On a class of binary cyclic codes with an increasing gap between the BCH bound and the van Lint–Wilson bound

Valeriy Lomakov
<vl@guap.ru>

Saint Petersburg State University of
Aerospace Instrumentation

Algebraic and Combinatorial Coding Theory ACCT2012
June 15-21, 2012, Pomorie, Bulgaria

Overview

We define and study a family of binary cyclic codes of

- length $n = 2^{2(\ell+1)} - 1$
- and dimension $k = 2^{\ell+2}(2^{\ell} - 1)$

with

- the Bose–Ray-Chaudhuri–Hocquenghem bound $\delta_{BCH} = 4$,
- and the van Lint–Wilson bound $\delta_{LW} \geq 2(\ell + 1)$.

These codes can be decoded up to the designed distance $2(\ell + 1)$.

The binary number system

Every nonnegative integer can be written by a string of 1's and 0's

$$\forall v \geq 0: \;\; v = \nu_0 + \nu_1 2 + \nu_2 2^2 + \nu_3 2^3 + \ldots.$$

The binary representation defines a number *uniquely*, e.g.

$$477 = 1 + 0 \cdot 2 + 1 \cdot 2^2 + 1 \cdot 2^3 + 1 \cdot 2^4 + 0 \cdot 2^5 + 1 \cdot 2^6 + \\ +1 \cdot 2^7 + 1 \cdot 2^8 + \cdots \leftrightarrow \blacksquare\square\blacksquare\blacksquare\blacksquare\square\blacksquare\blacksquare\blacksquare \ldots.$$

And

$$\underbrace{\blacksquare\blacksquare\blacksquare \ldots \blacksquare}_{2\ell+1} \square\square \cdots \leftrightarrow 2^{2(\ell+1)} - 1.$$

Integers in base four

Let W be the infinite set of all nonnegative integers which are *the sum of distinct powers of* 4, i.e.

$$\forall w \in W: \; w = \omega_0 + \omega_2 4 + \omega_4 4^2 + \omega_6 4^3 + \dots .$$

The first few elements of W are

0	□□□□□□□□ ...	64	□□□□□□■□ ...
1	■□□□□□□□ ...	65	■□□□□□■□ ...
4	□□■□□□□□ ...	68	□□■□□□■□ ...
5	■□■□□□□□ ...	69	■□■□□□■□ ...
16	□□□□■□□□ ...	80	□□□□■□■□ ...
17	■□□□■□□□ ...	81	■□□□■□■□ ...
20	□□■□■□□□ ...	84	□□■□■□■□ ...
21	■□■□■□□□ ...	85	■□■□■□■□ ...

First integers in base four

The base four representation defines a number *uniquely* and W with the usual definition of $<$ is a *strict total ordered set*:

$$0 < 1 < 4 < 5 < 16 < 17 < 20 < 21 < 64 < 65 < 68 < 69 < 80 < 81 < \ldots.$$

Definition

For each $\ell \geq 0$, let W_ℓ be the first $2^{\ell+1}$ elements of W, i.e.

ℓ	W_ℓ	w	$B_\ell(w)$
0	$\{0\}$	0	□□
1	$\{0, 1, 4, 5\}$	5	■□■□
2	$\{0, 1, 4, 5, 16, 17, 20, 21\}$	21	■□■□■□
3	$\{0, 1, 4, 5, 16, 17, 20, 21, 64, 65, 68, 69, 80, 81, 84, 85\}$	85	■□■□■□■□

and $w < 2^{2(\ell+1)}$.

A class of binary cyclic codes

A binary cyclic code has

- blocklength n,
- dimension k,
- generator polynomial $g(x) \in GF(2)[x]$,
- minimum distance d,
- defining set $R \subset \{0, 1, 2, \ldots, n-1\}$,
- complete defining set $Z \subseteq R$.

Definition

For $\ell \geq 1$, consider a cyclic code of length $n = 2^{2(\ell+1)} - 1$ over $GF(2)$ whose defining set $R = W_\ell$.

