5-1995

On Primitive BCH Codes with Unequal Error Protection Capabilities

Robert H. Morelos-Zaragoza
Osaka University, robert.morelos-zaragoza@sjsu.edu

Shu Lin
University of Hawaii at Manoa

Recommended Citation

Robert H. Morelos-Zaragoza and Shu Lin. "On Primitive BCH Codes with Unequal Error Protection Capabilities" *Faculty Publications* (1995): 788-790. doi:10.1109/18.382027

Finally, for BCH codes we get

Theorem 3: Let $t = o(n^{\frac{1}{4}})$ and $l = [(i+1)/2]$, then in the BCH code of length $n = 2^m - 1$ and with minimum distance $2t+1$

$$b_i = \frac{\binom{n}{i}}{(n+1)^t}(1 + E_{2l})$$

where the error term is upperbounded as follows:

$$|E_{2l}| \leq \sqrt{2}\,(2l)^l \exp\left[2(t-1)^2 - \frac{l(n-2l)}{n}\right] n^{t-l}(1+o(1)).$$

Note:

After the correspondence had been submitted we were informed that a similar, slightly weaker (by a factor $\sqrt{n}$), bound can be derived from arguments presented in [2]. Their approach is quite different from that of ours.

Acknowledgment

The authors are grateful to the anonymous referees for helpful suggestions.

References

[1] W. Feller, *An Introduction to Probability Theory and Its Applications*. New York: Wiley, 1970.

[2] I. Gashkov and V. Sidelnikov, "Linear ternary quasiperfect codes correcting double errors," *Probl. Peredachi Inform.*, vol. 22, no. 4, pp. 43–48, 1986.

[3] T. Kasami, T. Fujiwara, and S. Lin, "An approximation to the weight distribution of binary linear codes," *IEEE Trans. Inform. Theory*, vol. IT-31, no. 6, pp. 769–780, 1985.

[4] I. Krasikov and S. Litsyn, "Bounds for Krawtchouk polynomials," in preparation.

[5] G. Lachaud, "Distribution of the weights of the dual code of the Melas code," *Discrete Math.*, vol. 79, pp. 103–106, 1989.

[6] G. Lachaud and J. Wolfmann, "The weights of the orthogonals of the extended quadratic binary Goppa codes," *IEEE Trans. Inform. Theory*, vol. 36, pp. 686–692, 1990.

[7] V. Levenshtein, "Krawtchouk polynomials and universal bounds for codes and designs in Hamming spaces," submitted for publication.

[8] J. H. van Lint, *Introduction to Coding Theory*. New York: Springer-Verlag, 1992.

[9] S. Litsyn, C. J. Moreno, and O. Moreno, "Divisibility properties and new bounds for cyclic codes and exponential sums in one and several variables," *Applicable Algebra in Eng., Commun. Comput.*, vol. 5, pp. 105–116, 1994.

[10] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. New York: North-Holland, 1977.

[11] C. J. Moreno and O. Moreno, "Exponential sums and Goppa codes I," *Proc. Amer. Math. Soc.*, vol. 111, pp. 523–531, 1991.

[12] ——, "Exponential sums and Goppa codes II," *IEEE Trans. Inform. Theory*, vol. 38, pp. 1222–1229, 1992.

[13] O. Moreno and C. J. Moreno, "The MacWilliams-Sloane conjecture on the tightness of the Carlitz-Uchiyama bound and the weights of duals of BCH codes," *IEEE Trans. Inform. Theory*, vol. 40, pp. 1894–1907, Nov. 1994.

[14] F. Rodier, "On the spectra of the duals of binary BCH codes of designed distance $\delta = 9$," *IEEE Trans. Inform. Theory*, vol. 38, pp. 478–479, 1992.

[15] V. M. Sidelnikov, "Weight spectrum of binary Bose–Chaudhuri–Hocquenghem codes," *Probl. Peredachi Inform.*, vol. 7, no. 1, pp. 14–22, 1971.

[16] P. Solé, "A limit law on the distance distribution of binary codes," *IEEE Trans. Inform. Theory*, vol. 36, pp. 229–232, 1990.

[17] G. Szegö, *Orthogonal Polynomials*. Providence, RI: Amer. Math. Soc. Colloq. Publ., vol. 23, 1975.

