Thirteenth International Workshop on Algebraic and Combinatorial Coding Theory
June 15-21, 2012, Pomorie, Bulgaria *pp. 246–251*

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
St. Petersburg State University of Aerospace Instrumentation
190000, Bolshaya Morskaya, 67, St. Petersburg, Russia

Abstract. A class of binary cyclic $\left(2^{2(\ell+1)}-1, 2^{\ell+2}(2^{\ell}-1)\right)$-codes is characterized. The BCH bound implies that the minimum distance is greater than four for these codes, but the van Lint–Wilson bound asserts that $\geq 2(\ell+1)$.

1 Introduction

Every nonnegative integer can be uniquely represented in base two, namely in the form

$$v = \nu_0 + \nu_1 2 + \nu_2 2^2 + \nu_3 2^3 + \dots \tag{1}$$

with ν_i from the finite field $GF(2)$. Let $B(v)$ designate the binary representation of v:

$$v \leftrightarrow B(v) = \nu_0\nu_1\nu_2 \cdots \leftrightarrow \langle i_0, i_1, i_2, \dots\rangle, \tag{2}$$

where $\langle i_0, i_1, i_2, \dots\rangle$ is the subset of indices such that $\nu_{i_j} = 1$, $j \geq 0$.

Let W be the infinite set of all nonnegative integers which are the sum of distinct powers of four [1], i. e. $\{0, 1, 4, 5, 16, 17, 20, 21, 64, 65, 68, 69, 80, 81 \dots\}$. The following lemma states that every $w \in W$ can be represented in exactly one way as $w = \sum_{i=0}^{\infty} \omega_{2i} 2^{2i}$, $\omega_i \in GF(2)$.

Lemma 1. *Suppose $w, w' \in W$. Then $w = w'$ if and only if $w_{2i} = w'_{2i}$, $i \geq 0$.*

The proof is based on the observation that $B(w) = \omega_0 0 \omega_2 0 \omega_4 \dots$ and $B(w') = \omega'_0 0 \omega'_2 0 \omega'_4 \dots$ and the uniqueness of the binary representation of a nonnegative integer. One consequence of the lemma is that W with the usual definition of $\leq$ is a totally ordered set.

Definition 1. *For each $\ell \geq 0$, let W_ℓ be the first $2^{\ell+1}$ elements of W; that is*

$$W_\ell = \left\{ w \,|\, w = \sum_{i=0}^{\ell} \omega_{2i} 2^{2i} \right\}. \tag{3}$$

Note that it follows from this definition that for each $w \in W_\ell$ the Hamming weight of $B(w) = \omega_0 0 \omega_2 0 \dots \omega_{2\ell} 000 \dots$ is at most $\ell + 1$. For simplicity of notation, we use $B_\ell(w) = \omega_0\omega_1\omega_2 \dots \omega_{2\ell}\omega_{2\ell+1}$ instead of $B(w)$ for $w < 2^{2(\ell+1)}$.

2 Definition

Let α be a primitive nth root of unity in the extension field $GF\left(2^{2(\ell+1)}\right)$ of $GF(2)$. A cyclic code of length n over $GF(2)$ is generated by a generator polynomial $g(x) \in GF(2)[x]$. The minimum distance of the cyclic code is denoted by d.

We can also describe a cyclic code by the set of zeros of $g(x)$. If R is a subset of $\{0, 1, 2, \dots, n-1\}$ such that $g(\alpha^v) = 0$ for all $v \in R$, then we shall say that R is a defining set for the cyclic code. If R is the maximal defining set for the cyclic code, we shall call it complete and denote by Z. The dimension k of a cyclic code is equal to $n - |Z|$ [2, §7.3].

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

3 Dimension

A binary cyclic code must have $2v$ in R whenever v is in R. Consider the set $2W_\ell$. Any $w \in 2W_\ell$ must be of the form $w = \sum_{i=0}^{\ell} \omega_{2i} 2^{2i+1}$ and it has the following binary representation: $B_\ell(w) = 0\omega_0 0\omega_2 \dots 0\omega_{2\ell}$.

