MINIMUM DISTANCE OF BCH CODES OF LENGTH $2^m + 1$

Alberto Cáceres
Department of Mathematics, Humacao University College, Humacao Puerto Rico

CONGRESUS NUMERANTUM
VOLUME 78, December 1990

ABSTRACT. The main result of this investigation is the estimation of the minimum distance of BCH codes of length $n = 2^m + 1$. We prove that for some designed distances, the generating set $A = \{\beta^i\}$ of those codes, where $\beta$ is a primitive $n$-th root of unity and the $\beta^i$s are roots of the generating polynomial $g(x) = m_1(X)m_2(X) \ldots m_{2k-1}(X)$ contains three consecutive subsets of roots. This fact permits the use of Hartman-Tzeng (HT) bound to obtain substantial improvement over results obtained by the use of the BCH bound.

INTRODUCTION. A cyclic code $C$ of length $n$ over $\mathbb{F}_q$ is defined as an ideal in the quotient ring $\mathbb{F}_q[X]/(X^n - 1)$. This ideal is generated by a polynomial $g(X)$ which is a divisor of $X^n - 1$. If $\beta$ is a primitive $n$-th root of unity in an extension field $\mathbb{F}_{q^m}$ of $\mathbb{F}_q$ then some powers $\beta^i$ of $\beta$ are roots of $g(X)$. Let $m_i(X)$ be the minimal polynomial of $\beta^i$ over $\mathbb{F}_q$ and $g(X)$ be the product of polynomials $m_i(X)$. For any integer $k > 0$, $\beta^{p^k}$ is also a root of $m_i(X)$. The sets $C_i = \{ip^k \pmod{n}\}$ are called cyclotomic cosets modulo $n$. $\lambda \in C_i \iff \beta^\lambda$ is a root of $m_i(X)$. A set of $n$-th roots of unity $A = \{\beta^1, \beta^2, \ldots, \beta^n\}$ defines a cyclic code $C$ by setting $c \in C \iff c(\xi) = 0, \forall \xi \in A$.

By the Van Lint-Wilson notation [2], we call $A$ the defining set of $C, M = \{\beta^1, \beta^{i+1}, \ldots, \beta^{i+\lambda-1}\}$ a consecutive set of length $\lambda$ and $d_A$ the minimum distance of the code. A BCH code of designed distance $\delta$ has a consecutive set $M = \{\beta^1, \beta^2, \ldots, \beta^{1+\delta-2}\}$ as defining set. We invoke the following well known results as they appear in [1] and [2].

**Proposition 1.** (BCH bound) If a defining set $A$ of a cyclic code contains a consecutive set of length $\delta - 1$, then $\delta_A \geq \delta$.

**Proposition 2.** (HT bound) If $A = \{\alpha^{1}, \alpha^{i}, \ldots, \alpha^{i}\}$ is a defining set for a cyclic code and if $\beta$ is a primitive $n$-th root of unity such that $A$ contains the consecutive sets $\{\beta^{1+j}, \beta^{1+j+ja}, \ldots, \beta^{1+\delta-2+ja}\}$, $0 \leq j \leq s$ and if $gcd(a, n) < \delta$, then $d_A \geq \delta + s$.

**Lemma 1.** For $n = 2^m + 1$, $m > 3$, the union of cyclotomic cosets modulo $n$, $C_1 \cup C_3$ contains $s + 1 = 3$ consecutive subsets of length $\delta - 1 = 4$.