On Primitive BCH Codes with Unequal Error Protection Capabilities

Robert H. Morelos-Zaragoza, *Member, IEEE*,
and Shu Lin, *Fellow, IEEE*

***Abstract*—We present a class of binary primitive BCH codes that have unequal-error-protection (UEP) capabilities. We use a recent result on the span of their minimum weight vectors to show that binary primitive BCH codes, containing second-order punctured Reed–Muller (RM) codes of the same minimum distance, are binary-cyclic UEP codes. The values of the error correction levels for this class of binary LUEP codes are estimated.**

***Index Terms*—Unequal error protection codes, binary primitive BCH codes.**

I. Introduction

Unequal error protection codes protect some of the encoded message symbols against more errors than the error correction level given by their minimum Hamming distance. Linear unequal error protection (LUEP) codes were first introduced by Masnick and Wolf [1]. They discussed linear codes, specified by their parity check matrices, providing a level of error correction beyond that given by the minimum distance of the code, for some codeword positions. Gore and Kilgus [2] introduced an example $(15, 9)$ binary-cyclic UEP code with minimum distance 4 that can correct one information bit against the occurrence of two errors. That is, the most significant bit can always be decoded in the presence of up to two random errors in a received vector. Since then, other cyclic UEP codes have been introduced [3], [4]. Binary BCH codes form a popular family of cyclic codes that have found numerous practical applications, due to their ability to correct multiple random errors, as well as their efficient coding and decoding procedures. Therefore, it is of interest to find conditions under which binary BCH codes are binary LUEP codes.

To analyze the multilevel error correcting capabilities of binary linear codes, the concept of set of minimum weight vectors is fundamental.

Definition [5]: Let C be an (n, k, d) linear code. The set of minimum-weight codewords, denoted $\mathcal{M}$, is defined as

$$\mathcal{M} \triangleq \{\bar{c} \in C : 0 < \mathrm{wt}\,(\bar{c}) \leq 2\epsilon, \epsilon > t\}$$

where $\mathrm{wt}\,(\bar{c})$ denotes the Hamming weight of vector $\bar{c}$, and $t = \lfloor (d-1)/2 \rfloor$.

With the above definition, Boyarinov and Katsman [5] found conditions for linear codes to be LUEP codes:

Lemma 1: To provide the protection level ϵ for at least k^* information digits of an (n, k, d) linear code C, it is necessary and

Manuscript received August 18, 1993; revised May 2, 1994. Part of this work was supported by NASA under Grant NAG 5-931, and by the NSF under Grants NCR-88813480 and NCR-9115400. The material in this correspondence was presented at the International Symposium on Information Theory, Trondheim, Norway, 1994.

R. H. Morelos-Zaragoza was with the Department of Information and Computer Sciences, Faculty of Engineering Science, Osaka University, Toyonaka, Osaka 560, Japan. He is now with the Third Department, Institute of Industrial Science, University of Tokyo, 7-22-1, Roppongi, Minatoku, Tokyo 106, Japan.

S. Lin is with the Department of Electrical Engineering, University of Hawaii at Manoa, Honolulu, HI 96822 USA.

IEEE Log Number 9410417.

sufficient that the rank $r_{\mathcal{M}}$ of the set of minimum-weight codewords $\mathcal{M}$ be no greater than $k - k^*$.

In other words, if the set of minimum-weight vectors of a linear code C does not span it, then C is an LUEP code. In this correspondence, we consider binary codes with two levels of error protection. The above Lemma means that, in addition to correcting up to t random errors, C decodes k^* most important information bits when up to $\epsilon > t$ errors occur in a received vector. C is said to be a binary two-level error correcting code with separation vector $\overline{s} = (2\epsilon + 1, 2t + 1)$ for the message space $M = M_1 \times M_2$, where $M_1 = \{0, 1\}^{k^*}$ and $M_2 = \{0, 1\}^{k-k^*}$.

An interesting observation is the following: It is well known that k cyclic shifts of its generator polynomial span a cyclic code [6]. The condition of Lemma 1 implies that the generator polynomial of a cyclic UEP code must have Hamming weight greater than the minimum distance of the code.

II. Binary Primitive BCH Codes

It is well known that primitive BCH codes contain as subcodes punctured Reed–Muller (RM) codes of the same designed distance [7]. It is also known that their set of minimum-weight vectors span RM codes (punctured or not) [7]. Therefore, it seems natural to ask if BCH codes containing RM codes as *proper* subcodes are spanned by their set of minimum-weight codewords. As we show in the following, the answer to the above question is no, at least for a class of binary primitive BCH codes. Recently, Augot, Charpin, and Sendrier [8] have shown that some binary primitive BCH codes, those containing second-order punctured RM codes of the same designed minimum distance as subcodes, are not spanned by their set of minimum-weight codewords. In particular, they have found a proof, based on Newton's identities for minimum-weight codewords, of the following theorem.