Lemma 2. *Suppose that $s(v) = 2v \pmod n$. Then functions $s : W_\ell \to 2W_\ell$ and $s : 2W_\ell \to W_\ell$ are bijective functions.*

Proof. We first observe that $s(v)$ is a cyclic right-shift function under $B_\ell(v)$ because $B_\ell(s(v)) = \nu_{2\ell+1}\nu_0 \dots \nu_{2\ell}$. Set $w \in W_\ell$, then $B_\ell(w) = \omega_0 0\omega_2 0 \dots \omega_{2\ell} 0$. Hence $B_\ell(s(w)) = 0\omega_0 0\omega_2 \dots 0\omega_{2\ell}$ and $s(w) \in 2W_\ell$. Set $w \in 2W_\ell$, then $B_\ell(w) = 0\omega_0 0\omega_2 \dots 0\omega_{2\ell}$. Hence $B_\ell(s(w)) = \omega_{2\ell} 0\omega_0 0 \dots \omega_{2\ell-2} 0$ and $s(w) \in W_\ell$. Combining these statements with Lemma 1 gives that $s(v)$ is the bijective function with domain W_ℓ and codomain $2W_\ell$, and vice versa. □

By extension, we will use the notation $s^j(v)$ to denote the jth cyclic right-shift function. That is $s^2(v) = s(s(v)) = \nu_{2\ell}\nu_{2\ell+1}\nu_0 \dots \nu_{2\ell-1}$, etc.

Corollary 1. $|W_\ell| = |2W_\ell|$.

Corollary 2. $W_\ell \cap 2W_\ell = \{0\}$*, and consequently* $|W_\ell \cap 2W_\ell| = 1$.

Proof. The proof uses the fact that $B(w) = \omega_0 0\omega_2 0 \dots \omega_{2\ell} 0 = 0\nu_0 0\nu_2 \dots 0\nu_{2\ell} = B(v)$ if and only if $\omega_{2i} = \nu_{2i} = 0$, $0 \leq i \leq \ell$, and so $w = v = 0$, where $w \in W_\ell$ and $v \in 2W_\ell$. □

Corollary 3. $|W_\ell \cup 2W_\ell| = 2|W_\ell| - 1$.

Proof. The proof is immediate because $|W_\ell \cup 2W_\ell| = |W_\ell| + |2W_\ell| - |W_\ell \cap 2W_\ell| = 2|W_\ell| - 1$. □

We will denote by w^* the maximal element in W_ℓ:

$$w^* = \max\{w \mid w \in W_\ell\}. \tag{4}$$

Since $B_\ell(w^*) = 1010\ldots10$, we have $w^* = \sum_{i=0}^{\ell} 2^{2i}$. On the other hand, $B_\ell(2w^*) = 0101\ldots01$, and this gives that $2w^* = \sum_{i=0}^{\ell} 2^{2i+1}$ is the maximal element in $2W_\ell$.

Lemma 3. *If $w \in W_\ell$, then $w \le \frac{1}{3}n$.*

Proof. By definition, $n = 2^{2(\ell+1)} - 1$. Hence we see that

$$3w^* = w^* + 2w^* = \sum_{i=0}^{\ell} 2^{2i} + \sum_{i=0}^{\ell} 2^{2i+1} = \sum_{i=0}^{2\ell+1} 2^i = n. \tag{5}$$

This implies that $w^* = \frac{1}{3}n$, which proves the lemma because $w \le w^*$. $\square$

Corollary 4. *If $w \in 2W_\ell$, then $w \le \frac{2}{3}n$.*

Corollary 5. *The maximal elements in the sets W_ℓ and $2W_\ell$ are $w^* = \frac{1}{3}n$ and $2w^* = \frac{2}{3}n$, respectively.*

