On the Triple-Error-Correcting Cyclic Codes with Zero Set $\{1, 2^i + 1, 2^j + 1\}$

Vincent Herbert[1] (Joint work with Sumanta Sarkar[2])

IMACC 2011

[1] Inria Paris-Rocquencourt, France

[2] University of Calgary, Canada

Agenda

1. 3-error-correcting cyclic codes

2. Equivalence of codes with 3-error-correcting BCH code

3. Lower bound on spectral immunity of a Boolean function

What are cyclic codes?

Set $m > 0$, q a prime power and $n \mid q^m - 1$.

Consider α a primitive n^{th} root of unity in $\mathbb{F}_{q^m}$ and denote $M^{(i)}(x)$, the minimal polynomial of α^i over $\mathbb{F}_q$.

A cyclic code of length n on $\mathbb{F}_q$ is defined by:

- Zero Set $Z \subseteq [\![1, n]\!]$.
- Generator polynomial $g \in \mathbb{F}_q[x]$, $g(x) = \text{lcm}(\{M^{(z)}(x)\}_{z \in Z})$.

It consists in the ideal of the ring $\mathbb{F}_q[x]/(x^n - 1)$ generated by g.

In our case, we consider $n = 2^m - 1$.

One example: BCH code

$\{1, 3, 5\}$ is the zero set of the binary 3-error-correcting BCH code.

Henceforth, we denominate this code, the 3-BCH code.

The q-cyclotomic coset of i modulo n is the set:

$$C_i = \{(iq^j \mod n) \in \mathbb{Z}_n : j \in \mathbb{N}\}.$$

Set $q = 2$ and $n = 2^4 - 1$.

$$C_1 = \{1, 2, 4, 8\}, \quad C_3 = \{3, 6, 12, 9\}, \quad C_5 = \{5, 10\}.$$

How many errors can a cyclic code correct?

A code is *t-error-correcting* if its minimum distance is $2t + 1$.

Consider primitive, binary and cyclic codes.

Five classes of 3-error-correcting codes have been identified in 40 years.

We ignore how to compute efficiently the minimum distance of a cyclic code.

Known classes of 3-error-correcting cyclic codes

Zero Set	Conditions	Year
$\{1, 2^{\ell}+1, 2^{3\ell}+1\}$	$\gcd(\ell, m) = 1$ odd m	1971
$\{2^{\ell}+1, 2^{3\ell}+1, 2^{5\ell}+1\}$	$\gcd(\ell, m) = 1$ odd m	1971
$\{1, 2^{\ell+1}+1, 2^{\ell+2}+3\}$	$m = 2\ell + 1$ odd m	2000
$\{1, 2^{\ell}+1, 2^{2\ell}+1\}$	$\gcd(\ell, m) = 1$ any m	2009
$\{1, 3, 13\}$	odd m	2010

Sufficient condition to be 3-error-correcting

For all m, a code with the zero set

$$\left\{1, 2^{\ell}+1, 2^{p\ell}+1\right\} \quad \text{where } \gcd(\ell, m) = 1$$

is 3-error-correcting if for all $\beta \in \mathbb{F}_{2^m}^*, \gamma \in \mathbb{F}_{2^m}$, the equation:

$$x^{2^{p\ell}+1} \sum_{i=0}^{p-1} \left(\beta x^{-(2^{\ell}+1)}\right)^{2^{i\ell}} = \gamma$$

has at most 5 solutions in $\mathbb{F}_{2^m}^*$.

Search for new 3-error-correcting cyclic code

Consider the cyclic codes with the zero set:

$$\left\{1, 2^i + 1, 2^j + 1\right\} \quad \text{where } \gcd(i, m) = 1.$$

It is known that their minimum distance d verifies:

$$d \in \{5, 7\}$$

and that there exist codewords of weight $d + 1$.

We employ Chose-Joux-Mitton algorithm to search for codewords of weight 6 in these codes.

No new 3-error-correcting cyclic code in this form for $m < 20$.

What is the equivalence of codes?

Two binary linear codes are equivalent if they are equal up to a permutation of the coordinates.

How do we determine the equivalence of codes?

Two equivalent codes share:

- the length
- the dimension
- the minimum distance
- the weight distribution of the code
- the weight distribution of the hull
- etc.

These invariants provide necessary conditions but not sufficient ones to determine the equivalence between two codes.

Studied codes are self-orthogonal. Their hull is their dual code.

Numerical results

None of the 3-error-correcting cyclic codes with the zero set:

$$\left\{1, 2^i + 1, 2^j + 1\right\} \quad \text{where } i \neq j$$

is equivalent to the 3-BCH code for $m = 7$, $m = 8$ and $m = 10$.

