San Jose State University
SJSU ScholarWorks

Faculty Publications | Electrical Engineering Department

1-1-1994

On a Class of Optimal Nonbinary Linear Unequal-Error-Protection Codes for Two Sets of Messages

Robert H. Morelos-Zaragoza
University of Hawaii at Manoa, robert.morelos-zaragoza@sjsu.edu

Shu Lin
University of Hawaii at Manoa

Follow this and additional works at: http://scholarworks.sjsu.edu/ee_pub

Part of the Electrical and Computer Engineering Commons

Recommended Citation
Robert H. Morelos-Zaragoza and Shu Lin. "On a Class of Optimal Nonbinary Linear Unequal-Error-Protection Codes for Two Sets of Messages" *Faculty Publications* 40.1 (1994): 196-200. doi:10.1109/18.272481

This Article is brought to you for free and open access by the Electrical Engineering Department at SJSU ScholarWorks. It has been accepted for inclusion in Faculty Publications by an authorized administrator of SJSU ScholarWorks. For more information, please contact scholarworks@sjsu.edu.

Proposition 6: Let $m \geq p$ and j arbitrary. If all weights in $\mathcal{C}$ are divisible by 2^p, then the degree of the set $\sum_{i \equiv j(2^m)} \mathcal{A}_i$ does not exceed $2^m - 2^p$.

Proof: If the set $\sum_{i \equiv j(2^m)} \mathcal{A}_i$ is empty, the proposition is trivial. If $\sum_{i \equiv j(2^m)} \mathcal{A}_i$ is nonempty, then j must be divisible by 2^p. Hence, the set $\sum_{i \equiv j(2^m)} \mathcal{S}_i$ of degree $2^m - 1$ is contained in the set $\sum_{i \equiv 0(2^p)} \mathcal{S}_i$ of degree $2^p - 1$. By assumption, the latter set contains the code $\mathcal{C}$, so $\deg_{\mathcal{C}} (\mathcal{C} \cap \sum_{i \equiv 0(2^p)} \mathcal{S}_i) = 0$. Hence,

$$\deg_{\mathcal{C}} \left(\mathcal{C} \cap \sum_{i \equiv j(2^m)} \mathcal{S}_i \right) = \deg \left(\sum_{i \equiv j(2^m)} \mathcal{A}_i \right) \leq (2^m - 1) - (2^p - 1) = 2^m - 2^p. \quad \square$$

Note that Brouwer's theorem 1 corresponds to the case $p = 1$, $m = 2$, and $j = 0$. It directly follows from known facts about the structure of second order Reed–Muller codes. Much more can be said if $p = m - 1$.

Proposition 7: If all weights in the linear code $\mathcal{C}$ are divisible by 2^{m-1}, then the degree of $\sum_{i \equiv 0(2^m)} \mathcal{A}_i$ does not exceed m.

Proof: (Based on Brouwer's proofs of Theorems 2 and 3.) In virtue of Proposition 1, part iii), we have to show that an $(m+1)$-dimensional linear code $\mathcal{C}$ all of whose words have weight divisible by 2^{m-1} must have an even number of codewords whose weight is divisible by 2^m. We proceed by induction on m. The case $m = 1$ is trivial. Take $m \geq 2$ and choose a minimal codeword $X \in \mathcal{C}$ such that $|X| \equiv 2^{m-1}(2^m)$. (We are done if X does not exist.) The formula

$$|X + Y| - |Y| = |X| - 2|X \cap Y|$$

implies that $|X \cap Y| \equiv 0(2^{m-2})$ for all $Y \in \mathcal{C}$. The punctured code $\mathcal{C}_{\overline{X}} := \{Y \backslash X \mid Y \in \mathcal{C}\}$ satisfies the induction hypothesis for $m - 1$, so it contains an even number of words with $|Y \backslash X| \equiv 0(2^{m-1})$. Now from

$$|X + Y| \equiv |Y|(2^m) \Leftrightarrow 2|X \cap Y| \equiv 2^{m-1}(2^m) \Leftrightarrow |Y \backslash X| \equiv 2^{m-2}(2^{m-1})$$

we infer that an even number of cosets of $\{\phi, X\}$ in $\mathcal{C}$ contains exactly one word whose weights is divisible by 2^m and each of the remaining cosets contains an even number of words whose weight is divisible by 2^m. $\square$

Open Problem: Does a result comparable to Proposition 7 exist for $p \leq m - 2$? The first nontrivial case is $m = 4, p = 2$. Proposition 6 implies that in all doubly even codes the words whose weight is divisible by 16 constitute a set of degree ≤ 12. On the other hand, the direct sum of three [7, 3, 4] simplex codes is 9-dimensional code for which the zero vector is the only word whose weight is divisible by 16. Does a doubly even code with $\deg(\sum_{i \equiv 0(16)} \mathcal{A}_i) = 10$ exist? The following proposition may be of some value.

Proposition 8: Let $\mathcal{C}$ be a binary linear $[n, k]$ code, and let $\mathcal{X} \subset \mathcal{C}$ be any subset. Then $\deg_{\mathcal{C}} (\mathcal{X}) < k - r$ if and only if all shortened codes $\mathcal{C}^{\overline{T}}$ with respect to coordinate sets T of cardinality $\leq r$ intersect $\mathcal{X}$ in an even number of codewords.

