on the weights of various walks that avoid **0** in the state diagram. This is closely tied to the minimum weight to length ratio of cycles in the diagram, which is not obviously directly dependent on m. This observation should also be true about $\tau_{\min}$ in Hemmati and Costello [3], though $\tau_{\min}$ is of the order of four to six times m for the examples they consider. The fact that low weight cycles in the state diagram cause the requirement that the guard space be large is consistent with the fact that codes which are catastrophic have state diagrams which contain a nontrivial zero weight cycle.

Finally, we would like to observe that there are good reasons to view an error pattern as beginning as usual when the first incorrectly transmitted digit is received, but not ending until the decoder has returned to an e-ready state.

References

[1] J. B. Cain and G. C. Clark, "Some results on the error-propagation of convolutional feedback decoders," *IEEE Trans. Inform. Theory*, vol. IT-18, pp. 681–683, 1972.

[2] G. D. Forney, Jr., "Convolutional codes II: Maximum likelihood decoding," *Inform. Contr.*, vol. 25, pp. 222–266, 1974.

[3] F. Hemmati and D. J. Costello Jr., "Asymptotically catastrophic convolutional codes," *IEEE Trans. Inform. Theory*, vol. IT-26, pp. 298–304, 1980.

[4] F. Hemmati and D. J. Costello, Jr., "Truncation error probability in Viterbi decoding," *IEEE Trans. Commun.*, vol. COM-25, pp. 530–532, 1977.

[5] H. Kummer, "Recommendation for space data system standards: Telemetry channel coding: Issue-1," Consult. Comm. Space Data Syst., Sept. 1983.

[6] S. Lin and D. J. Costello, Jr., *Error Control Coding: Fundamentals and Applications*. Englewood Cliffs, NJ: Prentice Hall, 1983.

[7] J. L. Massey and R. W. Liu, "Application of Lyaponov's direct method to the error-propagation effect in convolution codes," *IEEE Trans. Inform. Theory*, vol. IT-10, pp. 248–250, 1964.

[8] J. L. Massey and M. K. Sain, "Inverses of linear sequential circuits," *IEEE Trans. Comput.*, vol. C-17, pp. 330–337, 1968.

[9] R. J. McEliece, *The Theory of Information and Coding, Encyclopedia of Matheamtics and its Applications*. Reading, MA: Addison-Wesley, 1977.

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

[11] J. P. Robinson, "Error propagation and definite decoding of convolutional codes," *IEEE Trans. Inform. Theory*, vol. IT-14, pp. 121–128, 1968.

[12] A. J. Viterbi and J. K. Omura, *Principles of Digital Communication and Coding*. New York: McGraw-Hill, 1979.

Comments on "Convergence and Performance Analysis of the Normalized LMS Algorithm with Uncorrelated Gaussian Data"

DENNIS R. MORGAN, MEMBER, IEEE

***Abstract*—Comments are expressed on the presentation of results in the paper by Tarrab and Feuer.**

In the above paper[1] a fine analysis is presented for the convergence and misadjustment of the NLMS algorithm. Unfortunately, the results and comparisons with the LMS algorithm are not in a form that readily enables the reader to draw practical conclusions. Plotting mean square error on a linear, instead of logarithmic (dB), scale hides the important detail of the error as it converges to its minimum value, which is exactly the region where the practical engineer requires detailed knowledge to assess performance. Moreover, in the comparison of the NLMS and LMS algorithm convergence rate and misadjustment, the practitioner wants to know how fast the algorithm will converge when the misadjustment is constrained to a specified value. It has been pointed out [1] that *comparison of convergence rates is meaningless without specifying the level of misadjustment*! Thus Figs. 5–8 are like comparing apples and oranges; one would have liked to know how the convergence compares with the *same misadjustment*. This simple but crucial point is far too often ignored.

References

[1] D. R. Morgan, "*Adaptive Signal Processing*, by B. Widrow and S. D. Stearns," *IEEE Trans. Acoust. Speech Signal Processing*, vol. ASSP-34, pp. 1017–1018, Aug. 1986.

Manuscript received November 28, 1988; revised February 24, 1989.

The author is with AT&T Bell Laboratories, Whippany, NJ 07981.