For $m = 7$ and $m = 8$, we employ Magma (Leon's algorithm).

For $m = 10$, we apply the support splitting algorithm.

The used invariant to determine the non-equivalence is the multiset of weight distributions of punctured codes.

An example to understand better

Let C be the cyclic code with $Z = \{1, 9, 17\}$ and the 3-BCH code.

Their codimensions are less than $3m$.

Their weight distributions are identical for $m = 9$ and $m = 10$.

We puncture $C^{\perp}$ and the dual of the 3-BCH code in any position.

We puncture the codes a second time in each position.

- $m = 9$
  - The multisets possess a unique and same element.
  - 250 000 weight distributions to compute to go forward.
  - We can not conclude on the question of equivalence.
- $m = 10$
  - The multisets possess 8 and 10 elements.
  - C is not equivalent with the 3-BCH code.

How to find a lower bound the minimum distance of a cyclic code?

In theory, many lower bounds are known.

A number of them is based on the regular distribution of patterns contained in the zero set.

- BCH bound (1960)
- Hartmann-Tzeng bound (1972)
- Roos bound (1982)
- van Lint-Wilson bounds (1986)
- etc.

In practice, van Lint-Wilson bounds are hard to compute.

We employ Schaub algorithm which takes a different approach.

How does Schaub algorithm work?

A subcode of a cyclic code C is said zero-constant if its codewords possess exactly the same zeroes.

We associate to each zero-constant subcodes of C, a circulant matrix defined on a semiring $\{0, 1, X\}$,

$$\begin{pmatrix} B_0 & B_1 & \dots & B_{n-2} & B_{n-1} \\ B_1 & B_2 & \dots & B_{n-1} & B_0 \\ \vdots & \vdots & & \vdots & \vdots \\ B_{n-1} & B_0 & \dots & B_{n-3} & B_{n-2} \end{pmatrix},$$

where $B_i = 0$ if i is a zero of the subcode and $B_i = 1$ elsewhere.

How does Schaub algorithm work? (cont.)

The zero-constant subcodes form a partition of the code C.

We lower bound their minimal weight by using the laws:

$+$	0	1	X
0	0	1	X
1	1	X	X
X	X	X	X

$*$	0	1	X
0	0	0	0
1	0	1	X
X	0	X	X

The minimum value obtained is the Schaub bound.

Let κ be the number of cyclotomic cosets which do not belong to Z.

- $\#$ constant-zero subcodes of $C = 2^\kappa$
- Rank bounding algorithm $\mathcal{O}(n^3)$

How do we optimize Schaub algorithm?

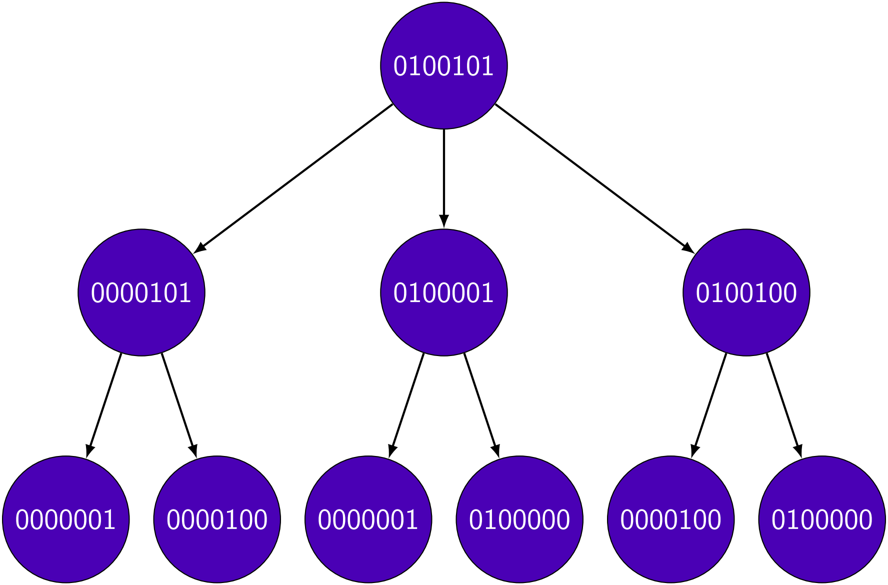
We represent the zero-constant subcodes of C by a tree.

We decrease the number of treated subcodes by identifying equivalent matrices as well as the size of considered matrices.