Proof: The codes $\mathcal{C}^{\overline{T}}$ with $|T| \leq r$ generate the Reed–Muller code $\mathfrak{RM}(r, \mathcal{C})$. Now apply part iii) of Proposition 1. $\square$

Example: Let $\mathcal{C}$ be the extended binary Golay code, and let $I := \{0, 16\}$. Using the fact that the words of fixed weight in $\mathcal{C}$ form a five-design, we calculate the number of codewords in $\mathcal{C} \cap \mathcal{A}_I$. For $|T| = 0, 1, 2, 3, 4, 5$, this number is 760, 254, 78, 22, 6, 2, respectively, but for $|T| = 6$, odd intersections must occur. Hence, $\deg(\mathcal{A}_I) = 6$.

References

[1] A. E. Brouwer, "The linear programming bound for binary linear codes," *IEEE Trans. Inform. Theory*, vol. 39, pp. 677–680, 1993.

[2] J. Dieudonné, *La géométrie des groupes classiques.* Berlin: Springer, 1971.

[3] T. Kasami, N. Tokura, and S. Azumi, "On the weight enumeration of weights less than 2.5d of Reed–Muller codes," *Inform. Contr.*, vol. 30, pp. 380–395, 1976.

[4] ——, "On the weight enumeration of weights less than 2.5d of Reed–Muller Codes," Faculty of Eng. Sci., Rep. Osaka Univ., Japan, 1974.

[5] M. E. Lucas, "Sur les congruences des nombres Euleriennes, et des coefficients différentials des fonctions trigonométriques, suivant un-module premier," *Bull. Soc. Math. France*, vol. 6, pp. 49–54, 1878.

[6] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes.* New York: North-Holland, 1983.

[7] J. Simonis, "Reed-Muller codes," Faculty of Mathemat. Inform., Rep. 87-23, ISSN 0920-8577, Delft Univ. of Technol., 1987.

On a Class of Optimal Nonbinary Linear Unequal-Error-Protection Codes for Two Sets of Messages

Robert H. Morelos-Zaragoza and Shu Lin

***Abstract*— Several authors have addressed the problem of designing good linear unequal error protection (LUEP) codes. However, very little is known about good *nonbinary* LUEP codes. We present a class of *optimal nonbinary* LUEP codes for two different sets of messages. By combining t-error-correcting Reed–Solomon (RS) codes and shortened nonbinary Hamming codes, we obtain nonbinary LUEP codes that protect one set of messages against any t or fewer symbol errors and the remaining set of messages against any single symbol error. For $t \geq 2$, we show that these codes are optimal in the sense of achieving the Hamming lower bound on the number of redundant symbols of a nonbinary LUEP code with the same parameters.**

***Index Term*—Unequal error protection codes.**

I. Introduction

Let C be a linear (n, k) block code over $\mathrm{GF}(q)$ with generator matrix G. Let message vectors $\overline{u} \in \mathrm{GF}(q)^k$ consist of 2 parts $\overline{u}_1, \overline{u}_2$ where $\overline{u}_i$ is a k_i-symbol component message, for $i = 1, 2$, $k = k_1 + k_2$, i.e.,

$$\overline{u} = (\overline{u}_1, \overline{u}_2), \quad \overline{u}_1 \in \mathrm{GF}(q)^{k_1}, \quad \overline{u}_2 \in \mathrm{GF}(q)^{k_2}.$$

Define the *separation vector* of C as

$$\overline{s}(G) = (s_1(G), s_2(G))$$

with

$$s_i(G) = \min\{\mathrm{wt}(\overline{u}G) | \overline{u}_j \in \mathrm{GF}(q)^{k_j}, \ j = 1, 2, \ \overline{u}_i \neq 0\}$$

where $i = 1, 2$, $k = k_1 + k_2$, and $\mathrm{wt}(\overline{x})$ is the Hamming weight of $\overline{x} \in \mathrm{GF}(q)^n$. The parameter

$$t_i(G) \triangleq \lfloor (s_i(G) - 1)/2 \rfloor,$$

Manuscript received June 9, 1992; revised October 23, 1993. This work was supported by the NSF under Grants NCR-88813480, NCR-9115400, and by NASA under Grant NAG 5-931. This paper was presented in part at the International Symposium on Information Theory and Its Applications, Honolulu, HI, November 27–30, 1990.

The authors are with the Department of Electrical Engineering, University of Hawaii at Manoa, Honolulu, HI 96822.

IEEE Log Number 9215117.

0018-9448/94$04.00 © 1994 IEEE

is called the *level of protection* for the ith component message, $i = 1, 2$. ($\lfloor x \rfloor$ denotes the largest integer less than or equal to x.) Note that if $s_1(G) = s_2(G)$, then C is a conventional linear (n, k) block code with minimum distance $d_{\min} = s_2(G)$ that protects all k message symbols against any $\lfloor (s_2(G)-1)/2 \rfloor$ or less random errors.

For convenience, we will write s_i and t_i instead of $s_i(G)$ and $t_i(G)$, keeping in mind that both parameters depend on the encoding rule of linear code C, i.e., the generator matrix G. We will also assume, without loss of generality, that we have an LUEP code C with separation vector $\bar{s}$, with both components distinct, i.e., $s_1 > s_2$.