Lemma 4. *The code has the complete defining set $Z = W_\ell \cup 2W_\ell$.*

Proof. Z is the union of cyclotomic cosets [2, §7.5]. The cyclotomic coset containing w consists of $w, 2w \pmod n, 2^2w \pmod n, 2^3w \pmod n, \ldots$ for binary codes. In other words, it consists of the integers $w, s(w), s^2(w), s^3(w), \ldots$. From Lemma 2, in the case where $w \in W$ we have $s^j(w) \in W_\ell$ for even values of j and $s^j(w) \in 2W_\ell$ for odd values of j. Similarly, in the case where $w \in 2W_\ell$ we have $s^j(w) \in W_\ell$ for odd values of j and $s^j(w) \in 2W_\ell$ for even values of j. Further, from Lemma 3 and Corollary 4 we conclude that $w \pmod n \equiv w$ for all $w \in (W_\ell \cup 2W_\ell)$. Finally, there is no $w \in W_\ell$ for which $s^j(w) \pmod n \notin (W_\ell \cup 2W_\ell)$, and this is precisely the assertion of the lemma because $R = W_\ell$. $\square$

Now we are ready to estimate the dimension of the code.

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

Proof. Indeed, $k = n - |Z|$. Lemma 4 gives $|Z| = |W_\ell \cup 2W_\ell|$. From Corollary 3 we obtain $|Z| = 2|W_\ell| - 1$. By Definition 1, we know that $|W_\ell| = 2^{\ell+1}$. Summing up, we have

$$k = n - |Z| = (2^{2(\ell+1)} - 1) - (2 \cdot 2^{\ell+1} - 1) = 2^{\ell+1}(2^\ell - 1). \tag{6}$$

$\square$

4 The BCH bound

A cyclic code of length n is a BCH code [3] of designed distance δ_{BCH} if, for some nonnegative integers a and c, where $\gcd(c, n) = 1$, the set

$$S = \{a + ic \pmod{n} \mid 0 \le i \le \delta_{BCH} - 2\} \tag{7}$$

is a subset or equal to Z and $|S| = \delta_{BCH} - 1$. This lower bound δ_{BCH} on the minimum distance is the so-called BCH bound of the cyclic code.

In this section we will examine δ_{BCH}, but before we need some lemmas.

Lemma 5. *Suppose $w \in Z$. Then $3w \pmod{n} \in Z$ if and only if either $w = 0$, or $w = w^*$, or $w = 2w^*$.*

Proof. If $w \in Z$, then $w \in W_\ell$ or $w \in 2W_\ell$. Therefore $B_\ell(w) = \omega_0 0 \omega_2 0 \dots \omega_{2\ell} 0$ and $B_\ell(2w) = 0\omega_0 0\omega_2 \dots 0\omega_{2\ell}$ for $w \in W_\ell$ or $B_\ell(w) = 0\omega_0 0\omega_2 \dots 0\omega_{2\ell}$ and $B_\ell(2w) = \omega_{2\ell} 0\omega_0 0 \dots \omega_{2\ell-2} 0$ for $w \in 2W_\ell$. Since $3w = w + 2w \pmod{n}$, $B_\ell(3w) = \omega_0\omega_0\omega_2\omega_2 \dots \omega_{2\ell}\omega_{2\ell}$ or $B_\ell(3w) = \omega_{2\ell}\omega_0\omega_0\omega_2 \dots \omega_{2\ell-2}\omega_{2\ell}$. Finally $3w \pmod{n} \in Z$ if and only if $3w = 0 \pmod{n}$, in other words, if and only if $\omega_{2i} = 0$ or $\omega_{2i} = 1$ for $0 \le i \le 2\ell$. This gives the assertion of the lemma. □

Corollary 6. *Suppose $w \in Z$ and $3w \ne 0 \pmod{n}$. Then there is one and only one partition $w + 2w = 3w \pmod{n}$ over Z.*

Corollary 7. *Suppose $w \le n$ and $w = 0 \pmod{n}$. Then there are two and only two partitions $0 + 0 = w^* + 2w^* = w \pmod{n}$ over Z.*

These corollaries immediately follow from the binary representation of w, $2w \pmod{n}$ and $3w \pmod{n}$ and the definition of w^*.

