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

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 $n = 2^m - 1,\ m \geq 2,\ d = 3$.

$\mathcal{H}^n$ – 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 $n = 2^m - 1$, $m \geq 2$, $d = 3$.

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

Definitions

A detection kernel of $D \subset \mathbf{F}^n$:
$Ker_d(D) = \{e \in \mathbf{F}^n | e + d \in D, \forall d \in D\}$.

Definitions

A detection kernel of $D \subset \mathbf{F}^n$:
$Ker_d(D) = \{e \in \mathbf{F}^n | e + d \in D, \forall d \in D\}$.

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

Definitions

A detection kernel of $D \subset \mathbf{F}^n$:
$Ker_d(D) = \{e \in \mathbf{F}^n | e + d \in D, \forall d \in D\}$.

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

Alg_D – an error correcting algorithm for D
D_{er} – a set of errors which Alg_D tries to correct

Definitions

A detection kernel of $D \subset \mathbf{F}^n$:
$Ker_d(D) = \{e \in \mathbf{F}^n | e + d \in D, \forall d \in D\}$.

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

Alg_D – an error correcting algorithm for D
D_{er} – a set of errors which Alg_D tries to correct

Definitions

A code $D \subset \mathbf{F}^n$ is a robust code if $Ker_d(D) = 0$.

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

Definitions

A code $D \subset \mathbf{F}^n$ is a robust code if $Ker_d(D) = 0$.

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

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

A systematic $(n, 2^k, d)$-code D is a partially robust code if $|Ker_d(D)| < 2^k$.

Definitions

A code $D \subset \mathbf{F}^n$ is a robust code if $Ker_d(D) = 0$.

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

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

A systematic $(n, 2^k, d)$-code D is a partially robust code if $|Ker_d(D)| < 2^k$.

The error masking probability of D:

$$Q_{mc}(D) = max_{(e \notin Ker_d(D))} Q_D(e).$$

Definitions

A code $D \subset \mathbf{F}^n$ is a robust code if $Ker_d(D) = 0$.

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

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

A systematic $(n, 2^k, d)$-code D is a partially robust code if $|Ker_d(D)| < 2^k$.

The error masking probability of D:

$$Q_{mc}(D) = max_{(e \notin Ker_d(D))} Q_D(e).$$

Definitions

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

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

Measure of the function f nonlinearity:

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

Definitions

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

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

Measure of the function f nonlinearity:

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

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

Definitions

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

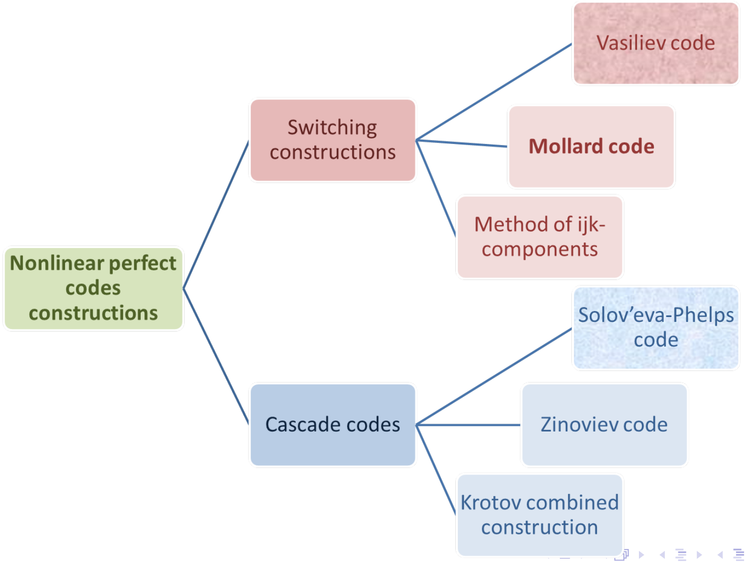
$$D_v f(x) = f(x+v) + f(x), v \in \mathbf{F}^k.$$

Measure of the function f nonlinearity:

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

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

Definitions



The Vasiliev code construction:

C^s – any perfect binary code of length s

$f : C^s \to \{0, 1\}$ – some boolean function

The Vasiiev code:

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

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

- $\star$ V^{2s+1} – a partially robust code
- $\star$ $|Ker_d(V^{2s+1})| = 2^s$
- $\star$ $Q_{mc}(V^{2s+1}) = P_f$

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, $d_B \geq 3$, $0 \in B^m$.
- $f : A^t \to \mathbf{F}^m$ – any function.
- An arbitrary vector $x \in \mathbf{F}^{tm}$:

$$x = (x_{11}, x_{12}, \ldots, x_{1m}, x_{21}, x_{22}, \ldots, x_{2m}, \ldots, x_{t1}, x_{t2}, \ldots, x_{tm}).$$

- The generalized parity check functions:

$$p_1(x) = (v_1, v_2, \ldots, v_t) \in \mathbf{F}^t, v_i = \sum_{j=1}^{m} x_{ij},$$

$$p_2(x) = (w_1, w_2, \ldots, w_m) \in \mathbf{F}^m, w_i = \sum_{i=1}^{t} x_{ij}.$$

The classic Mollard code construction.