We call C a linear (t_1, t_2)-error-correcting code over $\mathrm{GF}(q)$ for the message space

$$M = \mathrm{GF}(q)^{k_1} \times \mathrm{GF}(q)^{k_2}.$$

Boyarinov and Katsman's (BK) optimal binary LUEP codes of separation vector (5, 3) [1], were constructed by combining parity check matrices of binary 2-error-correcting and 1-error-correcting BCH codes. Recently, M. C. Lin and S. Lin [2] generalized the above class and constructed optimal binary LUEP codes of separation vector (5, 3) by combining the parity check matrix of a binary 2-error-correcting BCH code of length $2^m - 1$, and the parity check matrix of a shortened binary Hamming code, whose columns belong to the field $\mathrm{GF}(2^{l+m})$. For $l = m$, these codes are equivalent to BK LUEP codes. Unfortunately, the construction method used in [2] yields binary $(t, 1)$-error-correcting codes which are not optimal for $t > 2$.

In [1], a class of binary LUEP codes with separation vector $(2t+1, 3)$, $t \geq 2$, based on t-error-correcting BCH codes and Hamming codes is also presented, and it is shown that these codes are asymptotically optimal. In this paper, the class of optimal binary LUEP codes of [2] is generalized to symbols over the field $\mathrm{GF}(2^s)$. The codes obtained are optimal not only for separation vector (5, 3), as in the binary case, but in general for separation vectors $\bar{s} = (2t+1, 3)$, with $t \geq 2$. Our result constitutes a generalization of the asymptotically optimal binary LUEP codes of Boyarinov and Katsman to codes over any Galois field $\mathrm{GF}(2^s)$, $s \geq 3$.

II. Binary (2, 1)-Error-Correcting Codes

Let α be a primitive element of $\mathrm{GF}(2^m)$. Let $C(2)$ be the binary linear code with parity check matrix

$$H(2) = \left(\begin{array}{cccc|ccc} 1 & \alpha & \cdots & \alpha^{2^m-2} & 0_m & \cdots & 0_m \\ 1 & \alpha^3 & \cdots & \alpha^{3(2^m-2)} & \beta_1 & \cdots & \beta_{2^{m+l}-2^m} \\ 0_l & 0_l & \cdots & 0_l & & & \end{array}\right) \tag{1}$$

where each power of α is represented by a binary column vector of length m, 0_m, 0_l represent all zero column vectors of lengths m and l, respectively, and, for $l \geq 0$, $\beta_1, \cdots, \beta_{2^{m+l}-2^m}$ represent all binary column vectors of length $m+l$ having the last l entries not all zero.

Theorem 1: $C(2)$ is a $(2^{m+l}-1, 2^{m+l}-2m-l-1)$ LUEP code, with separation vector $\bar{s} = (s_1, s_2)$, $s_1 \geq 5$, and $s_2 = 3$, for the message space $M = M_1 \times M_2$ where $M_1 = \{0, 1\}^{2^m-m-1}$ and $M_2 = \{0, 1\}^{2^{m+l}-2^m-m-l}$.

Proof: See [2].

III. (2, 1)-Error-Correcting Codes Over $\mathrm{GF}(2^s)$

Let γ be a primitive element of $\mathrm{GF}(2^{ms})$. Let $C(2^s)$ be the linear code over $\mathrm{GF}(2^s)$ with parity check matrix

$$H(2^s) = \left(\begin{array}{cccc|ccc} 1 & \gamma & \cdots & \gamma^{2^{sm}-2} & 0_m & \cdots & 0_m \\ 1 & \gamma^2 & \cdots & \gamma^{2(2^{sm}-2)} & 0_m & \cdots & 0_m \\ 1 & \gamma^3 & \cdots & \gamma^{3(2^{sm}-2)} & & & \\ 1 & \gamma^4 & \cdots & \gamma^{4(2^{sm}-2)} & \phi_1 & \cdots & \phi_{n_b} \\ 0_l & 0_l & \cdots & 0_l & & & \end{array}\right) \tag{2}$$

where each power of γ is represented as a column vector of length m over $\mathrm{GF}(2^s)$, $s > 1$, 0_i represents a $(2^s$-ary) column vector of i zeros, and $\phi_1, \cdots, \phi_{n_b}$ represent column vectors, not multiples of each other, of length $2m+l$ over $\mathrm{GF}(2^s)$ for which the last l entries are not all zeros where

$$n_b = \frac{2^{s(2m)}(2^{sl}-1)}{2^s-1}.$$

Note that $H(2^s)$ can be written as

$$H(2^s) = \begin{pmatrix} H_{aa}(2^s) & O_1 \\ H_{ab}(2^s) & H_{ba}(2^s) \\ O_2 & H_{bb}(2^s) \end{pmatrix} = (H_1 \mid H_2) \tag{3}$$

where

$$H_a(2^s) = \begin{pmatrix} H_{aa}(2^s) \\ H_{ab}(2^s) \end{pmatrix}$$

is the parity check matrix of a BCH code $C_a(2^s)$ over $\mathrm{GF}(2^s)$ of length $n_a = 2^{sm}-1$, dimension $k_a \geq 2^{sm}-4m-1$, and minimum distance $d_a \geq 5$; $H_{aa}(2^s)$ is the parity check matrix of a BCH code $C_{aa}(2^s)$ over $\mathrm{GF}(2^s)$, which contains $C_a(2^s)$, of length n_a, dimension $k_{aa} \geq 2^{sm}-2m-1$, and minimum distance $d_{aa} \geq 3$;

$$H_b(2^s) = \begin{pmatrix} H_{ba}(2^s) \\ H_{bb}(2^s) \end{pmatrix}$$

is the parity check matrix of a shortened Hamming code $C_b(2^s)$ of length $n_b = 2^{2sm}(2^{sl}-1)/(2^s-1) = 2^{2sm}(2^{s(l-1)}+\cdots+2^s+1)$, dimension $k_b = n_b - 2m - l$ and minimum distance $d_b \geq 3$; and $C_{bb}(2^s)$ is a linear code over $\mathrm{GF}(2^s)$, containing $C_b(2^s)$, of length n_b, dimension $k_{bb} \geq n_b - l$ and minimum distance $d_{bb} = 2$; and O_1 and O_2 denote all zero matrices of appropriate dimensions.