Lemma 6. *The BCH bound of the code is $\delta_{BCH} \ge 4$.*

Proof. Let $a = 0$ and $c = 1$. Then $S = \{0, 1, 2\}$ is a subset of Z for $\ell \ge 1$ and we have $\delta_{BCH} \ge 4$ by the BCH bound (7). □

Lemma 7. *The BCH bound of the code is $\delta_{BCH} < 5$.*

Proof. Assume to the contrary that $\delta_{BCH} \ge 5$. It follows from (7) that $S = \{a, a + c \pmod{n}, a + 2c \pmod{n}, a + 3c \pmod{n}\}$ is a subset or equal to Z. We will show that there is no a and c such that $|S| = 4$.

Let $b = a+c \pmod{n}$ and $w = a+3c \pmod{n}$. This means that $w = 3b-2a \pmod{n}$, so that $w + 2a = 3b \pmod{n}$. We only have the cases where $3b \ne 0 \pmod{n}$ and $3b = 0 \pmod{n}$.

Consider first the case $3b \ne 0 \pmod{n}$. Then $w = b$ and $2a = 2b \pmod{n}$ by Corollary 6 implying that (a) $S = \{a, a, a, a\}$. Or $w = 2b \pmod{n}$ and $2a = b \pmod{n}$, hence (b) $S = \{a, 2a \pmod{n}, 3a \pmod{n}, 4a \pmod{n}\}$. Using Lemma 5 we deduce that $a = 0$ and $S = \{0, 0, 0, 0\}$, or $a = w^*$ and $S = \{w^*, 2w^*, 0, w^*\}$, or $a = 2w^*$ and $S = \{2w^*, w^*, 0, 2w^*\}$.

Now suppose that $3b = 0 \pmod{n}$. We apply Lemma 5 and see that this equation has three possible values of b in Z, namely 0, w^* and $2w^*$.

Assume that $b = 0$. Then it follows from Corollary 7 that $w = 0$ and $a = 0$ and S is the same as in case (a), or $w = w^*$ and $2a = 2w^* \pmod{n}$ and $S = \{w^*, 0, 2w^*, w^*\}$, or $w = 2w^*$ and $2a = w^* \pmod{n}$ and $S = \{2w^*, 0, w^*, 2w^*\}$.

In case $b = w^*$ we have that $w = 0$ and $a = 0$ and $S = \{0, w^*, 2w^*, 0\}$, or $w = w^*$ and $2a = 2w^* \pmod{n}$ and this is similar to case (a), or $w = 2w^*$ and $2a = w^* \pmod{n}$ and it gives case (b).

We finally consider the case where $b = 2w^*$. The possible values are $w = 0$ and $a = 0$ and $S = \{0, 2w^*, w^*, 0\}$, or $w = w^*$ and $2a = 2w \pmod{n}$ and S must be as in case (b), or $w = 2w^*$ and $2a = w^* \pmod{n}$ and this is similar to case (a).

Applying Corollary 5, we can now make a list of all possibilities for S: $\{a, a, a, a\}$, $\left\{\frac{1}{3}n, \frac{2}{3}n, 0, \frac{1}{3}n\right\}$, $\left\{\frac{2}{3}n, \frac{1}{3}n, 0, \frac{2}{3}n\right\}$, $\left\{\frac{1}{3}n, 0, \frac{2}{3}n, \frac{1}{3}n\right\}$, $\left\{\frac{2}{3}n, 0, \frac{1}{3}n, \frac{2}{3}n\right\}$, $\left\{0, \frac{1}{3}n, \frac{2}{3}n, 0\right\}$, $\left\{0, \frac{2}{3}n, \frac{1}{3}n, 0\right\}$, where $a \in Z$. Thus in all cases, $a = a + 3c \pmod{n}$. So it follows that $|S| \leq 3$, and this completes the proof. □

Theorem 2. *The BCH bound of the code is* $\delta_{BCH} = 4$.