Roots of the (binary) code

Consider the sets W_ℓ and $2W_\ell$, e.g.

w	$B_\ell(w)$	$2w$	$B_\ell(2w)$
0	□□□□□□	0	□□□□□□
1	■□□□□□	2	□■□□□□
4	□□■□□□	8	□□□■□□
5	■□■□□□	10	□■□■□□
16	□□□□■□	32	□□□□□■
17	■□□□■□	34	□■□□□■
20	□□■□■□	40	□□□■□■
21	■□■□■□	42	□■□■□■

Then $W_\ell \leftrightarrow 2W_\ell$, and $|W_\ell| = |2W_\ell|$, and $W_\ell \cap 2W_\ell = \{0\}$.

The maximal elements

Consider the strict total ordered sets W_ℓ:

$$0 < 1 < 4 < 5 < 16 < 17 < 20 < 21 < 64 < 65 < \cdots < w^*,$$

and $2W_\ell$:

$$0 < 2 < 8 < 10 < 32 < 34 < 40 < 42 < 128 < 130 < \cdots < 2w^*$$

with the maximal elements:

$$\begin{array}{rcll} & w^* & = & \blacksquare\square\blacksquare\square\ldots\blacksquare\square \\ + & & & \\ & 2w^* & = & \square\blacksquare\square\blacksquare\square\ldots\blacksquare \\ \hline & 3w^* & = & \blacksquare\blacksquare\blacksquare\blacksquare\blacksquare\ldots\blacksquare \quad = \quad n \end{array}$$

Then $w^* = \frac{1}{3}n$, and $2w^* = \frac{2}{3}n$, and $\forall w \in (W_\ell \cup 2W_\ell) : \; w < n$.

Cyclotomic cosets

For bynary codes a cyclotomic coset containing w consists of

$$w \to 2w \pmod{n} \to 2^2 w \pmod{n} \to 2^3 w \pmod{n} \to \cdots \to w$$

or

$$\cdots \to \in W_\ell \to \in 2W_\ell \to \in W_\ell \to \in 2W_\ell \to \in W_\ell \to \in 2W_\ell \to \ldots.$$

For $W_2 = \{0, 1, 4, 5, 16, 17, 20, 21\}$ and $2W_2 = \{\underline{0}, \underline{2}, \underline{8}, \underline{10}, \underline{32}, \underline{34}, \underline{40}, \underline{42}\}$, e.g.

$$\begin{aligned} C_0 &= \{0\}, \\ C_1 &= \{1, \underline{2}, 4, \underline{8}, 16, \underline{32}\}, \\ C_5 &= \{5, \underline{10}, 20, \underline{40}, 17, \underline{34}\}, \\ C_{21} &= \{21, \underline{42}\}. \end{aligned}$$

The complete defining set and the dimension

Lemma

The code has the complete defining set $Z = W_\ell \cup 2W_\ell$.

Theorem

The dimension of the code is $k = 2^{\ell+2}(2^\ell - 1)$.

Proof.

$$k = n - |Z| = (2^{2(\ell+1)} - 1) - (2 \cdot 2^{\ell+1} - 1) = 2^{\ell+1}(2^\ell - 1).$$

□

E.g.

n	k	Z
15	8	$\{0, 1, 2, 4, 5, 8, 10\}$
63	48	$\{0, 1, 2, 4, 5, 8, 10, 16, 17, 20, 21, 32, 34, 40, 42\}$
255	224	$\{0, 1, 2, 4, 5, 8, 10, 16, 17, 20, 21, 32, 34, 40, 42, 64, 65, \dots, 170\}$
...	...	...

The BCH bound

For some nonnegative integers a and c, where $\gcd(c,n)=1$, the set

$$S=\{a+ic \pmod n \mid 0\le i\le \delta_{BCH}-2\}$$

is a subset or equal to Z and $|S|=\delta_{BCH}-1$.

Lemma

The BCH bound of the code is $\delta_{BCH}\ge 4$.

Proof.