Theorem 2: $C(2^s)$ is an (n, k) LUEP code over $\mathrm{GF}(2^s)$, $s > 2$, with parameters,

$$n = 2^{2sm}(2^{s(l-1)} + 2^{s(l-2)} + \cdots + 2^s + 1) + 2^{sm} - 1,$$

$$k \geq n - 4m - l,$$

$$\bar{s} = (s_1, s_2), \quad s_1 \geq 5, \quad s_2 = 3,$$

for the message space $M = \mathrm{GF}(2^s)^{k_1} \times \mathrm{GF}(2^s)^{k_2}$ where

$$k_1 \geq 2^{sm} - 2m - 1, \quad \text{and}$$
$$k_2 \geq 2^{2sm}(2^{s(l-1)} + \cdots + 2^s + 1) - 2m - l.$$

In other words, $C(2^s)$ protects the first $2^{sm} - 2m - 1$ information symbols against any combination of 2 or less symbol errors, and the remaining information symbols against any single symbol error.

Code $C(2^s)$ can be transformed into a systematic code with the same parameters and separation vector. This is done by performing elementary row operations on its parity check matrix, which do not change the error protection level of any code symbol, as indicated in [1].

Note that for $m = 1$, $C_a(2^s)$ and $C_{aa}(2^s)$ are Reed–Solomon (RS) codes over $\mathrm{GF}(2^s)$. In this case, the expressions for k_1 and k_2 in Theorem 2 above become equalities.

Proof: (Similar to [1, Theorem 1]) That $C(2^s)$ has minimum distance $d_{\min} = s_2 = 3$ follows easily from the fact that all columns of $H(2^s)$ in (3) are different and we can find 3 columns from H_2 in (3) that add to the all-zero vector [3]. It remains to show that $s_1 \geq 5$. Let $\bar{h}_i^{(j)}$ denote the ith column of submatrix H_j in (3), $j = 1, 2$. We need to prove that any column $\bar{h}_i^{(1)}$ is linearly dependent on no less than four other columns of $H(2^s)$. This is done by considering the following cases of linear combinations of columns of $H(2^s)$.

- Three columns:
  i) $\overline{h}_{i_1}^{(1)} + \overline{h}_{i_2}^{(1)} + \overline{h}_{i_3}^{(1)} \neq \overline{0}$, by definition of $H_a(2^s)$.
  ii) $\overline{h}_{i_1}^{(1)} + \overline{h}_{i_2}^{(1)} + \overline{h}_{i_3}^{(2)} \neq \overline{0}$, since $\overline{h}_{i_3}^{(2)} \neq \overline{0}$.
  iii) $\overline{h}_{i_1}^{(1)} + \overline{h}_{i_2}^{(2)} + \overline{h}_{i_3}^{(2)} \neq \overline{0}$, since $\overline{h}_{i_1}^{(1)} \neq \overline{0}$.
- Four columns:
  i) $\sum_{j=1}^{4} \overline{h}_{i_j}^{(1)} \neq \overline{0}$, by definition of $H_a(2^s)$.
  ii) $\sum_{j=1}^{3} \overline{h}_{i_j}^{(1)} + \overline{h}_{i_4}^{(2)} \neq \overline{0}$, since $\overline{h}_{i_4}^{(2)} \neq \overline{0}$.
  iii) $\overline{h}_{i_1}^{(1)} + \overline{h}_{i_2}^{(1)} + \overline{h}_{i_3}^{(2)} + \overline{h}_{i_4}^{(2)} \neq \overline{0}$, since columns are different.
  iv) $\overline{h}_{i_1}^{(1)} + \sum_{j=2}^{4} \overline{h}_{i_j}^{(2)} \neq \overline{0}$, since $\overline{h}_{i_1}^{(1)} \neq \overline{0}$.

Example: Let $l = m = 1$ and $s = 3$. $C(2^3)$ is then a (71, 66) LUEP code over GF(2^3), with 5 information symbols protected against any two or less random errors, and 61 information symbols protected against any single random error. This code meets the Hamming lower bound on the number of redundant symbols from GF(2^3), as will be shown in the next paragraph, and therefore is an example of an optimal linear two-level (2, 1)-error-correcting code over GF(2^3).