**Proof:** $C_1 = \{1, 2, 4, \ldots, 2^{2m-1}\}, C_3 = \{3, 6, 12, \ldots, 3(2^m-1)\}$, modulo $n = 2^m + 1$. $C_1 \cup C_3$ contains

---

1 This work was partially done under the auspices of the Gauss Computational Mathematics Laboratory at University of Puerto Rico-Rio Piedras, during Summer 1989.


a first consecutive subset \(\{1, 2, 3, 4\}\) of length 4. Since a code of length \(2^m + 1\) is reversible (see [2], page 268) \(C_1 \cup C_3\) contains also the subset \(\{2^m - 3, 2^m - 2, 2^m - 1, 2^m\}\). For any \(k, 0 \leq k \leq m, 2^k \in C_1\), hence \(2^{m-1} \in C_1\). By reversibility \(2^{m-1} + 1 \in C_1\). Since \(2^{m-1} - (2^m + 1) = 2^{m-1} - 1, 3 \cdot 2^{m-1} = 2^{m-1} - 1 \pmod{(2^m + 1)}\), i.e., \(2^{m-1} - 1 \in C_3\). By reversibility \(2^{m-1} + 2 \in C_3\). Therefore \(\{2^{m-1} - 1, 2^{m-1}, 2^{m-1} + 1, 2^{m-1} + 2\}\) is the third “middle” consecutive subset of \(C_1 \cup C_3\).

To satisfy the condition \(\gcd(a, n) < \delta\) of the HT bound we must exclude some cases.

**Lemma 2.** For \(m > 3\) and \(5|(2^{m-1} - 2)\) then \(\gcd(2^m + 1, 2^{m-1} - 2) = 1\)

**Proof:** \(2^m + 1 = 2(2^{m-1} - 2 + 5)\) and for \(m > 3\), \(5 < 2^{m-1} - 2\). Then the hypothesis \(5|(2^{m-1} - 2)\) implies \(\gcd(2^m + 1, 2^{m-1} - 2) = \gcd(2^m + 1, 5) = 1\)

**Theorem 1.** Let \(n = 2^m + 1, m > 3\) and \(5|(2^{m-1} - 2)\). The BCH code \(C\) of length \(2^m + 1\) and designed distance \(\delta = 5\) has minimum distance \(d \geq 7\).

**Proof:** Given the designed distance \(\delta = 5\) we can write the defining set \(A = \{\beta^k : k \in C_1 \cup C_3\}\), which as in Lemma 1 contains the following consecutive subsets of roots:
\[
\{\beta^{1+j(2^{m-1}-2)}, \beta^{2+j(2^{m-1}-2)}, \beta^{3+j(2^{m-1}-2)}, \beta^{4+j(2^{m-1}-2)}\}
\]
for \(j = 0, 1, 2\). Here \(a = 2^{m-1} - 2\) and \(\delta - 1 = 4\), since \(5|(2^{m-1} - 2)\), we have \(\gcd(2^m + 1, 2^{m-1} - 2) = 1 \pmod{4}\). Now by HT Bound and BCH distance we obtain \(d \geq d_{BCH} + s \geq 7\).

**Theorem 2.** A BCH code of length \(n = 2^m + 1\), where \(m \equiv 0, 1, 3 \pmod{4}\) and designed distance \(\delta = 5\) has minimum distance \(d \geq 7\).

**Proof:** \(5|(2^{m-1} - 2)\) if and only if \(m - 2 \equiv 0 \pmod{4}\), if and only if \(m \equiv 2 \pmod{4}\)

We generalize these resultsto BCH codes of larger designed distances. Indeed, as we take more roots and enlarge the defining set , the three consecutive subsets also grow by 2.

**Lemma 3.** Let \(n = 2^m + 1, m > 3\) and \(2k - 1 < 2^{(m/2)} + 1\). The union of cyclotomic cosets \(M = C_1 \cup C_3 \cup \ldots \cup C_{2k-1}\) contains 3 consecutive subsets of length \(2k\).

