \tilde{M}^n, \ t - \text{length of } A^t, \ m - \text{length of } B^m \)

<table>
<thead>
<tr>
<th>n</th>
<th>t, m, z</th>
<th>Set</th>
<th>$\tilde{H}^n$</th>
<th>$\tilde{M}^n$</th>
<th>$\tilde{V}^n$</th>
</tr>
</thead>
<tbody>
<tr>
<td>62</td>
<td>( t = 31 )</td>
<td>( m = 15 )</td>
<td>( z = 15 )</td>
<td>(</td>
<td>C</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>( 2^{55} )</td>
<td>( 2^{26} )</td>
</tr>
<tr>
<td>62</td>
<td>( t = 31 )</td>
<td>( m = 7 )</td>
<td>( z = 23 )</td>
<td>(</td>
<td>C</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>( 2^{55} )</td>
<td>( 2^{27} )</td>
</tr>
<tr>
<td>62</td>
<td>( t = 31 )</td>
<td>( m = 3 )</td>
<td>( z = 27 )</td>
<td>(</td>
<td>C</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>( 2^{55} )</td>
<td>( 2^{28} )</td>
</tr>
<tr>
<td>62</td>
<td>( t = 15 )</td>
<td>( m = 31 )</td>
<td>( z = 15 )</td>
<td>(</td>
<td>C</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>( 2^{55} )</td>
<td>( 2^{41} )</td>
</tr>
<tr>
<td>62</td>
<td>( t = 15 )</td>
<td>( m = 3 )</td>
<td>( z = 43 )</td>
<td>(</td>
<td>C</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>( 2^{55} )</td>
<td>( 2^{44} )</td>
</tr>
<tr>
<td>62</td>
<td>( t = 7 )</td>
<td>( m = 31 )</td>
<td>( z = 23 )</td>
<td>(</td>
<td>C</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>( 2^{55} )</td>
<td>( 2^{49} )</td>
</tr>
</tbody>
</table>

Darya Kovalevskaya
On the Mollard code as a partially robust code
The number of undetectable and miscorrected multiple errors for \( \tilde{M}^n \) is much smaller than for \( \tilde{H}^n \).

If \( t = 2^\lceil \log_2 n \rceil - 1 \), the number of undetectable errors of \( \tilde{M}^n \) is less than the number of undetectable errors of \( \tilde{V}^n \). (Also, \( |\tilde{M}^n| < |\tilde{V}^n| \)).

If \( t < 2^\lceil \log_2 n \rceil - 1 \) and \( n > 2^\lceil \log_2 n \rceil + 1 - \lfloor \log_2 n \rfloor \), the number of miscorrected errors of \( \tilde{M}^n \) is less than the number of miscorrected errors of \( \tilde{V}^n \). (Also, \( |\tilde{M}^n| \leq |\tilde{V}^n| \)).

For some parameters, \( \tilde{M}^n \) have less undetectable or miscorrected errors than \( \tilde{V}^n \).

The class of different generalized Mollard codes is larger than the class of different generalized Vasil’ev codes.
Thank you for your attention!