Theorem 1: The minimum-weight codewords of the primitive BCH code of length $2^m - 1$ and minimum distance $2^{m-2} - 1$ are those of the punctured RM code of the same length and order 2.

We note that the above result holds for extended BCH and RM codes as well. Combining the results from Theorem 1 and Lemma 1, we obtain the following corollary.

Corollary 1: The $(2^m - 1, k, 2^{m-2} - 1)$ binary primitive BCH code is a binary two-level error correcting code with separation vector

$$\overline{s} = (2\epsilon + 1, 2^{m-2} - 1), \quad \epsilon > 2^{m-3} - 1$$

for the message space $M = M_1 \times M_2$, where $M_1 = \{0, 1\}^{k^*}$, $M_2 = \{0, 1\}^{k-k^*}$, with

$$k^* = k - \sum_{i=0}^{2} \binom{2^m}{i}.$$

Corollary 1 indicates that some primitive BCH codes are two-level error correcting codes. However, the level of error correction, ϵ, for the k^* most important information bits is unknown. How to obtain the value of ϵ is illustrated in the following examples.

Example 1: Let C be a $(63, 24, 15)$ BCH code. Then C contains a (63,22,15) second-order cyclic RM code, $\mathrm{RM}^*_{2,m}$, as a proper subcode. By directly computing the weight distribution of all cosets of $\mathrm{RM}^*_{2,m}$ in C, we verified that the minimum Hamming weight of codewords in $C - \mathrm{RM}^*_{2,m}$ is 17. It follows that C is a binary two-level error correcting code with separation vector $\overline{\boldsymbol{s}} = (17, 15)$ for the message space $M = \{0, 1\}^2 \times \{0, 1\}^{22}$. In other words, although C is capable of correcting any seven or less random errors, it decodes successfully the two most important bits even when $\epsilon = 8$ random errors occur in a received vector. This binary cyclic UEP code was found previously in a computer search [9] (it is the first $(63, 24)$ cyclic code listed, equivalent to C under the permutation $X^i \rightarrow X^{5i}$). △△

Example 2: The $(128, 36, 32)$ extended BCH code, denoted e-BCH(128), is a subcode of the $(128, 64, 16)$ third-order RM code, $\mathrm{RM}_{3,7}$, all of whose codewords have Hamming weight multiple of 4 [7], and the next Hamming weight, greater than 32, of codewords in $\mathrm{RM}_{3,7}$ is 36 [10]. Code e-BCH(128) contains the $(128, 29, 32)$ second-order RM code as a proper subcode. From Theorem 1, it follows that e-BCH(128) is an LUEP code with separation vector $\overline{\boldsymbol{s}} = (s_1, 32)$, $s_1 \geq 36$ for the message space $M = \{0, 1\}^7 \times \{0, 1\}^{29}$. With the aid of a computer, we found a codeword in e-BCH(128) of weight 36. Therefore, the $(127, 36, 31)$ primitive BCH code, obtained by puncturing e-BCH(128), is a binary two-level error correcting code with the same message space as e-BCH(128) and separation vector $\overline{\boldsymbol{s}} = (2\epsilon + 1, 2t + 1)$, with $\epsilon = 17, t = 15$. △△

The above examples show how difficult it is to find the exact value of ϵ. For $m \geq 8$, one way to find a lower bound on the value of ϵ is to determine the smallest binary cyclic RM code containing the given BCH code as a subcode. Let S_{BCH} denote the set of exponents of the zeros of the $(2^m - 1, k, 2^{m-2} - 1)$ binary primitive BCH code, $\mathrm{BCH}\,(2^m - 1, 2^{m-2} - 1)$, i.e., $S_{\mathrm{BCH}} = \{i : g(\alpha^i) = 0\}$, where $g(X)$ is the generator polynomial of C_{BCH}. In this correspondence we consider *narrow-sense* BCH codes, so that

$$S_{\mathrm{BCH}} = \{1, 2, \cdots, 2^{m-2} - 2\}.$$

For an integer i, let $\boldsymbol{b}(i)$ denote the binary representation of i, $\boldsymbol{b}(i) = (b_{i0}, b_{i1}, \cdots, b_{i(m-1)})$, such that