**Proof:** We know by [3] that under the hypothesis on \(k\) the cyclotomic cosets \(C_1, C_3, \ldots, C_{2k-1}\) are all different, hence disjoint. Reflecting on the Lemma 1, \(M\) contains the consecutive subset \(\{1, 2, \ldots, 2k\}\) and by reversibility the subset \(\{2^m + 1 - i : i = 1, 2, \ldots, 2k\}\), both of length \(2k\). We will prove that the “middle” subset
\[
\{2^m - (k - 1), 2^m - (k - 2), \ldots, 2^{m-1}, 2^{m-1} + 1, \ldots, 2^{m-1} + k\}
\]
is also contained in \(M\). It is clear that \(2^{m-1} \in C_1\). We will prove that for \(1 \leq i \leq k, 2^{m-1} + i \in C_{2i-1}\), i.e., the elements to the right of \(2^{m-1}\) are in \(M\). Indeed
\[
(2i - 1)2^{m-1} - (2^{m-1} + i) = [2^{m-1}(2i - 1) - i](2^m + 1)
\]
which means that \(2^{m-1} + i \equiv (2i - 1) \pmod{(2^m + 1)}\). Now to the left, for every \(2^{m-1} + i \in C_{2i-1}\), since both add up to \(2^m + 1\)
Lemma 4. Let \( m > 3, 2k + 1 < 2^{m-1} - k \) and \((2k + 1)|((2^{m-1} - k). Then \( \gcd(2^m + 1, 2^{m-1} - k) < 2k - 1. \)

Proof: By the division algorithm \( 2^m + 1 = 2(2^{m-1} - k) + (2k + 1) \). Both hypothesis on \( k \) imply the result.

Theorem 3. Let \( m > 3, n = 2^m + 1, (2k + 1)|(2^{m-1} - k) \) and designed distance \( 2k - 1 \), has distance \( d \geq 2k + 3 \).

Proof: The defining set of \( C \) is \( A = \{ \beta^k : k \in C_1 \cup C_3 \cup \ldots \cup C_{2k-1} \} \) which by Lemma 3 contains the following \( s + 1 = 3 \) consecutive sets of length \( \delta - 1 = 2k \),

\[
\{\beta^{i+j}(2^{m-1} - k) : i = 1, 2, \ldots, 2k; j = 0, 1, 2\}
\]

By Lemma 4, \( \gcd(2^m + 1, 2^{m-1} - k) < \delta \), and invoking HT bound for \( a = 2^{m-1} - k \), we obtain \( d \geq d_{BCCH} + s \geq 2k + 1 + 2 = 2k + 3 \).

There are two extremal cases on which we can improve the distance even further, since the union of cyclotomic cosets contains consecutive subsets of greater length. For \( m \) even, the improvement is by 2; for \( m \) odd it is by 4.

Lemma 5. Let \( n = 2^m + 1, m \geq 3, m \) even and \( 2k - 1 = 2^{m/2} - 1 \). The union \( M = C_1 \cup C_3 \cup \ldots \cup C_{2k-1} \) contains 3 consecutive sets of length \( \delta - 1 = 2k + 2 \).

Proof: By Theorem 3 we know that \( 1, 2, \ldots, 2k \in M \). Also \( 2k + 2 \in C_{k+1} \subseteq M \). The identity

\[
(2^{m/2} - 1)2^{3m/2} - (2^{m/2} + 1) = (2^m + 1)(2^m - 2^{m/2} - 1)
\]

proves that \( 2k + 1 = 2^{m/2} + 1 \in C_{2k-1} \). Again by reversibility, the set of negatives modulo \( 2^m + 1 \) is also part of \( M \). Now we prove that the “middle” set increases by the element \( 2^{m-1} + k + 1 = 2^{m-1} + 2^{m/2} - 1 \) to the right and \( 2^{m-1} - k \) to the left. Indeed both elements belong to \( C_{2k-1} \) as the following identity shows for the first one

\[
(2^{m/2} - 1)2^{3m/2} - (2^{m-1} + 2^{m/2} - 1 + 1) = (2^m + 1)(2^{m-1} - 2^{m/2} - 1).
\]

Reversibility is used for the second one.

Theorem 4. Let \( n = 2^m + 1, m > 3, (2^{m/2} + 3)|(2^{m-1} - 2^{m/2} - 1) \) and \( 2k - 1 = 2^{m/2} - 1 \). The BCH code of length \( n \) and designed distance \( 2k - 1 \), has distance \( d \geq 2k + 5 \).