Proof. Lemma 6 and Lemma 7 immediately yield the theorem. □

5 The van Lint–Wilson bound

We first inductively define the notation of an independent set with respect to S, as follows [4, §5]: (1) the empty set is independent with respect to S, (2) 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, and (3) if A is independent with respect to S and $0 < c < n$, then $\{c + a \,|\, a \in A\}$ is independent with respect to S. The maximal size of a set which is independent with respect to Z is called the van Lint–Wilson bound δ_{LW} of a cyclic code.

We will examine δ_{LW} of the code, and this is aided by the following lemma.

Lemma 8. *Suppose a is odd and c is even. Then* $2^a + 2^c \notin Z$.

Proof. If $w \in Z$, then $w \in W_\ell$ or $w \in 2W_\ell$. Consequently, we can write $B_\ell(w) \leftrightarrow \langle i_0, i_1, i_2, \ldots \rangle$ where i_j are even if $w \in W_\ell$ or odd if $w \in 2W_\ell$. But $B_\ell(2^a + 2^c) \leftrightarrow \langle a, c \rangle$ with odd a and even c. Therefore $2^a + 2^c \notin Z$. □

Theorem 3. *The van Lint–Wilson bound of the code is* $\delta_{LW} \geq 2(\ell + 1)$.

Proof. Since the van Lint–Wilson bound is a generalization of the BCH bound [4, §5] and $\delta_{BCH} = 4$ by Theorem 2, we only need to show that $\delta_{LW} \geq 2(\ell + 1)$ for $\ell \geq 2$. We construct the sequence $A_0 = \emptyset, A_1, A_2, \ldots, A_{2\ell+2}$ of subsets of $GF\left(2^{2(\ell+1)}\right)$ that are independent with respect to Z. In order to simplify the notation, we will use the index representation $\langle \ldots \rangle$ of an integer.

Let $a_0 = 0$, $a_1 = n - 2^0$, $a_2 = 2^{2(\ell-1)} - 2^0$, $a_3 = 2^{2(\ell-2)} - 2^{2(\ell-1)}$, $\ldots$, $a_\ell = 2^2 - 2^4$, $a_{\ell+1} = n - 2^2$, $a_{\ell+2} = 2^{2(\ell-1)} - 2^0$, $a_{\ell+3} = 2^{2(\ell-2)} - 2^{2(\ell-1)}$, $\ldots$, $a_{2\ell} = 2^2 - 2^4$, $a_{2\ell+1} = n - 2^2$ and $b_0 = 2^1 + 2^0$, $b_1 = 2^{2\ell} + 2^1$, $b_2 = 2^{2\ell-1} + 2^0$, $b_3 = 2^{2\ell-3} + 2^0$, $\ldots$, $b_\ell = 2^2 + 2^1$, $b_{\ell+1} = 2^{2\ell} + 2^1$, $b_{\ell+2} = 2^{2\ell-1} + 2^0$, $b_{\ell+3} = 2^{2\ell-3} + 2^0$, $\ldots$, $b_{2\ell} = 2^2 + 2^1$, $b_{2\ell+1} = 2^1 + 2^0$. (Remark: $b_j \notin Z$ for all $0 \leq j \leq 2\ell + 1$ by Lemma 8.) Then