$S=\{0,1,2\}\subset (W_1\cup 2W_1)\subset (W_2\cup 2W_2)\subset (W_3\cup 2W_3)\subset \dots$. □

If $\delta_{BCH}\ge 5$, then

$$S=\{a, a+c \pmod n, a+2c \pmod n, a+3c \pmod n\}=\{a,b,v,w\}\subseteq Z$$

where $w=3b-2a \pmod n$ and $a,b\in Z$.

The generating function

Consider the generating function

$$P(z) = \underbrace{F(z) + F(z^2) - 1}_{Z}$$

where $F(z) = (1+z)(1+z^4)(1+z^{16})(1+z^{64})\dots$ and

$$W(z) = \underbrace{P(z^3)P(z^{-2}) \pmod{z^n - 1}}_{w=3b-2a \pmod{n}} = \sum_{i=0}^{n-1} w_i z^i.$$

For $W_2 = \{0,1,4,5,16,17,20,21\}$ and $2W_2 = \{0,2,8,10,32,34,40,42\}$, e.g.

$$P(z) = z^{42} + z^{40} + z^{34} + z^{32} + z^{21} + z^{20} + z^{17} + z^{16} + z^{10} + \\ + z^8 + z^5 + z^4 + z^2 + z + 1$$

The number of representations

And

ℓ	$w_i \in Z$
1	$[3, 3, 3^{1)}, 3, \underline{5}, 3, \underline{5}^{2)}]$
2	$[3, 3, 3, 3, 3, 3, 3, 3, 3^{3)}, 3, \underline{3}, 3, 3, 3, \underline{3}]$
3	$[3, 3, 3, \ldots, 3, \underline{5}, 3, \ldots, 3, \underline{5}]$
4	$[3, 3, 3, \ldots, 3, \underline{3}, 3, \ldots, 3, \underline{3}]$
5	$[3, 3, 3, \ldots, 3, \underline{5}, 3, \ldots, 3, \underline{5}]$
$\ldots$	$\ldots$

where

$$^{1)}2 = 3 \cdot \underbrace{2}_{b} - 2 \cdot \underbrace{2}_{a} = 3 \cdot \underbrace{4}_{b} - 2 \cdot \underbrace{5}_{a} = 3 \cdot \underbrace{1}_{b} - 2 \cdot \underbrace{8}_{a} \pmod{15}$$

$$^{2)}10 = 3 \cdot 4 - 2 \cdot 1 = 3 \cdot 1 - 2 \cdot 4 = 3 \cdot 0 - 2 \cdot 10 = 3 \cdot 5 - 2 \cdot 10 = \\ = 3 \cdot 10 - 2 \cdot 10 \pmod{15}$$

$$^{3)}17 = 3 \cdot 32 - 2 \cdot 8 = 3 \cdot 17 - 2 \cdot 17 = 3 \cdot 40 - 2 \cdot 20 \pmod{63}$$

Four consecutive roots

For $\ell = 2$, e.g.

S	Case	S	Case
$\{0,0,0,0\}$	$\{a,a,a,a\}$	$\{0,21,42,0\}$	$\{0,\frac{1}{3}n,\frac{2}{3}n,0\}$
$\{0,42,21,0\}$	$\{0,\frac{2}{3}n,\frac{1}{3}n,0\}$	$\{17,17,17,17\}$	$\{a,a,a,a\}$
$\{34,34,34,34\}$	$\{a,a,a,a\}$	$\{1,1,1,1\}$	$\{a,a,a,a\}$
$\{2,2,2,2\}$	$\{a,a,a,a\}$	$\{20,20,20,20\}$	$\{a,a,a,a\}$
$\{4,4,4,4\}$	$\{a,a,a,a\}$	$\{21,0,42,21\}$	$\{\frac{1}{3}n,0,\frac{2}{3}n,\frac{1}{3}n\}$
$\{21,21,21,21\}$	$\{a,a,a,a\}$	$\{21,42,0,21\}$	$\{\frac{1}{3}n,\frac{2}{3}n,0,\frac{1}{3}n\}$
$\{5,5,5,5\}$	$\{a,a,a,a\}$	$\{40,40,40,40\}$	$\{a,a,a,a\}$
$\{8,8,8,8\}$	$\{a,a,a,a\}$	$\{42,0,21,42\}$	$\{\frac{2}{3}n,0,\frac{1}{3}n,\frac{2}{3}n\}$
$\{42,21,0,42\}$	$\{\frac{2}{3}n,\frac{1}{3}n,0,\frac{2}{3}n\}$	$\{42,42,42,42\}$	$\{a,a,a,a\}$
$\{10,10,10,10\}$	$\{a,a,a,a\}$	$\{32,32,32,32\}$	$\{a,a,a,a\}$
$\{16,16,16,16\}$	$\{a,a,a,a\}$		