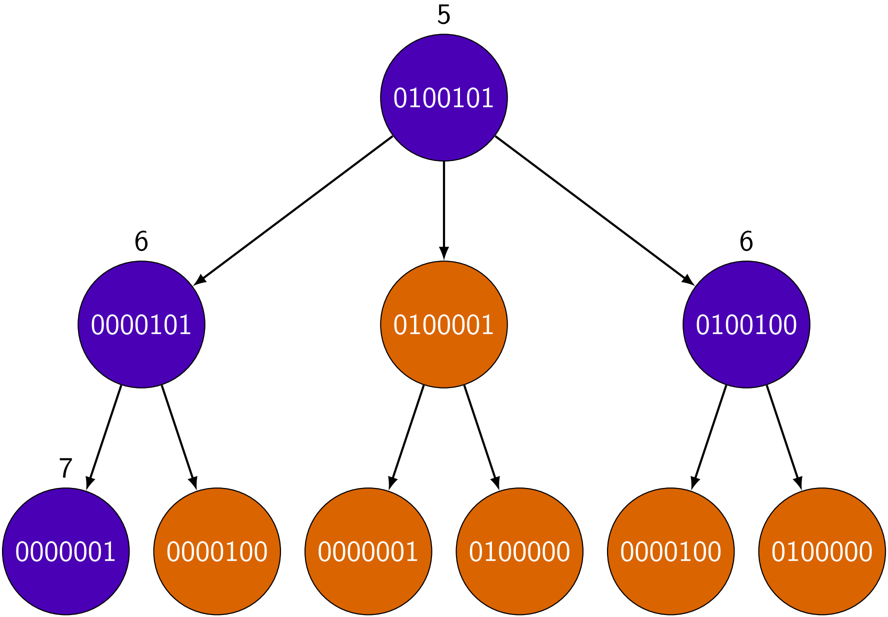
We prune the subcodes whose root is a node where the BCH bound is greater than the computed Schaub bound.

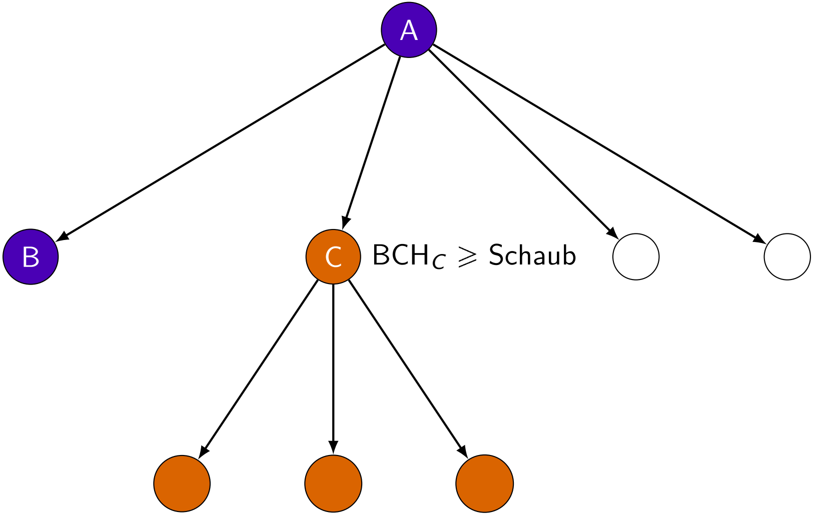
Computation time is longer if we use Hartmann-Tzeng bound.

$q = 8,\ n = 7,\ Z = \{1, 3, 4, 6\}.$


0100101
0000101
0100001
0100100
0000001
0000100
0000001
0100000
0000100
0100000

$q = 8,\ n = 7,\ Z = \{1, 3, 4, 6\}.$


5
0100101
6
0000101
0100001
6
0100100
7
0000001
0000100
0000001
0100000
0000100
0100000


A
B
C
$\mathrm{BCH}_C \geqslant \mathrm{Schaub}$

Spectral immunity and cyclic codes

We employ our version of Schaub algorithm to lower bound spectral immunity of Boolean functions.

Let f be a Boolean function in univariate form on $\mathbb{F}_{2^m}$.

The spectral immunity of f is the minimal weight in the 2^m-ary cyclic codes of length $n = 2^m - 1$ with the generator polynomials:

$$G(x) = \gcd(f(x), x^n + 1)$$

$$H(x) = \frac{x^n + 1}{G(x)}$$

Tor Helleseth and Sondre Rønjom.
Simplifying algebraic attacks with univariate analysis. ITA 2011

An instance and some figures

Let g be the generator polynomial of the 3-BCH code.

Code length	Lower bound spectral immunity $\mathrm{Tr}(g(x))$	$\deg(G)$	$\deg(H)$
127	11	56	71
255	14	139	116

G and H possess binary coefficients.