IEEE Log Number 8931669.

[1] M. Tarrab and A. Feuer, *IEEE Trans. Inform. Theory*, vol. IT-34, pp. 680–691, July 1988.

Optimal Codes for Minimax Criterion on Error Detection

M. G. KARPOVSKY, SENIOR MEMBER, IEEE, AND P. NAGVAJARA, MEMBER, IEEE

***Abstract*—Nonlinear quadratic codes are presented that are optimal for the minimax error detection. Characteristic functions for these codes are asymptotically bent. For a given block size n and the number of codewords $|C|$, these codes minimize $\max_{e\neq 0} Q(e)$ where $Q(e)$ is the conditional error-masking probability given the error pattern e. The codewords are blocks of n symbols from GF(q). We have the following parameters associated with the quadratic codes: $n = 2m$, $|C| = q^{2m-1} - q^{m-1}$, $\max_{e\neq 0} Q(e) = (q^{2m-2} + q^{m-1})|C|^{-1}$ and $\min_{e\neq 0} Q(e) = (q^{2m-2} - q^{m-1})|C|^{-1}$. Encoding and decoding procedures for these codes are described.**

I. Introduction

We present a construction for optimal error-detecting codes for the case where distributions of errors in the channel are not known or are difficult to model. A minimax criterion such that an error-detection capability for a code is optimized under the worst case scenario is the strategy taken for designing the codes. We will use the following probability as the measure for the error-detection capability of a code.

Let x denote a codeword and $\tilde{x}$ denote a received message. We define the conditional error-masking probability given error e ($e \neq 0$) for the code C as follows:

$$Q(e) = \frac{|\{(x, \tilde{x}) : \tilde{x} = x + e, x, \tilde{x} \in C\}|}{|C|}. \tag{1}$$

For a given number of codewords $|C|$ and a block size n our goal is to construct a code such that maxima of $Q(e)$ over all $e \neq 0$ are minimal. The problem can be formulated as follows. For a given code rate $R = n^{-1} \log_q |C|$ (codewords are blocks of q-ary symbols of length n), construct a code based on

Manuscript received March 11, 1988; revised February 21, 1989. This work was supported by the National Science Foundation under Grant MIP-881348.

The authors are with the Department of Electrical, Computer and System Engineering, 44 Cummington Street, Boston, MA 02215.

IEEE Log Number 8931671.

$\min_{C \in V^R} \max_{e \neq 0} Q(e)$, where V^R denotes the set of all codes with the rate R.

We note that a similar minimax criterion has been used in the design of match filters to combat jamming and other modeling uncertainties for communication channels [1]. This criterion can also be used for error detection in computation channels (VLSI chips), where the distribution of errors (errors are manifestations of physical failures at the outputs of the chip) is difficult to characterize [2], [3]. Hence the presented error-detecting codes are applicable for a design of fault-tolerant devices [4]. In the area of computer hardware testing, optimal compression of test responses based on the minimax approach were developed in [3].

The advantage of the proposed codes is related to the fact that for these codes, $\lim_{n \to \infty} Q(e) =$ constant for all $e \neq 0$. Thus these codes are useful for channels with unknown error distributions, since the total error-masking probability $Q_t = \sum_{e \neq 0} Q(e)P(e)$, is asymptotically independent of a distribution of errors $P(e)$ as the block size $n \to \infty$.

II. Lower Bound on Maxima of Conditional Error-Masking Probabilities

Theorem 1: Consider a code C defined in an n-dimensional space V_n over GF(q) where $q = p^s$ and p is a prime. The maxima of conditional error-masking probabilities (1) are lower-bounded by

$$\max_{e \neq 0} Q(e) \geq \begin{cases} \dfrac{2}{|C|}\left\lceil \dfrac{|C|(|C|-1)}{2(q^n-1)} \right\rceil, & p = 2 \\ \dfrac{1}{|C|}\left\lceil \dfrac{|C|(|C|-1)}{q^n-1} \right\rceil, & p > 2. \end{cases} \tag{2}$$