A. Hamming Bound

For a binary linear (t_1, t_2)-error-correcting (n, k) code, the following Hamming bound was first derived by Boyarinov and Katsman [1]:

$$2^{n-k} \geq \sum_{i=0}^{t_2} \binom{n}{i} + \sum_{j=t_2+1}^{t_1} \sum_{i=0}^{t_2} \binom{n-k_1}{i} \binom{k_1}{j-i}. \tag{4}$$

For linear codes over GF(2^s), we obtain a lower bound on the number of redundant symbols as follows: 1) the number of cosets is now $2^{s(n-k)}$; 2) the number of vectors in $(\mathrm{GF}(2^s))^n$ of weight less than or equal to t_2 is

$$\sum_{i=0}^{t_2} \binom{n}{i} (2^s - 1)^i;$$

and iii) the number of vectors over GF(2^s) of weight w, such that $t_2 < w \leq t_1$, with at least one nonzero component in the k_1 most significant positions is

$$\sum_{j=t_2+1}^{t_1} \sum_{i=0}^{t_2} \binom{n-k_1}{i} \binom{k_1}{j-i} (2^s - 1)^j.$$

As a result, we obtain the following Hamming bound for a linear two-level (t_1, t_2)-error-correcting code over GF(2^s):

$$2^{s(n-k)} \geq \sum_{i=0}^{t_2} \binom{n}{i} (2^s - 1)^i + \sum_{j=t_2+1}^{t_1} \sum_{i=0}^{t_2} \binom{n-k_1}{i} \binom{k_1}{j-i} (2^s - 1)^j. \tag{5}$$

For the class of codes of Theorem 2, we let $t_1 = 2$ and $t_2 = 1$ in (5), obtaining

$$\begin{aligned} 2^{s(n-k)} \geq\ & 1 + (2^{sm} - 1)(2^s - 1) \\ & + (2^{sm} - 2m - 1)(2^{sm-1} + m - 1)(2^s - 1)^2 \\ & + 2^{2sm}(2^{sl} - 1)[1 + (2^{sm} - 2m - 1)(2^s - 1)]. \end{aligned} \tag{6}$$

We have evaluated (6) for different values of l, s, and m and found that Theorem 2 gives optimal codes for $m = 1$, $s > 2$, and $l > 0$. From (6), with $m = 1$, we can show that

$$2^{s(n-k)} \geq 2^{s(l+4)-1}(1 + \Delta)$$

where $0 < \Delta < 1$. Therefore, $n - k \geq l + 4$. Note that for $m = 1$, codes from Theorem 2 have redundancy $n - k = l + 4$.

We conclude that linear (2, 1)-error-correcting codes over GF(2^s), with parity check matrix (2) and $m = 1$ (i.e., the upper left submatrix of (2) is the parity check matrix of an RS code), are optimal linear codes.

IV. $(t, 1)$-Error-Correcting Codes OverGF(2^s)

Let $C(2^s)$ be the linear code over GF(2^s) with parity check matrix as in (3) where $H_a(2^s)$ is now the parity check matrix of a t-error-correcting BCH code $C_a(2^s)$ over GF(2^s) of length $n_a = 2^{sm} - 1$ and dimension $k_a \geq 2^{sm} - 2mt - 1$, and $H_{aa}(2^s)$ is the parity-check matrix of a $(t-1)$-error-correcting BCH code $C_{aa}(2^s)$ over GF(2^s) of length $n_{aa} = 2^{sm} - 1$ and dimension $k_{aa} \geq 2^{sm} - 2m(t-1) - 1$.

Theorem 3: $C(2^s)$ is an (n, k) LUEP code over GF(2^s), $s > 2$, with parameters

$$\begin{aligned} & n = 2^{2sm}(2^{s(l-1)} + 2^{s(l-2)} + \cdots + 2^s + 1) + 2^{sm} - 1 \\ & k \geq n - 2mt - l \\ & \overline{s} = (s_1, s_2), \quad s_1 \geq 2t + 1, \quad s_2 \geq 3 \end{aligned} \tag{7}$$

for the message space $M = \mathrm{GF}(2^s)^{k_1} \times \mathrm{GF}(2^s)^{k_2}$ where

$$\begin{aligned} & k_1 \geq 2^{sm} - 2m(t-1) - 1 \quad \text{and} \\ & k_2 \geq 2^{2sm}(2^{s(l-1)} + \cdots + 2^s + 1) - 2m - l. \end{aligned}$$

Code $C(2^s)$ can be transformed into a systematic code with the same parameters and separation vector. This is done by performing elementary row operations on its parity check matrix, which do not change the error protection level of any code symbol, as indicated in [1]. Again note that for $m = 1$, $C_a(2^s)$ and $C_{aa}(2^s)$ are Reed–Solomon (RS) codes over GF(2^s). In this case, the expressions for k_1 and k_2 in Theorem 3 above become equalities.

Proof: (Similar to the proof of Theorem 2) The minimum distance of $C(2^s)$ is $d_{\min} = s_2 = 3$. That any column $\overline{h}_i^{(1)}$ from submatrix H_1 in (3) is linearly dependent on no less than $2t$ other columns of $H(2^s)$ is shown as follows.

- Up to $2t - 2$ columns: $\sum_{j=1}^{m} \overline{h}_{i_j}^{(1)} + \sum_{j'=1}^{2t-2-m} \overline{h}_{i_{j'}}^{(2)} = \overline{0}$, contradicts the definition of $H_{aa}(2^s)$, for $1 \leq m \leq 2t - 2$.
- $2t - 1$ columns: $\sum_{j=1}^{m} \overline{h}_{i_j}^{(1)} + \sum_{j'=1}^{2t-1-m} \overline{h}_{i_{j'}}^{(2)} = \overline{0}$. Divide into two cases:
  i) $m = 2t - 1$, contradicts the definition of $H_a(2^s)$.
  ii) $1 \leq m \leq 2t - 2$, contradicts the definition of $H_{aa}(2^s)$.
- $2t$ columns: $\sum_{j=1}^{m} \overline{h}_{i_j}^{(1)} + \sum_{j'=1}^{2t-m} \overline{h}_{i_{j'}}^{(2)} = \overline{0}$. Divide into three cases:
  i) $m = 2t$, contradicts the definition of $H_a(2^s)$.
  ii) $m = 2t - 1$, impossible because $\overline{h}_{i_{j'}}^{(2)} \neq \overline{0}$.
  iii) $1 \leq m \leq 2t - 2$, contradicts the definition of $H_{aa}(2^s)$. □