$$
\begin{aligned}
A_1 &= \{\langle 0, 1\rangle\},\\
A_2 &= \{\langle 1\rangle, \langle 1, 2\ell\rangle\},\\
A_3 &= \{\langle 0, 2(\ell-1)\rangle, \langle 0, 2(\ell-1), 2\ell\rangle, \langle 0, 2\ell-1\rangle\},\\
A_4 &= \{\langle 0, 2(\ell-2)\rangle, \langle 0, 2(\ell-2), 2\ell\rangle, \langle 0, 2(\ell-2)\rangle, \langle 0, 2\ell-3\rangle\},\\
&\ldots\\
A_{\ell+1} &= \{\langle 0, 2\rangle, \langle 0, 2, 2\ell\rangle, \langle 0, 2, 2(\ell-1)\rangle, \ldots, \langle 0, 2, 4\rangle, \langle 1, 2\rangle\},\\
A_{\ell+2} &= \{\langle 0\rangle, \langle 0, 2\ell\rangle, \langle 0, 2(\ell-1)\rangle, \ldots, \langle 0, 4\rangle, \langle 1\rangle, \langle 1, 2\ell\rangle\},\\
A_{\ell+3} &= \{\langle 2(\ell-1)\rangle, \langle 2(\ell-1), 2\ell\rangle, \langle 2\ell-1\rangle, \ldots, \langle 4, 2(\ell-1)\rangle, \langle 0, 2(\ell-1)\rangle,\\
&\qquad \langle 0, 2(\ell-1), 2\ell\rangle, \langle 0, 2\ell-1\rangle\},\\
A_{\ell+4} &= \{\langle 2(\ell-2)\rangle, \langle 2(\ell-2), 2\ell\rangle, \langle 2(\ell-2), 2(\ell-1)\rangle, \ldots, \langle 4, 2(\ell-2)\rangle,\\
&\qquad \langle 0, 2(\ell-2)\rangle, \langle 0, 2(\ell-2), 2\ell\rangle, \langle 0, 2(\ell-2)\rangle, \langle 0, 2\ell-3\rangle\},\\
&\ldots\\
A_{2\ell+1} &= \{\langle 2\rangle, \langle 2, 2\ell\rangle, \langle 2, 2(\ell-1)\rangle, \ldots, \langle 2, 4\rangle, \langle 0, 2\rangle, \langle 0, 2, 2\ell\rangle, \langle 0, 2, 2(\ell-1)\rangle,\\
&\qquad \ldots, \langle 0, 2, 4\rangle, \langle 1, 2\rangle\},\\
A_{2\ell+2} &= \{0, \langle 2\ell\rangle, \langle 2(\ell-1)\rangle, \ldots, \langle 4\rangle, \langle 0\rangle, \langle 0, 2\ell\rangle, \langle 0, 2(\ell-1)\rangle, \ldots, \langle 0, 4\rangle,\\
&\qquad \langle 1\rangle, \langle 0, 1\rangle\}.
\end{aligned}
$$

It easy to see that $A_j \setminus \{b_{j-1}\} \subseteq Z$ for all $1 \leq j \leq 2\ell+2$ because the elements of these sets are the sums of even powers of two, i. e. in W_ℓ, or a power of two (see $\langle 1\rangle$ in $A_{\ell+2}$ and $A_{2\ell+2}$). Since the independent set $A_{2\ell+2}$ has the cardinality $2(\ell+1)$, we have $\delta_{LW} \geq 2(\ell+1)$. □

Corollary 8. *The minimum distance of the code is* $d \geq 2(l+1)$.

References

[1] N. G. de Bruijn, Some Direct Decompositions of the Set of Integers, *Math. Comput.,* **18**, 537–546, 1964.

[2] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes,* North-Holland, Amsterdam, 1977.

[3] R. C. Bose and D. K. Ray-Chaudhuri, On a Class of Error Correcting Binary Group Codes, *Inform. Contr.,* **3**, 68–79, 1960.

[4] J. H. van Lint and R. M. Wilson, On the Minimum Distance of Cyclic Codes, *IEEE Trans. on Inform. Theory*, **32**, 23–40, 1986.