Proof: Let

$$B(e) = |\{x: x, x+e \in C\}| = \sum_x f(x)f(x+e),$$

$$f(x) = 1 \text{ iff } x \in C, f(x) \in \{0,1\}. \tag{3}$$

(Note that $B(e)$ is known as the autocorrelation function for the characteristic function $f(x)$ of the code C. These functions have been widely used in digital design [5], testing [3], and digital filtering [6].) Further,

$$\sum_{e \neq 0} B(e) = |C|(|C|-1). \tag{4}$$

Since, for $p = 2$, $B(e)$ is an even integer for any $e \neq 0$, we have

$$\max_{e \neq 0} B(e) \geq 2\left\lceil \frac{|C|(|C|-1)}{2(q^n-1)} \right\rceil \tag{5}$$

where $\lceil i \rceil$ is the smallest integer greater than or equal to i. Since $Q(e) = B(e)|C|^{-1}$, (2) follows immediately from (5) for $p = 2$. For p odd we have

$$\max_{e \neq 0} B(e) \geq \left\lceil \frac{|C|(|C|-1)}{(q^n-1)} \right\rceil, \text{ for } p > 2, \text{ Q.E.D.} \tag{6}$$

Note that, from (5) with $\max_{e \neq 0} B(e) = 2$, $p = 2$, we have

$$|C|(|C|-1) \leq 2(2^n-1). \tag{7}$$

We will construct below optimal codes satisfying (7) with $\max_{e \neq 0} Q(e) = 2|C|^{-1}$ and $|C| = 2^{n/2} - 1$.

A separate issue of maximizing $|C|$ for a given $\max_{e \neq 0} Q(e)$ is not considered in this correspondence. However, we point out that, if all values of $B(e)$, $e \neq 0$, are maxima (the characteristic function of the code is bent [7]), then, by (4), $|C|$ is maximized. In other words, an equal protection against all errors e ($Q(e)$ is constant, satisfying the equality in (2)) implies an efficient packing of information ($|C|$ is maximized).

III. Quadratic Codes

For a code C constructed by binary bent functions [5], [7]–[12], and defined as $(u, v) \in C$ if and only if $\langle u, v \rangle = \sigma$, $u, v \in V_m$ over GF(2), $\sigma \in$ GF(2), and $\langle u, v \rangle$ is the inner product over GF(2), the autocorrelation $B_\sigma(t, \tau)$ for the characteristic function $f_\sigma(u, v) = 1$ iff $\langle u, v \rangle = \sigma$, where $B_\sigma(t, \tau) = |\{(u, v): (u, v), (u + t, v + \tau) \in C\}|$, $e = (t, \tau)$, $t, \tau \in V_m$ over GF(2), is given by

$$B_\sigma(t, \tau) = \begin{cases} 2^{2m-1} + (-1)^\sigma 2^{m-1}, & (t, \tau) = 0 \\ 2^{2m-2} + (-1)^\sigma 2^{m-1}, & (t, \tau) \neq 0. \end{cases} \tag{8}$$

Unfortunately, these optimal codes based on bent functions and satisfying (2) for $p = 2$ have the property that their conditional error-masking probabilities $Q(t, \tau) = B_\sigma(t, \tau)\,|C|^{-1}$, $|C| = B_\sigma(0, 0)$, are asymptotically equal to 0.5 for all errors $e = (t, \tau) \neq 0$ as $n = 2ms \to \infty$.

We develop codes based on asymptotically bent binary functions. For these codes we can obtain $Q(t, \tau) \sim p^{-s}$, as $n \to \infty$ (p is prime) for any p and s.

Definition: Let $u, v \in V_m$ over GF(q), $q = p^s$; that is,

$$u = (u_0, \cdots, u_{m-1}),\ v = (v_0, \cdots, v_{m-1}),$$

where $u_i, v_i \in$ GF(q). For a given $\sigma \in$ GF(q) the quadratic code C over GF(q) with block size $n = 2m$ (q-ary symbols) is defined by

$$(u, v) \in C \text{ iff } \langle u, v \rangle = \sigma \tag{9}$$

where $\langle u, v \rangle = u_0 v_0 + \cdots + u_{m-1} v_{m-1}$, is the inner product in GF(q).

Codewords are all pairs (u, v) of vectors in V_m over GF(q) such that their inner product equal to a given (scalar) constant σ in GF(q).