A. Hamming Bound, $t = 3$

Let $t_1 = 3$ and $t_2 = 1$ in inequality (5). Then

$$2^{s(n-k)} \geq \sum_{i=0}^{1} \binom{n}{i} (2^s - 1)^i + \sum_{j=2}^{3} \sum_{i=0}^{1} \binom{n-k_1}{i} \binom{k_1}{j-i} (2^s - 1)^j$$

with $m = 1$, we have for codes from Theorem 3,

$$\begin{aligned} 2^{s(n-k)} \geq\ & 1 + 2^{2s}(2^{sl} - 1) + (2^s - 1)(2^s - 1) \\ & + (2^s - 5)(2^{s-1} - 3)(2^s - 1)^2 \\ & + 2^{2s}(2^{sl} - 1)(2^s - 1) + 4(2^s - 5)(2^s - 1)^2 \\ & + \frac{1}{6}(2^s - 5)(2^s - 6)(2^s - 7)(2^s - 1)^3 \\ & + \{2^{2s}(2^{sl} - 1)(2^s - 1)^2 + 4(2^s - 1)^3\}(2^s - 5)(2^s - 3) \\ =\ & 2^{s(l+6)-1}(1 + \Delta) \end{aligned}$$

where $1 > \Delta > -\frac{1}{2}$, for $s \geq 4$. Therefore, a linear nonbinary two-level (3, 1)-error-correcting code with parameters as in (7) requires at least $l+6$ redundant symbols. For $t = 3$ and $m = 1$, the codes given by Theoerm 3 have $2t + l = l + 6$ redundant symbols. We conclude that the class of codes being considered is optimal for $t = 3$, and $m = 1$.

B. Asymptotic Hamming Bound

For $t_1 = t$, $t > 3$, and $t_2 = 1$, the Hamming bound (5) becomes practically impossible to evaluate. From (5), we obtain

$$2^{s(n-k)} \geq n(2^s - 1) + 1 + \sum_{j=2}^{t} \binom{k_1}{j} (2^s - 1)^j + (n - k_1) \sum_{j=2}^{t} \binom{k_1}{j-1} (2^s - 1)^j. \quad (8)$$

We are going to derive an asymptotic equivalent of (8), for fixed t and large s. A good lower bound on (8) is obtained by taking only the most dominant term,

$$2^{s(n-k)} > (n - k_1) \sum_{j=2}^{t} \binom{k_1}{j-1} (2^s - 1)^j. \quad (9)$$

A lower bound on the sum of binomial coefficients is given by [3]

$$\sum_{j=1}^{t} \binom{k_1}{j-1} \geq 2^{k_1\{H((t-1)/k_1) - (1/2k_1)\log_2[8k_2((t-1)/k_1)((k_1-t+1)/k_1)]\}} \quad (10)$$

where $H(\cdot)$ denotes the binary entropy function. In addition, it is possible to show that

$$\lim_{s\to\infty} \frac{k_1\left\{H\left(\frac{t-1}{k_1}\right) - \frac{1}{2k_1}\log_2\left[8k_1\left(\frac{t-1}{k_1}\right)\left(\frac{k_1-t+1}{k_1}\right)\right]\right\}}{k_1 H\left(\frac{t-1}{k_1}\right)} = 1 - \frac{1}{2(t-1)} \quad (11)$$

$$\lim_{s\to\infty} \frac{k_1 H\left(\frac{t-1}{k_1}\right)}{(t-1)\log_2 k_1} = 1. \quad (12)$$

On the other hand,

$$k_1 H\left(\frac{t-1}{k_1}\right) > (t-1)\log_2 k_1 - (t-1)\log_2(t-1) \quad (13)$$

and

$$\lim_{s\to\infty} \frac{(t-1)\log_2 k_1}{(t-1)\log_2 k_1 + (t-1)\log_2(t-1)} = 1. \quad (14)$$

Using (11)–(14) in (10), and the inequality $(2^s - 1)^t > 2^{(s-1)t}$, we obtain

$$s(n-k) \gtrsim \left\lceil \log_2(n - k_1) + \left(1 - \frac{1}{2(t-1)}\right) \cdot [(t-1)\log_2 k_1 - (t-1)\log_2(t-1)] + (s-1)t \right\rceil \quad (15)$$

where $a(s) \sim b(s)$ [read $a(s)$ asymptotic to $b(s)$] means that

$$\lim_{s\to\infty} \frac{a(s)}{b(s)} = 1.$$

(Note that both n and k_1 grow exponentially with s.) In other words, the expression on the right-hand side (RHS) of (9) is asymptotic (after taking logarithm base 2) to the RHS of (15) and, at the same time, the RHS of (9) is greater than the RHS of (15).

