The Stopping Distance of Binary BCH-code Parity-check Matrices

M. Esmaeili** and Z. Hooshmand*
*Department of Mathematical Sciences
Isfahan University of Technology, 84156-83111, Isfahan, Iran
*Dept. of Electrical and Computer Engineering
University of Victoria, Victoria, B.C., Canada V8W 3P6
emorteza@{cc.iut.ac.ir, ece.uvic.ca}, zohreh_jazi@yahoo.com

Abstract

Given a parity-check matrix H with n columns, an ℓ-subset T of $\{1, 2, \cdots, n\}$ is called a stopping set of size ℓ for H if the ℓ-column submatrix of H consisting of columns with coordinate indexes in T has no row of Hamming weight one. The size of the smallest non-empty stopping sets for H is called the *stopping distance* of H.

In this paper, the stopping distance of $H_m(2t+1)$, parity-check matrices representing binary t-error-correcting BCH codes, is addressed. It is shown that if m is even then the stopping distance of this matrix is three. We conjecture that this property holds for all integers $m \geq 3$.

Keywords: Stopping set, stopping distance, BCH codes.

1 Introduction and Background

1.1 Introduction

Let C be a linear block code of length n represented by a parity-check matrix H. For decoding C on the binary erasure channel by iterative decoding algorithms, the algorithms are performed on the Tanner graph [1] representing H. The performance of C is determined by a type of combinatorial structure on the parity-check matrix H referred to as *stopping sets* [2].

[1]This research was in part supported by a grant from Iran Telecommunication Research Center (ITRC).

An ℓ-subset $T \subset \{1, 2, \cdots, n\}$ is called a stopping set of size ℓ for H if the ℓ-column submatrix of H consisting of columns with coordinate indexes in T has no row of Hamming weight one. The size of the smallest non-empty stopping sets for H is called the *stopping distance* of H, denoted by $s(H)$ [3]-[9]. The role of $s(H)$ on the performance of C under iterative decoding on the binary erasure channel is very similar to that of minimum distance of C under maximum likelihood decoding.

The stopping distance of full-rank parity-check matrices of the Hamming codes is studied in [10]. The class of binary Hamming codes is in fact the class of single-error-correcting BCH codes. In this paper we consider binary t-error-correcting BCH codes of length $n = 2^m - 1$. It is shown that the stopping distance of the associated parity-check matrices, denoted $H_m(2t+1)$, is 3 when m is even. We conjecture that this property also holds for the cases wherein m is odd.

Necessary background materials are given in the following subsection. In Section 2, we show that the parity-check matrices $H_m(5)$, $3 \leq m \leq 8$, that is matrices representing two-error-correcting BCH codes of lengths 7, 15, 31, 63, 127, and 255, have stopping distance 3. Based on this, we believe that for any integer $m \geq 3$ the stopping distance of $H_m(2t+1)$ is three. It is shown in Section 3 that this property holds for $H_{2r}(2t+1)$, the parity-check matrix representing binary t-error-correcting BCH code of length $2^{2r} - 1$.

1.2 Background

Cyclic codes For a prime power q, suppose n and q are relatively prime, denoted $(n, q) = 1$, and let α_1, α_2, $\cdots$, α_t be a set of nth roots of unity over F_q, and let C be the largest q-ary length-n cyclic code having α_i, $1 \leq i \leq t$, among its zeros. Then C is the set of all polynomial-codewords $f(x) = f_0 + f_1 x + \cdots + f_{n-1}x^{n-1}$, $f_i \in F_q$, satisfying

$$f(\alpha_i) = f_0\alpha_i^0 + f_1\alpha_i + f_2\alpha_i^2 + \cdots + f_{n-1}\alpha_i^{n-1} = 0, \quad 1 \leq i \leq t.$$

If the splitting field of $x^n - 1$ over F_q is F_{q^d}, then any element β of F_{q^d}, in particular any nth root of unity, is expressed as a d-tuple $[\beta]$ over F_q. Therefore,

$$f(x) \in C \text{ if and only if } f_0\,[\alpha_i^0] + f_1\,[\alpha_i^1] + \cdots + f_{n-1}\,[\alpha_i^{n-1}] = 0, \quad 1 \leq i \leq t.$$

This implies that the following matrix H over F_q, with possibly linearly dependent rows, is a parity-check matrix for C.

$$\mathrm{H} = \begin{pmatrix} [\alpha_1^0] & [\alpha_1^1] & \cdots & [\alpha_1^{n-1}] \\ [\alpha_2^0] & [\alpha_2^1] & \cdots & [\alpha_2^{n-1}] \\ \vdots & \vdots & \cdots & \vdots \\ [\alpha_t^0] & [\alpha_t^1] & \cdots & [\alpha_t^{n-1}] \end{pmatrix} \tag{1}$$

Definition 1 The ith cyclotomic coset of q modulo n is the set $C_i(q) := \{i, iq, iq^2, \cdots, iq^{d-1}\}$ where d is the smallest positive integer such that $iq^d = i \pmod{n}$.