Example 1: The quadratic code with the block size $n = 4$ and symbols from GF(2^2), with the syndrome $\sigma = 1$, is presented in Table I, where the following parameters apply:

- number of message symbols $k = 3$,
- block size $n = 4$ symbols from GF(2^2), $|C| = 60$,
- $(u_0, u_1, v_0, v_1) \in C \Leftrightarrow \langle (u_0, u_1), (v_0, v_1) \rangle = 1$,
- $(u_0, u_1), (v_0, v_1) \in V_2$ over GF(2^2),
- $u_i, v_i, 1 \in$ GF(2^2), (see Table II).

TABLE I
Example of a Quadratic Code

Messages			Codewords			
M_0	M_1	M_2	u_0	u_1	v_0	v_1
0	1	0	0	1	0	**1**
0	1	1	0	1	1	**1**
0	1	α	0	1	α	**1**
0	1	α^2	0	1	α^2	**1**
0	α	0	0	α	0	α^2
	⋮				⋮	
1	0	0	1	0	**1**	0
1	0	1	1	0	**1**	1
1	0	α	1	0	**1**	α
1	0	α^2	1	0	**1**	α^2
1	1	0	1	0	1	**1**
	⋮				⋮	
α^2	α^2	α	α^2	α^2	α	**0**
α^2	α^2	α^2	α^2	α^2	α^2	**1**

TABLE II
Elements of GF(2^2)

0	0	0
1	0	1
α	1	0
α^2	1	1

For a codeword (u_0, u_1, v_0, v_1), $u_i v_i \in \mathrm{GF}(2^2)$, v_1 is the redundant symbol if for the message (M_0, M_1, M_2), $M_1 \neq 0$, and v_0 is the redundant symbol if $M_1 = 0$, $M_0 \neq 0$. (In Table I, the redundant symbols are in boldface). (Note that $(M_0, M_1) = (u_0, u_1) \neq 0$, since $(u, v) \in C$ iff $\langle u, v \rangle = \sigma = 1$.)

As one can see from Example 1, quadratic codes are nonlinear and nonsystematic. For these codes, positions of redundant symbols depend on messages, but the number of redundant symbols is the same for any codeword. Procedures for encoding and decoding for quadratic codes will be presented in Section V.

The following theorems will show that quadratic codes are asymptotically optimal with respect to the lower bound (2) on maxima of $Q(e)$, as the block size $n \to \infty$, for a wide range of $|C|$.

Theorem 2: Let $(u, v) \in C$ iff $\langle u, v \rangle = \sigma$, $u, v \in V_m$ over $\mathrm{GF}(q)$, $m > 1$, $\sigma \in \mathrm{GF}(q)$, $q = p^s$. Then, C has the block size $2m$ q-ary ($2ms$ p-ary) symbols.

1) For $\sigma \neq 0$, $|C| = q^{2m-1} - q^{m-1}$, and we have for the probability of masking

$$Q(t, \tau) = \left(q^{2m-2} \pm q^{m-1}\right)|C|^{-1} = \left(q^{m-1} \pm 1\right)\left(q^m - 1\right)^{-1}, \quad \text{for any } (t, \tau) \neq 0, \quad (10)$$

where $t, \tau \in V_m$ over $\mathrm{GF}(q)$. Moreover, for $p = 2$ we have

$$Q(t, \tau) = \left(q^{m-1} + \mu(\sigma, T)\right)\left(q^m - 1\right)^{-1}, \quad \text{for any } (t, \tau) \neq 0 \quad (11)$$

where $t, \tau \in V_m$ over $\mathrm{GF}(2^s)$, $T = \langle t, \tau \rangle$ and $\mu(\sigma, T) = 1$ iff $\mathrm{tr}(\sigma T^{-1}) = 0$, $T \neq 0$, and $\mu(\sigma, T) = -1$ otherwise. ($\mathrm{tr}(\beta)$ denotes the trace of $\beta \in \mathrm{GF}(2^s)$ [7]).