TABLE I
SOME OPTIMAL $(t, 1)$-ERROR-CORRECTING CODES OVER $GF(2^s)$

s	l	n	k	k_1	$_2$	t
3	1	71	66	5	61	2
3	2	583	577	5	572	2
4	1	271	266	13	253	2
4	1	271	264	11	253	3
4	2	4367	4361	13	4348	2
4	2	4367	4359	11	4348	3
5	1	1055	1050	29	1021	2
5	1	1055	1048	27	1021	3
5	1	1055	1046	25	1021	4
6	1	4159	4152	59	4093	3
6	1	4159	4150	57	4093	4
6	1	4159	4148	55	4093	5

Inequality (15) can be rewritten as follows:

$$s(n-k) \gtrsim \lceil \log_2 n + (t - 3/2)\log_2 k_1 + st + \log_2(1 - k_1/n) - [(t - 3/2)\log_2(t-1) = t] \rceil. \quad (16)$$

Let $c(t) = (t - 3/2)\log_2(t-1) + t$, a constant that depends on t but not on s (and therefore not on n nor on k_1). Then, for large s, we have that

$$\frac{c(t)}{s} \approx 0.$$

In addition, we assume that $k_1 < cn$ where $0 \leq c \ll 1$. It follows from (16) that

$$(n-k) \gtrsim \left\lceil \frac{1}{s}[\log_2 n + (t - 3/2)\log_2 k_1] + t \right\rceil \quad (17)$$

which is the desired asymptotic Hamming lower bound on the number of redundant symbols of a linear $(t, 1)$-error-correcting code over $GF(2^s)$. For codes with parameters as those in (7) we have, for large s,

$$n \gtrsim 2^{s(2m+l-1)} \quad \text{and} \quad k_1 \gtrsim 2^{sm-1}. \quad (18)$$

Let $m = 1$. It follows from (17) and (18) that the number of redundant symbols has the following asymptotic Hamming lower bound

$$n - k \gtrsim \left\lceil 2t + l - \left(\frac{1}{2} + \frac{(t - 3/2)}{s}\right) \right\rceil.$$

This bound reduces to

$$n - k \gtrsim \lceil 2t + l \rceil$$

because $(t - 3/2)/s \approx 0$. Note that, for $m = 1$, LUEP codes of Theorem 3 have exactly $2t + l$ redundant symbols, and thus achieve the Hamming bound. We have shown that the LUEP codes obtained from Theorem 3 are optimal when their parity-check matrices are combinations of parity-check matrices of t-error correcting Reed–Solomon codes and parity-check matrices of shortened Hamming codes, both over the field $GF(2^s)$, for large s, $s \geq 3$.

In Table I we present a list of some optimal linear $(t, 1)$-error-correcting codes over $GF(2^s)$.

ACKNOWLEDGMENT

We would like to thank Dr. E. Bertram, Department of Mathematics, University of Hawaii, for many helpful discussions. We would also like to thank the referees for their comments.

REFERENCES

[1] I. Boyarinov and G. Katsman, "Linear unequal error protection codes," *IEEE Trans. Inform. Theory*, vol. IT-27, pp. 168–175, Mar. 1981.

[2] M. C. Lin and S. Lin, "Codes with multi-level error correcting capabilities," *Discrete Mathemat.*, vol. 83, pp. 301–314, 1990.

[3] W. W. Peterson and E. J. Weldon, *Error-Correcting Codes*. Cambridge, MA: M.I.T. Press, 1972.

The n-Dimensional Key Equation and a Decoding Application

Hervé Chabanne and Graham H. Norton

***Abstract*—We introduce the n-dimensional key equation, which exhibits the error-locator polynomial of an n-dimensional cyclic code as a product of n univariate polynomials and the error-evaluator polynomial as an n-variable polynomial. We then reinterpret these polynomials in the context of linear recurring sequences. In particular, we reduce the decoding problem to successive application of the Berlekamp–Massey algorithm. With this new method, we are able to decode (up to half their minimum distance) many codes in a table of 2-D cyclic codes due to Jensen.**

I. INTRODUCTION AND NOTATION

Let $n \geq 2$, K be a finite field and $K[\boldsymbol{X}] = K[X_1, \cdots, X_n]$. An n-dimensional (n-D) cyclic or abelian code is an ideal in the polynomial algebra $K[\boldsymbol{X}]/(X_1^{N_1} - 1, \cdots, X_n^{N_n} - 1)$. See [1]–[3] for details. We consider the problem of decoding these codes. Our approach is based on generalizing the key equation to n dimensions and successive application of the ordinary Berlekamp–Massey algorithm. We give several examples of our algorithm at work; all of the 2-D cyclic codes in Jensen's table [8], whose minimum distance does not exceed eight, can be decoded.

In more detail, let

$$e(\boldsymbol{X}) = \sum_{\boldsymbol{i} \in \mathrm{Supp}\,(e)} e_{\boldsymbol{i}} \boldsymbol{X}^{\boldsymbol{i}}$$

be a nonzero polynomial corresponding to a transmitted codeword where $\boldsymbol{i} = (i_1, \cdots, i_n)$, $\mathrm{Supp}\,(e) = \{\boldsymbol{i} \in \mathbb{N}^n \colon e_{\boldsymbol{i}} \neq 0\}$ and $\boldsymbol{X}^{\boldsymbol{i}} = X_1^{i_1} \cdots X_n^{i_n}$. Denote by L the smallest extension of K containing an N_k^{th} primitive root of unity α_k for $1 \leq k \leq n$. (We do not exclude the case $K = L$.) Our key equation has the form

$$(\sigma_1 \cdots \sigma_n) S_e(\boldsymbol{X}^{-1}) = \boldsymbol{X}\omega$$

where for $1 \leq k \leq n$, $\sigma_k \in L[X_k]$ is the monic "error-locator X_k-polynomial," $\omega \in L[\boldsymbol{X}]$ is the error-evaluator polynomial, and

$$S_e(\boldsymbol{X}^{-1}) = \sum_{\boldsymbol{i} \leq \boldsymbol{0}} e(\alpha^{-\boldsymbol{i}}) \boldsymbol{X}^{\boldsymbol{i}} \in L[[\boldsymbol{X}^{-1}]].$$