Theorem 1 (Mollard M.).

A set
$M^n = \{(x, a + p_1(x), b + p_2(x) + f(a)) | x \in \mathbf{F}^{tm}, a \in A^t, b \in B^m\}$
is a binary code of length $n = tm + t + m$ which minimal distance equals to 3.

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

$$\Downarrow$$

M^n is a perfect binary code.

$\star$ $m = 1$, $t = 2^{t_1} - 1$

$$\Downarrow$$

The Mollard code = the Vasiliev code

The classic Mollard code construction.

Theorem 1 (Mollard M.).

A set
$M^n = \{(x, a + p_1(x), b + p_2(x) + f(a)) | x \in \mathbf{F}^{tm}, a \in A^t, b \in B^m\}$
is a binary code of length $n = tm + t + m$ which minimal distance equals to 3.

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

$$\Downarrow$$

M^n is a perfect binary code.

- $\star$ $m = 1$, $t = 2^{t_1} - 1$

$$\Downarrow$$

The Mollard code = the Vasiliev code

Lemma 1.

If A^t and B^m are systematic codes, the Mollard code $M^n = \{(x, a + p_1(x), b + p_2(x) + f(a)) | x \in \mathbf{F}^{tm}, a \in A^t, b \in B^m\}$ 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
- $P_1 : \mathbf{F}^{tm} \to \mathbf{F}^t$ and $P_2 : \mathbf{F}^{tm} \to \mathbf{F}^m$ – such mappings that the code distance of $(x, P_1(x), P_2(x))$ equals to 2

Theorem 2.

The Mollard code $M^{tm+t+m} = \{(x, a+P_1x, b+P_2x+f(a)) | x \in \mathbf{F}^{tm}, a \in A^t, b \in B^m\}$ 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 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
- $P_1 : \mathbf{F}^{tm} \to \mathbf{F}^t$ and $P_2 : \mathbf{F}^{tm} \to \mathbf{F}^m$ – such mappings that the code distance of $(x, P_1(x), P_2(x))$ equals to 2

Theorem 2.

The Mollard code $M^{tm+t+m} = \{(x, a+P_1x, b+P_2x+f(a)) | x \in \mathbf{F}^{tm}, a \in A^t, b \in B^m\}$ 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

$f : A^t \to \mathbf{F}^m$ – an arbitrary nonlinear function, $f(0) = 0$

Theorem 3.

The code

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

is a partially robust code with parameters

$$(n = z + t + m, \tfrac{2^{z+t+m}}{tm+t+m+1}, 3),$$

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 $max_{(e \notin Ker_d(D))} Q_D(e)$ like that of the code $\tilde{M}^n$.

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

Theorem 4.

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

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

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

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

$(n = z + t + m + 1 \text{ – } \textit{length of } \bar{M}^n,\ t \text{ – } \textit{length of } A^t,\ m \text{ – } \textit{length of } B^m)$

n	t, m, z	Set	$(\bar{H})^n$	$\bar{M}^n$	$\bar{V}^n$
37	$t = 31$	$\lvert C\rvert$	2^{30}	2^{29}	2^{30}
37	$m = 3$	$\lvert K_d\rvert$	2^{30}	2^3	2^4
37	$z = 2$	$\lvert K_c\rvert$	$127 \cdot 2^{30} - 37$	$52 \cdot 2^{30} - 20$	$8 \cdot 2^{30} + 22 \cdot 2^4 - 30$
37	$t = 15$	$\lvert C\rvert$	2^{30}	2^{29}	2^{30}
37	$m = 7,$	$\lvert K_d\rvert$	2^{30}	2^{18}	2^4
37	$z = 14$	$\lvert K_c\rvert$	$127 \cdot 2^{30} - 37$	$44 \cdot 2^{30} + 2^{20} - 25$	$8 \cdot 2^{30} + 22 \cdot 2^4 - 30$
37	$t = 15$	$\lvert C\rvert$	2^{30}	2^{30}	2^{30}
37	$m = 3$	$\lvert K_d\rvert$	2^{30}	2^{19}	2^4
37	$z = 18$	$\lvert K_c\rvert$	$127 \cdot 2^{30} - 37$	$44 \cdot 2^{30} + 2^{19} - 29$	$8 \cdot 2^{30} + 22 \cdot 2^4 - 30$
37	$t = 7$	$\lvert C\rvert$	2^{30}	2^{29}	2^{30}
37	$m = 15$	$\lvert K_d\rvert$	2^{30}	2^{25}	2^4
37	$z = 14$	$\lvert K_c\rvert$	$127 \cdot 2^{30} - 37$	$32 \cdot 2^{30} + 11 \cdot 2^{25} - 18$	$8 \cdot 2^{30} + 22 \cdot 2^4 - 30$
37	$t = 7$	$\lvert C\rvert$	2^{30}	2^{30}	2^{30}
37	$m = 7$	$\lvert K_d\rvert$	2^{30}	2^{26}	2^4
37	$z = 22$	$\lvert K_c\rvert$	$127 \cdot 2^{30} - 37$	$32 \cdot 2^{30} + 2^{28} - 26$	$8 \cdot 2^{30} + 22 \cdot 2^4 - 30$