Proof: In order to fulfill the HT-Bound conditions we observe from the division algorithm that \( 2^m + 1 = 2(2^{m-1} - 2^{[m/2]} - 1) + (2^{m/2} + 3) \) and by divisibility hypothesis \( \gcd(n, 2^{m-1} - 2^{[m/2]} - 1) < 2^{m/2} + 3 \). The previous Lemma exhibits \( s + 1 = 3 \) consecutive subsets of length \( \delta - 1 = 2k + 2 \). Then, again by HT-Bound \( d \geq d_{BCCH} + s \geq 2k + 3 + 2 = 2k + 5 \).

The second case considers \( m \) odd.

Lemma 6. Let \( n = 2^m + 1, m > 3, m \) odd \( 2k - 1 = 2^{m/2} - 3 \). The union \( M = C_1 \cup C_3 \cup \ldots \cup C_{2k-1} \) contains 3 consecutive sets of length \( \delta - 1 = 2k + 4 \).
Proof: Similar to Lemma 5, 1, 2, . . . , 2k ∈ M. Also 2k + 2 ∈ C_{k+1} ⊆ M and 2k + 4 ∈ C_{k+2} ⊆ M. The identities below show that 2k + 1 = 2^{(m+1)/2} - 1 ∈ C_k where k + 2 = 2^{(m-1)/2} + 1 and 2k + 3 = 2^{(m+1)/2} + 1 ∈ C_k, where k = 2^{(m-1)/2} - 1.

\[(2^{(m-1)/2} + 1)2^{(m+1)/2} - (2^{(m+1)/2} - 1) = 2^m + 1\]

\[(2^m - 1)2^{(3m+1)/2} - (2^{(m+1)/2} + 1) = (2^m + 1)[(2^{2m} + 1)(2^m + 1) - 2^{(m+1)/2}]\]

and hence the set is four elements longer. As before, inversibility produces the second set. The middle set of Lemma 3 is augmented also by 4 elements, 2^m + k + 1 and 2^m - k in C_j ⊆ M where j = 2^{(m+1)/2} + 1 and also 2^m - (k + 1) and 2^m + (k + 2), in C_j ⊆ M, where j = 2^{(m-1)/2} + 1. The following identities prove the first facts for each cyclotomic coset.

\[(2^{(m-1)/2} + 1) : 2^{(m-1)/2} = 2^{m-1} + 2^{(m-1)/2}\]
\[(2^{(m-1)/2} - 1) : 2^{(m-1)/2} = 2^{m-1} - 2^{(m-1)/2}\]

The other facts are given by reversibility.

Theorem 5. Let \( n = 2^m + 1, m > 3, \text{odd} \) and 2k - 1 = 2^{[m/2]} - 3. The BCH code of length \( n \) and designed distance 2k - 1, has distance \( d \geq 2^k + 7 \).

Proof: According to Lemma 6. the generating set containing \( s + 1 = 3 \) sets of roots of length \( \delta - 1 = 2k + 4 \). In order to satisfy the gcd condition observe that

\[2^m + 1 = 2 \cdot (2^{m-1} - 2^{m/2-1} - 1) + 2^{(m+1)/2} + 2.\]

Clearly \( 2^{(m+1)/2} + 2 \) does not divide \( 2^{m-1} - 2^{m/2-1} - 1 \), hence \( gcd < 2^{(m+1)/2} + 2.\)

As in Theorem 4, \( d \geq d_{BGH} + s \geq 2k + 5 + 2 = 2k + 7 \).

REFERENCES


[3] Cáceres A. and Moreno O., Number of Information Symbols of BCH codes of Length \( 2^m + 1 \), Proceedings of the Twenty Second Annual Allerton Conference on Communication, Control and Computing, University of Illinois at Urbana-Champaign, Illinois, 1984