It follows from definition that $u \in C_i(2)$ if and only if $2u \in C_i(2)$. This implies the following corollary.

Corollary 1 Let α be a primitive nth roots of unity over F_2 with $(n, 2) = 1$, that is α generates the cyclic group $E^{(n)}$ consisting of the nth roots of unity over F_2. Suppose $m_i(x)$ is the minimal polynomial of α^i. Then polynomials $g_1(x) = \mathrm{lcm}\{m_1(x), m_2(x), \cdots, m_{2t}(x)\}$, $g_2(x) = \mathrm{lcm}\{m_1(x), m_2(x), \cdots, m_{2t-1}(x)\}$ and $g_3(x) = \mathrm{lcm}\{m_1(x), m_3(x), \cdots, m_{2t-1}(x)\}$ generate the same length-n binary cyclic code.

BCH codes Let α be a primitive nth root of unity over F_q. Suppose $g(x)$ is the monic polynomial over F_q of minimum degree having α^{b+i}, $0 \le i \le \delta - 2$, among its zeros, that is

$$g(x) = \mathrm{lcm}\{m_b(x), m_{b+1}(x), \cdots, m_{b+\delta-2}(x)\}$$

where $m_i(x)$ is the monic minimal polynomial of α^i. The q-ary cyclic code of length n with the generator polynomial $g(x)$ is called a BCH code and dented by $B_q(n, \delta, \alpha, b)$. If $b = 1$ then this code is denoted by $B_q(n, \delta, \alpha)$ and referred to as a narrow-sense BCH code. Also, if α is a primitive field element, that is it generates the multiplicative group $F_{q^d}^* = F_{q^d} - \{0\}$ of the splitting field F_{q^d} of $x^n - 1$, then this code is called a primitive BCH code. If $b = 1$ then the binary BCH code $B_2(n, 2 = \delta, \alpha)$ is in fact the binary Hamming code.

It is known that the BCH code $B_q(n, \delta, \alpha, b)$ has minimum distance at least $d \ge \delta$ and that the binary Hamming code $B_2(n, 2 = \delta, \alpha)$ has minimum distance $d = 3$. The integer δ is called the *design distance* of $B_q(n, \delta, \alpha, b)$.

According to Corollary 1, to construct a binary BCH code we just need to consider odd design distances and in designing a code with design distance $2t + 1$ we employ $g_3(x) = \mathrm{lcm}\{m_1(x), m_3(x), \cdots, m_{2t-1}(x)\}$. In this paper we are concerned with binary narrow-sense primitive BCH codes.

Let α be a primitive nth root of unity with $n = 2^m - 1$. Hence the splitting field of $x^n - 1$ is F_{2^m} and any primitive field element is a primitive nth root of unity. We consider BCH code $B_2(n, 2t+1, \alpha)$, denoted by $C_m(2t+1)$, of length $n = 2^m - 1$ defined by zeros α, α^3, $\cdots$ and α^{2t-1}. Thus, according to (1), $C_m(2t+1)$ has parity-check matrix $H_m(2t+1)$ given below wherein the powers of α are computed modulo $n-1$.

$$H_m(2t+1) := \begin{pmatrix} [\alpha^0] & [\alpha^1] & \cdots & [\alpha^{2^m-2}] \\ [(\alpha^3)^0] & [(\alpha^3)^1] & \cdots & [(\alpha^3)^{2^m-2}] \\ \vdots & \vdots & \cdots & \vdots \\ [(\alpha^{2t-1})^0] & [(\alpha^{2t-1})^1] & \cdots & [(\alpha^{2t-1})^{2^m-2}] \end{pmatrix} \quad (2)$$

We note that the first block-row of $H_m(2t+1)$, consisting of the m binary rows specified by α, is a parity-check matrix of the binary Hamming code of length $n = 2^m - 1$.