(By $\boldsymbol{i} = (i_1, \cdots, i_n) \leq \boldsymbol{j} = (j_1, \cdots, j_n)$, we mean $i_k \leq j_k$ for *all* k, $1 \leq k \leq n$; $\boldsymbol{i} \geq \boldsymbol{j}$ is synonymous with $\boldsymbol{j} \leq \boldsymbol{i}$. Also, we abbreviate $\alpha_1^{-i_1} \cdots \alpha_n^{-i_n}$ to $\alpha^{-\boldsymbol{i}}$.) When S_e and the σ_k are known, we can recover e from the spectral properties of the σ_k and ω (Theorem 2.4).

Let $\tilde{e}$ be the n-D linear recurring sequence (lrs) with generating function $S_e(\boldsymbol{X}^{-1})$, and let $\mathrm{Ann}\,(\tilde{e})$ be its characteristic ideal. We show that σ_k generates $\mathrm{Ann}\,(\tilde{e}) \cap L[X_k]$ for $1 \leq k \leq n$ and give two methods of computing the generators (Theorems 3.4, 3.6). Thus we can compute e when S_e is known (Algorithm 3.7).

The last section begins with an introductory example of "decoding by sections" (Algorithm 4.3) at work and continues with several 3-error-correcting 2-D cyclic codes from [8].

The problem of decoding 2-D cyclic codes has recently been considered in [13], using the 2-D Berlekamp–Massey algorithm of [12] and the non-trivial theory of Gröbner bases. In contrast, our approach is self-contained (apart from two results on n-D lrs) and as far as we know, is the only method which can decode the 3-error-correcting 2-D cyclic codes of [8].

Although Berman [1] has shown that abelian codes form a class of good codes, we are unaware of codes which are useful in applications *and* which are decodable by sections. Also, it would be interesting to know if our key equation can be solved using the XPRS algorithm of [5], [6] or by the 2-D Berlekamp–Massey algorithm.

A preliminary version of this paper appeared in [4]. We conclude with a short list of additional notation:

Notation	Meaning
$\mathbb{N}$	$\{0, 1, \cdots\}$
$L[\widehat{X_k}]$	$L[X_1, X_2, \cdots X_{k-1}, X_{k+1}, \cdots, X_n]$
$L((\boldsymbol{X}^{-1}))$	Laurent series in $\boldsymbol{X}^{-1}$ over L
$\boldsymbol{0}$	$(0, \cdots, 0)$
$\boldsymbol{1}$	$(1, \cdots, 1)$
$\boldsymbol{i}$	$(i_1, i_2, \cdots, i_n)$
$\pi_k(\boldsymbol{i})$	i_k
$\pi_{\hat{k}}(\boldsymbol{i})$	$(i_1, \cdots, i_{k-1}, i_{k+1}, \cdots, i_n)$
$\delta_k(p)$	the degree of $p \in L[\boldsymbol{X}]$ considered as a polynomial in X_k
$\delta(p)$	$(\delta_1 p, \cdots, \delta_n p)$

II. THE n-D KEY EQUATION

Our goal is to write the series $S = S_e$ described in the Introduction as a quotient of two relatively prime polynomials. We begin with an important expression for S.

Lemma 2.1:

$$S = \boldsymbol{X} \sum_{\boldsymbol{i} \in \mathrm{Supp}\,(e)} \left(\frac{e_{\boldsymbol{i}}}{\prod_{k=1}^n (X_k - \alpha_k^{i_k})} \right)$$

Proof: By expanding and rewriting S, we obtain $S = \sum_{\boldsymbol{i} \in \mathrm{Supp}\,(e)} e_{\boldsymbol{i}} (\sum_{\boldsymbol{j} \geq \boldsymbol{0}} (\alpha^{\boldsymbol{i}} \boldsymbol{X}^{-1})^{\boldsymbol{j}})$. An easy induction on n shows that $\sum_{\boldsymbol{j} \geq \boldsymbol{0}} (\alpha^{\boldsymbol{i}} \boldsymbol{X}^{-1})^{\boldsymbol{j}} = \prod_{k=1}^n (1 - \alpha_k^{i_k} X_k^{-1})^{-1}$, which yields the result. □

In n dimensions, we will need a product of univariate error-locator polynomials.

Manuscript received July 7, 1992; revised February 24, 1993. The work of G. H. Norton was supported by SERC under Grant GR/H15141. This paper was presented at the 1993 IEEE International Symposium on Information Theory, San Antonio, TX, January 17–22, 1993.

H. Chabanne is with Projet Codes, INRIA, Rocquencourt, B.P. 105, 78153 Le Chesnay Cedex, France.

G. H. Norton is with the Centre for Communications Research, University of Bristol, Bristol BS8 1TR, United Kingdom.

IEEE Log Number 9215097.

0018–9448/94$04.00 © 1994 IEEE