In all cases (7), $a = a + 3c \pmod{n}$ and $\delta_{BCH} < 5$.

The BCH bound of the code

Theorem

The BCH bound of the code is $\delta_{BCH} = 4$.

Proof.

$\delta_{BCH} \geq 4$ and $\delta_{BCH} < 5$. □

E.g.

n	k	δ_{BCH}
15	8	4
63	48	4
255	224	4
…	…	…

The van Lint–Wilson bound

- The empty set is independent with respect to S;
- If A is independent with respect to S, and $A \subseteq S$, and $b \notin S$, then $A \cup \{b\}$ is independent with respect to S;
- If A is independent with respect to S and $0 < c < n$, then $\{c + a \,|\, a \in A\}$ is independent with respect to S.

δ_{LW} is the maximal size of a set which is independent with respect to Z.
Since

$$\begin{aligned} a_0 = 0, b_0 = 3 &: A_1 = \{\underline{3}\}, \\ a_1 = 14, b_1 = 3 &: A_2 = \{2, \underline{3}\}, \\ a_2 = 14, b_2 = 3 &: A_3 = \{1, 2, \underline{3}\}, \\ a_3 = 14, b_3 = 3 &: A_4 = \{0, 1, 2, \underline{3}\}, \end{aligned}$$

then $\delta_{LW} \geq \delta_{BCH}$ (for $\ell = 1$).

The van Lint–Wilson bound of the code

$\ell = 2\,(n = 63)$		$\ell = 3\,(n = 255)$	
$a_0 = 0, b_0 = 3$:	$A_1 = \{\underline{3}\}$,	$a_0 = 0, b_0 = 3$:	$A_1 = \{\underline{3}\}$,
$a_1 = 62, b_1 = 18$:	$A_2 = \{2, \underline{18}\}$,	$a_1 = 254, b_1 = 66$:	$A_2 = \{2, \underline{66}\}$,
$a_2 = 3, b_2 = 6$:	$A_3 = \{5, 21, \underline{6}\}$,	$a_2 = 15, b_2 = 33$:	$A_3 = \{17, 81, \underline{33}\}$,
$a_3 = 59, b_3 = 18$:	$A_4 = \{1, 17, 2, \underline{18}\}$,	$a_3 = 243, b_3 = 6$:	$A_4 = \{5, 69, 21, \underline{6}\}$,
$a_4 = 3, b_4 = 6$:	$A_5 = \{4, 20, 5, 21, \underline{6}\}$,	$a_4 = 251, b_4 = 66$:	$A_5 = \{1, 65, 17, 2, \underline{66}\}$,
$a_5 = 59, b_5 = 3$:	$A_6 = \{0, 16, 1, 17, 2, \underline{3}\}$.	$a_5 = 15, b_5 = 33$:	$A_6 = \{16, 80, 32, 17, 81, \underline{33}\}$,
		$a_6 = 243, b_6 = 6$:	$A_7 = \{4, 68, 20, 5, 69, 21, \underline{6}\}$,
		$a_7 = 251, b_7 = 3$:	$A_8 = \{0, 64, 16, 1, 65, 17, 2, \underline{3}\}$.
$\delta_{LW} \geq 6$		$\delta_{LW} \geq 8$	

Theorem

The van Lint–Wilson bound of the code is $\delta_{LW} \geq 2(\ell + 1)$.