2 Stopping distance of BCH-code parity-check matrices of lengths 7, 15, 31, 63, 127, 255

In this section, we show that the stopping distance of parity-check matrices $H_m(5)$, $3 \le m \le 8$, is three. The examples are illustrative and provide some useful ideas for proving this property for arbitrary values of m.

Theorem 1 ([11]) Let C be a linear binary code represented by a parity-check matrix H and that C has minimum distance $d \le 3$. Then $d = s(H)$.

Proof. If H has an all-zero column then $d = s(H) = 1$. Otherwise, any column of H has a nonzero entry and hence $s(H) > 1$. Thus if $d = 2$, then it follows from $s(H) \le d$ that $s(H) \le 2$, and hence $d = s(H) = 2$. If $d = 3$ then any two columns of H are linearly independent, and hence any matrix consisting of two columns of H has at least one row in the form 01 or 10, implying that $s(H) \ge 3$. This together with $s(H) \le d = 3$ gives $s(H) = d$.■

Corollary 2 Any parity-check matrix H of the $[2^m-1, 2^m-m-1, 3]$ binary Hamming code satisfies $s(H) = 3$; in particular, this holds for $H_m(3)$, the matrix consisting of the first m rows of $H_m(2t+1)$ given by (2).

Lemma 1 For the parity-check matrix $H_m(2t+1)$, given by (2), we have $s(H_m(2t+1)) \ge 3$.

Proof. As mentioned above, in $H_m(2t+1) = \begin{pmatrix} H_m(3) \\ H'' \end{pmatrix}$, given by (2), the matrix $H_m(3)$ consisting of the first m binary rows of $H_m(2t+1)$ satisfies

$s(H_m(3)) = 3$. It is obvious that if a matrix M consisting of some columns of $H_m(2t+1)$, has no rows of Hamming weight one, then the first m rows of M also satisfy this property, and hence any stopping set for $H_m(2t+1)$ is also an stopping set for $H_m(3)$. Thus $s(H_m(2t+1)) \geq 3$. ∎

Example 1 Set $m = 3$. The splitting field of $x^7 - 1$ is F_8 and any root α of the primitive polynomial $1 + x + x^3$ is a primitive field element for F_8 and a primitive 7th root of unity. F_8 is a 3-dimensional vector space over F_2 with basis $\{1, \alpha, \alpha^2\}$. Using $1 + \alpha + \alpha^2 = 0$, we obtain the binary representation of the 7th roots of unity: $1 = \alpha^0 = 001$, $\alpha^1 = 010$, $\alpha^2 = 100$, $\alpha^3 = 011$, $\alpha^4 = 110$, $\alpha^5 = 111$, $\alpha^6 = 101$. Thus we have the following parity-check matrix H_3.

$$H_3(5) = \begin{pmatrix} \alpha^0 & \alpha^1 & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ \alpha^0 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha^5 & \alpha^1 & \alpha^4 \end{pmatrix} = \left(\begin{array}{ccccccc} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ \hline 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \end{array}\right)$$

The matrix consisting of the first three rows of the binary matrix is a parity-check matrix for the length-7 Hamming code. The parity-check matrix of the length-7 Hamming code in its recursive form, expressed in terms of parity-check matrix of the length-3 Hamming code, is obtained by applying a column permutation on this matrix. In fact, we have

$$H_3(5) = \left(\begin{array}{ccccccc} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ \hline 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \end{array}\right) = \begin{pmatrix} \alpha^0 & \alpha^1 & \alpha^3 & \alpha^2 & \alpha^6 & \alpha^4 & \alpha^5 \\ \alpha^0 & \alpha^3 & \alpha^2 & \alpha^6 & \alpha^4 & \alpha^5 & \alpha^1 \end{pmatrix}$$

Columns 2, 4 and 6 of this binary matrix represent a stopping set and hence $s(H_3(5)) \leq 3$. This together with Lemma 1 gives $s(H_3(5)) = 3$. Note that in this example α^3 is also a primitive field element.