- $m = 8$
  - $2^{20} \simeq$ one million of treated constant-zero subcodes.
  - Rank bounding in $\mathcal{O}(2^{24})$.
  - We compute the Schaub bound in 13 hours.
  - Exhaustive search in $\mathcal{O}(2^{119})$.
  - Hartmann-Tzeng bound $= 9$ vs. Schaub bound $= 14$.

Conclusions & Perspectives

- We have presented a sufficient condition so that $\{1, 2^{\ell} + 1, 2^{p\ell} + 1\}$ corresponds to a 3-error-correcting cyclic code.
- The codes with $Z = \{1, 2^{i} + 1, 2^{j} + 1\}$ are not equivalent to the 3-BCH code in general, this supports the conjecture proposed in 1977 by Sloane and MacWilliams.
- We have improved the Schaub algorithm by pruning the tree of zero-constant subcodes at low-cost.
- This improved algorithm can be used to find a lower bound of the minimum distance of some other classes of q-ary cyclic codes.

Thank you very much IMACC 2011!

Any questions or comments?

Any further remarks or suggestions can be adressed at:

vincent.herbert@inria.fr

sarkas@ucalgary.ca

Slides will be available in a short time on:

`http://www-roc.inria.fr/secret/Vincent.Herbert/`

How does Schaub algorithm work?

It rests upon a result of Blahut.

Set q a prime power and α a primitive root of $\mathbb{F}_{q^m}$.

The weight of a word c of a n-length q-ary cyclic code is equal to the rank of the circulant matrix of order n,

$$\begin{pmatrix} A_0 & A_1 & \dots & A_{n-2} & A_{n-1} \\ A_1 & A_2 & \dots & A_{n-1} & A_0 \\ \vdots & \vdots & & \vdots & \vdots \\ A_{n-1} & A_0 & \dots & A_{n-3} & A_{n-2} \end{pmatrix},$$

where $A_i := c(\alpha^i)$.

Lower bound of the spectral immunity

Code length	Zero set	Lower bound spectral immunity $\mathrm{Tr}(g(x))$
127	$\{1,3,5\}$	11
	$\{1,3,9\}$	13
	$\{1,5,9\}$	12
255	$\{1,3,5\}$	14
	$\{1,5,9\}$	14

- g generator of a 3-error-correcting cyclic code $Z = \{1, 2^i + 1, 2^j + 1\}$.
- $x \mapsto \mathrm{Tr}(g(x))$ Boolean function on $\mathbb{F}_{2^m}$.
- $G(x) = \gcd(\mathrm{Tr}(g(x)), x^n + 1), \quad H(x) = \dfrac{x^n + 1}{G(x)}$.
- G and H possess binary coefficients.

How do we compute the weight distribution?

Consider a binary cyclic code C with $Z = \{1, a, b\}$.

The codimension of C is less than $3m$.

We construct its parity check matrix of size $(3m \times n)$.

$$\begin{pmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{(n-1)} \\ 1 & \alpha^a & \alpha^{2a} & \dots & \alpha^{(n-1)a} \\ 1 & \alpha^b & \alpha^{2b} & \dots & \alpha^{(n-1)b} \end{pmatrix}$$

We generate the words of the dual by using the Gray coding.

We compute their Hamming weight with an instruction SSE4.

Numerical results

Every 3-error-correcting cyclic codes with the zero set:

$$\left\{1, 2^i + 1, 2^j + 1\right\} \quad \text{where } i \neq j$$

possess the same weight distribution as the 3-BCH code for $m < 14$.

The weight distribution for odd m

The weight distribution of 3-BCH code is known for odd m.

The weight distribution of codes with the zero set:

$$Z = \left\{ 1, 2^i + 1, 2^j + 1 \right\} \quad \text{where } \gcd(i, m) = 1.$$

is identical to the one of 3-BCH code for odd m.

We prove it as a corollary of a theorem by Kasami.

Tadao Kasami. Weight Distributions of BCH Codes.
Combinatorial Mathematics and Its Applications, 1969.

Spectral immunity and cyclic codes

The concept of spectral immunity of a Boolean function appeared recently.

Boolean functions with low spectral immunity are not desired since algebraic attacks on certain stream ciphers can be mounted.

G. Gong, S. Rønjom, T. Helleseth, and H. Hu. Fast discrete Fourier spectra attacks on stream ciphers. IEEE Transactions on Information Theory, 2011.

We can compute this quantity by determining the minimum distance of primitive cyclic codes on $\mathbb{F}_{2^m}$.

We make use of our version of Schaub algorithm to lower bound spectral immunity of Boolean functions.