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

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

n	**t, m, z**	**Set**	$\bar{\mathbf{H}}^{\mathbf{n}}$	$\bar{\mathbf{M}}^{\mathbf{n}}$	$\bar{\mathbf{V}}^{\mathbf{n}}$
62	$t = 31$	$\|C\|$	2^{55}	2^{52}	2^{55}
62	$m = 15$	$\|K_d\|$	2^{55}	2^{26}	2^{29}
62	$z = 15$	$\|K_c\|$	$127 \cdot 2^{55} - 62$	$26 \cdot 2^{56} + 11 \cdot 2^{26} - 41$	$26 \cdot 2^{56} + 3 \cdot 2^{26} - 55$
62	$t = 31$	$\|C\|$	2^{55}	2^{53}	2^{55}
62	$m = 7$	$\|K_d\|$	2^{55}	2^{27}	2^{29}
62	$z = 23$	$\|K_c\|$	$127 \cdot 2^{55} - 62$	$26 \cdot 2^{56} + 2^{29} - 40$	$26 \cdot 2^{56} + 3 \cdot 2^{26} - 55$
62	$t = 31$	$\|C\|$	2^{55}	2^{54}	2^{55}
62	$m = 3$	$\|K_d\|$	2^{55}	2^{28}	2^{29}
62	$z = 27$	$\|K_c\|$	$127 \cdot 2^{55} - 62$	$26 \cdot 2^{56} + 2^{28}$	$26 \cdot 2^{56} + 3 \cdot 2^{26} - 55$
62	$t = 15$	$\|C\|$	2^{55}	2^{52}	2^{55}
62	$m = 31$	$\|K_d\|$	2^{55}	2^{41}	2^{29}
62	$z = 15$	$\|K_c\|$	$127 \cdot 2^{55} - 62$	$22 \cdot 2^{56} + 26 \cdot 2^{41} - 26$	$26 \cdot 2^{56} + 3 \cdot 2^{26} - 55$
62	$t = 15$	$\|C\|$	2^{55}	2^{55}	2^{55}
62	$m = 3$	$\|K_d\|$	2^{55}	2^{44}	2^{29}
62	$z = 43$	$\|K_c\|$	$127 \cdot 2^{55} - 62$	$22 \cdot 2^{56} + 2^{44} - 54$	$26 \cdot 2^{56} + 3 \cdot 2^{26} - 55$
62	$t = 7$	$\|C\|$	2^{55}	2^{53}	2^{55}
62	$m = 31$	$\|K_d\|$	2^{55}	2^{49}	2^{29}
62	$z = 23$	$\|K_c\|$	$127 \cdot 2^{55} - 62$	$16 \cdot 2^{56} + 26 \cdot 2^{49} - 27$	$26 \cdot 2^{56} + 3 \cdot 2^{26} - 55$

$\star$ The number of undetectable and miscorrected multiple errors for $\bar{M}^n$ is much smaller than for $\bar{\mathcal{H}}^n$.

$\star$ If $t = 2^{\lfloor log_2 n \rfloor} - 1$, the number of undetectable errors of $\bar{M}^n$ is less than the number of undetectable errors of $\bar{V}^n$.
(Also,$|\bar{M}^n| < |\bar{V}^n|$).

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

$$\Downarrow$$

$\star$ For some parameters, $\bar{M}^n$ have less undetectable or miscorrected errors than $\bar{V}^n$.

$\star$ The class of different generalized Mollard codes is larger than the class of different generalized Vasil'ev codes.

Thank you for your attention!