$$i = \sum_{j=0}^{m-1} b_{ij} 2^{m-j}, b_{ij} \in \{0, 1\}.$$

For $i \in S_{\mathrm{BCH}}$, $\boldsymbol{b}(i)$ is of the form

$$\boldsymbol{b}(i) = (00 b_{i2} \cdots b_{i(m-1)})$$

where $b_{i2}, \cdots, b_{i(m-1)}$ take all possible values except

$$b_{i2} = \cdots = b_{i(m-1)} = 1.$$

It is well known that an rth-order binary cyclic RM code of length $2^m - 1$, denoted $\mathrm{RM}^*_{r,m}$, has α^i as a zero if and only if $0 < W_2(i) \leq m - r - 1$, where $W_2(i)$ is the Hamming weight of $\boldsymbol{b}(i)$ [6]. That is, $g_{\mathrm{RM}}(\alpha^i) = 0$ if and only if $\boldsymbol{b}(i)$ has at least $(r + 1)$ zeros. The following vector of length $m = 2(r+1)$ and Hamming weight $r+1$

$$\boldsymbol{b}(i') = (0101 \cdots 01)$$

is the binary representation of the exponent of a zero $\alpha^{i'}$ of $\mathrm{RM}^*_{r,m}$, $i' \notin S_{\mathrm{BCH}}$. It follows that the order of $\mathrm{RM}^*_{r,m}$ must be such that $m < 2(r + 1)$ for i' to be in S_{BCH}, and we have that

$$\mathrm{RM}^*_{2,m} \subseteq \mathrm{BCH}\,(2^m - 1, 2^{m-2} - 1) \subset \mathrm{RM}^*_{r,m}$$

where $r \geq \lceil (m - 1)/2 \rceil$.

On the other hand, it is known [7] that codewords in $\mathrm{RM}_{r,m}$ have Hamming weight multiple of $2^{[(m-1)/r]}$, where $[x]$ denotes the

TABLE I
BINARY PRIMITIVE BCH CODES WITH UEP CAPABILITIES

m	n	k	d	k^*	$k-k^*$	ϵ	t
6	63	24	15	2	22	8	7
7	127	36	31	7	29	17	15
8	255	55	63	18	37	32 (*)	31
9	511	85	127	39	46	65 (*)	63
10	1023	133	255	77	56	128 (*)	127

integer part of a real number x. Therefore, with $r = \lceil(m-1)/2\rceil$, codewords in $\text{RM}_{r,m}$ have Hamming weight multiple of 2, for m even, and multiple of 4, for m odd. Let A_j denote the number of codewords in $\text{RM}^*_{r,m}$ of weight j. By a *gap* we mean the smallest integer δ such that $A_{2^{m-r}-1} \neq 0$, $A_{2^{m-r}} = \cdots = A_{2^{m-r}+(\delta-1)} = 0$, and $A_{2^{m-r}-1+\delta} \neq 0$. The above result says that the cyclic $\text{RM}^*_{r,m}$ code has a gap of at least 2 or 4, for m even or odd, respectively. We have proved the following theorem:

Theorem 2: The $(2^m-1, k, 2^{m-2}-1)$ binary primitive BCH code is a binary two-level error correcting code with separation vector

$$\bar{s} = (2\epsilon+1, 2t+1), \quad t = 2^{m-3}-1$$

$$\epsilon \geq \begin{cases} 2^{m-3}, & m \text{ even} \\ 2^{m-3}+1, & m \text{ odd} \end{cases}$$

for the message space $M = M_1 \times M_2$, where $M_1 = \{0,1\}^{k^*}$, $M_2 = \{0,1\}^{k-k^*}$, with

$$k^* = k - \sum_{i=0}^{2} \binom{2^m}{i}.$$

Some binary primitive BCH codes with UEP capabilities are listed in Table I. Entries indicated with (*) are lower bounds from Theorem 2.

REFERENCES

[1] B. Masnick and J. Wolf, "On linear unequal error protection codes," *IEEE Trans. Inform. Theory*, vol. IT-13, no. 4, pp. 600–607, July 1967.

[2] W. C. Gore and C. C. Kilgus, "Cyclic codes with unequal error protection," *IEEE Trans. Inform. Theory*, vol. IT-17, no. 2, pp. 214–215, Mar. 1971.

[3] V. N. Dynkin and V. A. Togonidze, "Cyclic codes with unequal symbol protection," *Prob. Pered. Inform.*, vol. 12, no. 1, pp. 24–28, Jan./Mar. 1976.

[4] W. J. van Gils, "Two topics on linear unequal error protection codes: Bounds on their length and cyclic code classes," *IEEE Trans. Inform. Theory*, vol. IT-29, no. 6, pp. 866–876, Nov. 1983.