Example 2 The splitting field of $x^{15} - 1$ is F_{16} and any root α of $1 + x + x^4$ is a primitive 15th root of unity. By a process similar to the given in Example 1 we get the following parity-check matrix $H_4(5)$.

$$H_4(5) = \begin{pmatrix} \alpha^0 & \alpha^1 & \alpha^4 & \alpha^2 & \alpha^8 & \alpha^5 & \alpha^{10} & \alpha^3 & \alpha^{14} & \alpha^9 & \alpha^7 & \alpha^6 & \alpha^{13} & \alpha^{11} & \alpha^{12} \\ \alpha^0 & \alpha^3 & \alpha^{12} & \alpha^6 & \alpha^9 & \alpha^0 & \alpha^0 & \alpha^9 & \alpha^{12} & \alpha^{12} & \alpha^6 & \alpha^3 & \alpha^9 & \alpha^3 & \alpha^6 \end{pmatrix}$$

$$= \left(\begin{array}{ccccccccccccccc} 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ \hline 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

In this case α^3 is not primitive and generates α^3, α^6, α^9, α^{12} and $\alpha^{15} = \alpha^0 = 1$. Columns 2, 12, and 14 give an stopping set and hence $s(H_4(5)) = 3$.

Example 3 For $m = 5$, the splitting field of $x^{31} - 1$ is F_{32} with primitive field element α which is a root of $1 + x^2 + x^5$. The matrix $H_5(5)$ given below is the corresponding parity-check matrix for the length-31 two-error-correcting binary BCH code.

$$H_5(5) = \left(\begin{array}{c} 00000000000000011111111111111111 \\ 00000001111111100000000011111111 \\ 00011110000111100000111100001111 \\ 01100110011001100110011001100110011 \\ 10101010101010101010101010101010101 \\ \hline 00001101100010101101111010100 11 \\ 01111001100110010011001011010 01 \\ 00101110001011110110010010011 01 \\ 00111101011010011100001101101 00 \\ 10101100110101000000110011111 1 \end{array}\right)$$

Columns 5, 12 and 13, associated with the top elements α^5, α^{20} and α^8, respectively, introduce an stopping set, and hence $s(H_5) = 3$. For this case α^3 is a primitive field element.

Following the same process, one can find 3-element stopping sets for the cases $m = 6, 7, 8$. These support the conjecture that the stopping distance of $H_m(2t + 1)$ is three.

3 Stopping distance of BCH-code parity-check matrix $H_{2^r}(2t + 1)$

In this section, it is shown that the stopping distance of BCH-code parity-check matrix $H_{2^r}(2t + 1)$ is three for any integer r.

Lemma 2 Suppose α is a primitive field element for F_{2^m} where m is an even integer. Then α^3 is not primitive for F_{2^m}.

Proof. Set $m = 2r$. By induction on r we show that $2^m - 1$ is a multiple of 3. This obviously holds for $r = 1$. Assume that this property holds for all integers $1 \leq i \leq r$. Hence $2^{2r} = 3k + 1$ for some integer k. This implies that

$$2^{2(r+1)} = 2^{2r}2^2 = 4(3k + 1) = 12k + 4 = 3(4k + 1) + 1 = 3k' + 1.$$

The order of α is $2^m - 1$, hence $(\alpha^3)^{\frac{2^m-1}{3}} = 1$, that is the order of α^3 is at most $\frac{2^m-1}{3}$ implying that α^3 is not primitive. We show that α^3 has order

$\frac{2^m-1}{3}$. Suppose $\ell < \frac{2^m-1}{3}$ and $(\alpha^3)^\ell = 1$, that is $\alpha^{3\ell} = 1$; but $3\ell < 2^m - 1$ which is a contradiction since the order of α is $2^m - 1$. ∎

Lemma 3 Suppose α is a primitive nth root of unity with $n = 2^m - 1$ where m is a positive even integer. Then

$$\alpha^{\frac{ni}{3}+\ell} + \alpha^{\frac{2ni}{3}+\ell} = \alpha^\ell,$$

for $0 \le \ell \le n-1$ and $1 \le i \le n-1$.
Proof. Suppose $\alpha^{\frac{ni}{3}} + \alpha^{\frac{2ni}{3}} = \alpha^t$; then

$$\alpha^{2t} = \left(\alpha^{\frac{ni}{3}} + \alpha^{\frac{2ni}{3}}\right)^2 = \alpha^{\frac{ni}{3}} + \alpha^{\frac{2ni}{3}} = \alpha^t.$$

Thus $2t = t \pmod n$, and hence $t = 0 \pmod n$, implying that $\alpha^{\frac{ni}{3}} + \alpha^{\frac{2ni}{3}} = \alpha^0$. Multiplying both sides of this equation by α^ℓ we get the required property. ∎

Theorem 2 Let α be a primitive nth root of unity over F_2 where $n = 2^m - 1$ and m is an even integer. Let C_i, $i = 1, 3, \cdots, 2t-1$, be the ith cyclotomic coset of 2 modulo n. Then the stopping distance of parity-check matrix $H_m(2t+1)$ given by (2) is 3.
Proof. By Lemma 2, α^3 is not primitive and its order is $\frac{2^m-1}{3}$. Hence in the second block-row of $H_m(2t+1)$, the row corresponding to α^3, there are $\frac{2^m-1}{3}$ distinct elements each of which appeared three times.