E.g.

n	k	δ_{BCH}	δ_{LW}
15	8	4	4
63	48	4	6
255	224	4	8
$\dots$	$\dots$	$\dots$	$\dots$

Decoding

Consider the $2(\ell+1) \times 2(\ell+1)$ submatrix of the syndrome matrix:

$$
\begin{array}{c|cccccccccccc}
 & 2^1+2^0 & 2^1 & 2^4+2^0 & \cdots & 2^{2(l-1)}+2^0 & 2^{2l}+2^0 & 2^0 & 2^4 & \cdots & 2^{2(l-1)} & 2^{2l} & 0 \\
\hline
0 & \underline{S_{2^1+2^0}} & \boxed{S_{2^1}} & S_{2^4+2^0} & \cdots & S_{2^{2(l-1)}+2^0} & S_{2^{2l}+2^0} & S_{2^0} & S_{2^4} & \cdots & S_{2^{2(l-1)}} & S_{2^{2l}} & S_0 \\
2^2 & & \underline{S_{2^2+2^1}} & S_{2^4+2^2+2^0} & \cdots & S_{2^{2(l-1)}+2^2+2^0} & S_{2^{2l}+2^2+2^0} & S_{2^2+2^0} & S_{2^4+2^2} & \cdots & S_{2^{2(l-1)}+2^2} & S_{2^{2l}+2^2} & S_{2^2} \\
2^4 & & & \underline{S_{2^5+2^0}} & \cdots & S_{2^{2(l-1)}+2^4+2^0} & S_{2^{2l}+2^4+2^0} & S_{2^4+2^0} & \boxed{S_{2^5}} & \cdots & S_{2^{2(l-1)}+2^4} & S_{2^{2l}+2^4} & S_{2^4} \\
\vdots & & & & \ddots & \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\
2^{2(l-1)} & & & & & \underline{S_{2^{2(l-1)}+2^0}} & S_{2^{2l}+2^{2(l-1)}+2^0} & S_{2^{2(l-1)}+2^0} & S_{2^{2(l-1)}+2^4} & \cdots & \boxed{S_{2^{2l-1}}} & S_{2^{2l}+2^{2(l-1)}} & S_{2^{2(l-1)}} \\
2^0 & & & & & & \underline{S_{2^{2l}+2^1}} & \boxed{S_{2^1}} & S_{2^4+2^0} & \cdots & S_{2^{2(l-1)}+2^0} & S_{2^{2l}+2^0} & S_{2^0} \\
2^2+2^0 & & & & & & & \underline{S_{2^2+2^1}} & S_{2^4+2^2+2^0} & \cdots & S_{2^{2(l-1)}+2^2+2^0} & S_{2^{2l}+2^2+2^0} & S_{2^2+2^0} \\
2^4+2^0 & & & & & & & & \underline{S_{2^5+2^0}} & \cdots & S_{2^{2(l-1)}+2^4+2^0} & S_{2^{2l}+2^4+2^0} & S_{2^4+2^0} \\
\vdots & & & & & & & & & \ddots & \vdots & \vdots & \vdots \\
2^{2(l-1)}+2^0 & & & & & & & & & & \underline{S_{2^{2l-1}+2^0}} & S_{2^{2l}+2^{2(l-1)}+2^0} & S_{2^{2(l-1)}+2^0} \\
2^1 & & & & & & & & & & & \underline{S_{2^{2l}+2^1}} & \boxed{S_{2^1}} \\
2^1+2^0 & & & & & & & & & & & & \underline{S_{2^1+2^0}}
\end{array}
$$

- $2^a + 2^b \in Z$ and $2^a + 2^b + 2^c \in Z$ if a, b, c are even;
- $\boxed{2^a} \in Z$;
- $\underline{2^a + 2^c} \notin Z$ if a is odd and c is even.