[5] I. M. Boyarinov and G. L. Katsman, "Linear unequal error protection codes," *IEEE Trans. Inform. Theory*, vol. IT-27, no. 2, pp. 168–175, Mar. 1981.

[6] W. W. Peterson and E. J. Weldon, Jr., *Error-Correcting Codes*, 2nd ed. Cambridge, MA: MIT Press, 1972.

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

[8] D. Augot, P. Charpin, and N. Sendrier, "Studying the locator polynomials of minimum weight codewords of BCH codes," *IEEE Trans. Inform. Theory*, vol. 38, no. 3, pp. 960–973, May 1992.

[9] M. C. Lin, C. C. Lin, and S. Lin, "Computer search for binary cyclic UEP codes of odd length up to 65," *IEEE Trans. Inform. Theory*, vol. 36, no. 4, pp. 924–935, July 1990.

[10] T. Kasami and N. Tokura, "Weight distribution of (128, 64) Reed–Muller code," *IEEE Trans. Inform. Theory*, vol. IT-17, Sept. 1971.

Constructing SCN Bases in Characteristic 2

Alain Poli

***Abstract*—A simple deterministic algorithm to construct a normal basis of GF(q^n) over GF(q) ($q = p^r$, p prime) is given. When $p = 2$, we deduce a (SCN) basis of GF(q^n) over GF(q) for n odd, or $n = 2t$, t odd. In characteristic 2 these cases are known to be the only possible ones for which there exists an SCN basis.**

***Index Terms*—Finite fields, self-complementary normal bases, normal bases.**

I. INTRODUCTION

Following Wang [6] we consider some element β in GF(q^n) ($q = 2^r$) which generates a normal basis over GF(q). From that β we deduce an element α which generates an SCN (self-complementary normal) basis over GF(q), that is a basis $\{\alpha, \alpha^q \ldots \alpha^{q^{n-1}}\}$ verifies $\text{Tr}_q(\alpha^{q^i}\alpha^{q^j}) = \delta_{i,j}$ (Tr_q is the trace function of GF(q^n) over GF(q)).

The correspondence is divided into two parts.

In Section II we give a deterministic construction of a normal basis of GF(q^n) over GF(q), available in the general case.

In Section III we first propose a very simple construction of an SCN basis, when n is odd and $q = 2^r$. Then we propose a second construction when $n = 2t$ (t odd) and q a power of 2. In both sections we use the factorization of $X^n - 1$ over GF(q).

II. CONSTRUCTING A NORMAL BASIS

Using [5, ch. 3, Proposition 29], for example, we find that the number of elements in GF(4^{10}) not generating a normal basis is 357,376. This is large enough to make a probabilistic search impossible in the worst case.

Suppose GF(q^n) is represented as GF(q)$[X]/(p(X))$, with $p(X)$ being some irreducible polynomial over GF(q). It may be possible that no power of X generates a normal basis, as it can be seen from the case $q = 2$ and $p(X) = 1 + X^3 + X^6$.

The construction we propose uses at most n elements in order to get a normal basis of GF(q^n) over GF(q). For example, at most 7 elements are necessary to obtain a normal basis of GF(4^{10}) over GF(4): $X, X^2, X^3, X^5, X^6, X^7, X^9$.

Now let us give our construction.

Set φ for the exponentiation by q in GF(q^n) ($q = p^r$, p prime). Suppose that the primary decomposition of $X^n - 1$ over GF(q) is $q_1 . q_2 \cdots q_N$ with $q_i = p_i^m$ (m is the multiplicity, p_i is irreducible). Now set $p_N = X - 1$, $M_i = (X^n - 1)/q_i$, and $Q_i = M_i(p_i)^{m-1}$, $i = 1, 2, \cdots, N$.

Lemma 1: We have the following points:

1) GF(q^n) is the direct sum of the GF(q)-vector spaces Ker $(q_i(\varphi))(= G_i)$, for $i = 1, 2, \cdots, N$.
2) An element of GF(q^n) generates a normal basis over GF(q) if and only if (iff) its component in G_i is in Ker$(q_i(\varphi))\backslash$Ker$(p_i^{m-1}(\varphi))$.

Manuscript received February 15, 1993; revised February 6, 1994.

The author is with AAECC/IRIT, University P. Sabatier, 31062 Toulouse Cedex, France.

IEEE Log Number 9410402.

0018-9448/95$04.00 © 1995 IEEE