The element α^0 appears three times in the second row of $H_m(2t+1)$; consider the three-element $\mathbf{v} := (\alpha^0, \alpha^0, \alpha^0)$ sub-row of the second row. The three-column submatrix of $H_m(2t+1)$ containing $\mathbf{v}$ is in the following form.

$$H = \begin{pmatrix} [\alpha^0] & [\alpha^{n/3}] & [\alpha^{2n/3}] \\ [(\alpha^3)^0] & [(\alpha^3)^0] & [(\alpha^3)^0] \\ [(\alpha^5)^0] & [(\alpha^5)^{n/3}] & [(\alpha^5)^{2n/3}] \\ \vdots & \vdots & \vdots \\ [(\alpha^{2t-1})^0] & [(\alpha^{2t-1})^{n/3}] & [(\alpha^{2t-1})^{2n/3}] \end{pmatrix}$$

We show that each block-row of H, considered as a binary matrix with m rows, represents a three-element stopping set, and hence the set of column-indices associated with H is an stopping set for $H_m(2t+1)$.

The columns of the second block-row of H are identical, and, by Lemma 3, the three columns of any other block-row of H are linearly dependent. Thus $s(H_m(2t+1)) \le 3$. This together with the fact that the first block-row of $H_m(2t+1)$ is $H_m(3)$ with stopping distance 3, implies $s(H_m(2t+1)) \le 3$.∎

References

[1] R.M. Tanner, "A recursive approach to low complexity codes," *IEEE Trans. Inform. Theory*, vol. 27, pp. 533–547, 1981.

[2] C. Di, D. Proietty, I.E. Telater, T.J. Richardson and R.L. Urbanke, "Finite-length analysis of low-density parity-check codes on the binary erasure channel," *IEEE Trans. Inform. Theory*, vol. 48, no. 6, pp. 1570–1579, June 2002.

[3] M. Esmaeili and V. Ravanmehr, "Stopping sets of binary parity-check matrices with constant weight columns and stopping redundancy of the associated codes," *Utilitas Math.*, vol. 76, pp. 265–276, July 2008.

[4] T. Etzion, "On the stopping redundancy of Reed-Muller codes," *IEEE Trans. Inform. Theory*, vol. 52, no. 11, pp. 4867–4879, Nov. 2006.

[5] M. Hivadi and M. Esmaeili, "On the stopping distance and stopping redundancy of product codes," *IEICE Trans. Fund.*, vol. E91-A, no. 8, pp. 2167–2173, Aug. 2008.

[6] N. Kashyap and A. Vardy, "Stopping sets in codes from designs," *Proc. IEEE Int. Symp. Inform. Theory*, p. 122, June-July, 2003.

[7] M. Esmaeili and M.J. Amoshahi, "On the Stopping distance of Array Code Parity-check Matrices," *IEEE Trans. Inform. Theory*, vol. 55, no. 8, pp. 3488–3493, Aug. 2009.

[8] A. Orlitsky, K. Viswanathan and J. Zhang, "Stopping set distribution of LDPC code ensembles," *IEEE Trans. Inform. Theory*, vol. 51, no. 3, pp. 929–953, Mar. 2005.

[9] S.-T. Xia and F.-W. Fu, "On the stopping distance of finite geometry LDPC codes," *IEEE Commun. Letters*, vol. 10, no. 5, pp. 381–383, May 2006.

[10] K.A.S. Abdel-Ghaffar and J.H. Weber, "Complete enumeration of stopping sets of full-rank parity-check matrices of Hamming codes," *IEEE Trans. Inform. Theory*, vol. 53, no. 9, pp. 3196–3201, Sept. 2007.

[11] M. Schwartz and A. Vardy, "On the stopping distance and the stopping redundancy of codes," *IEEE Trans. Inform. Theory*, vol. 52, no. 3, pp. 922–932, March 2006.