2) For $\sigma = 0$, $|C| = q^{2m-1} - q^{m-1} + q^m$,

$$Q(t, \tau) = \left(q^{2m-2} + q^{m-1} + \delta_T (q-2) q^{m-1}\right)|C|^{-1}, \quad \text{for any } (t, \tau) \neq 0 \quad (12)$$

where $\delta_T = 1$ if $T = 0$ and $\delta_T = 0$ otherwise.

Our proof of Theorem 2 requires the following lemmas.

Lemma 1: Let θ be the number of solutions for the following system of two linear equations over $\mathrm{GF}(q)$

$$\langle a, x \rangle = i$$
$$\langle b, x \rangle = j - c \quad (13)$$

where a, b, and x belong to V_m over $\mathrm{GF}(q)$, $(m > 1)$, and $i, j, c \in \mathrm{GF}(q)$.

Then, for $\gamma \in \mathrm{GF}(q)$ (γ is a scalar constant),

$$\theta = \begin{cases} q^{m-2}, & b \neq \gamma a; \\ q^{m-1}, & b = \gamma a,\ c = j - \gamma i,\ a \neq 0; \\ 0, & b = \gamma a,\ c \neq j - \gamma i \text{ or } a = 0. \end{cases} \quad (14)$$

Proof: The system (13) of two linear equations over $\mathrm{GF}(q)$ has m variables $x = (x_0, \cdots, x_{m-1})$, $x_i \in \mathrm{GF}(q)$, and the number of solutions θ is given by (14) for the cases of the system being two linearly independent equations, or one linear equation, or an inconsistent system, according to the coefficients a, b, and constant c. Q.E.D.

Lemma 2 (Autocorrelation Functions for the Characteristic Functions of Quadratic Codes for $m > 1$): Let $B_\sigma(t, \tau) = |\{(u, v): (u, v), (u + t, v + \tau) \in C\}|$ where $(u, v) \in C$ iff $\langle u, v \rangle = \sigma$, $u, v, t, \tau \in V_m$ over $\mathrm{GF}(q)$, $m > 1$, and $\sigma \in \mathrm{GF}(q)$, $q = p^s$. Then $B_\sigma(t, \tau)$ is the number of solutions (u, v) of the following system of two quadratic equations over $\mathrm{GF}(q)$,

$$\langle u, v \rangle = \sigma$$
$$\langle (u + t), (v + \tau) \rangle = \sigma. \quad (15)$$

1) For $\sigma \neq 0$,

$$B_\sigma(t, \tau) = \begin{cases} q^{2m-1} - q^{m-1}, & t = \tau = 0 \\ q^{2m-2} \pm q^{m-1}, & \text{otherwise.} \end{cases} \quad (16)$$

Moreover, for $p = 2$

$$B_\sigma(t, \tau) = \begin{cases} q^{2m-1} - q^{m-1}, & t = \tau = 0 \\ q^{2m-2} + \mu(\sigma, T) q^{m-1}, & \text{otherwise,} \end{cases} \quad (17)$$

where

$$T = \langle t, \tau \rangle \qquad \mu(\sigma, T) = \begin{cases} 1, & \mathrm{tr}(\sigma T^{-1}) = 0,\ T \neq 0 \\ -1, & \text{otherwise,} \end{cases} \quad (18)$$

and $\mathrm{tr}(\alpha) = 1 + \alpha + \alpha^2 + \cdots + \alpha^{2^{s-1}}$, $\mathrm{tr}(\alpha) \in \mathrm{GF}(2)$.

2) For $\sigma = 0$,

$$B_\sigma(t, \tau) = \begin{cases} q^{2m-1} - q^{m-1} + q^m, & t = \tau = 0 \\ q^{2m-2} + q^{m-1} + \delta_T \cdot (q-2) q^{m-1}, & \text{otherwise.} \end{cases} \quad (19)$$

where $\delta_T \in \{0, 1\}$, $\delta_T = 1$ iff $T = 0$.

Proof: 1) For $t = \tau = 0$ the system of two quadratic equations (15) can be reduced to $\langle u, v \rangle = \sigma$. In this case for $\sigma \neq 0$ and any given $u \neq 0$, there exist q^{m-1} values of v satisfying $\langle u, v \rangle = \sigma$ and $B(0,0) = (q^m - 1) q^{m-1}$.

For $(t, \tau) \neq (0, 0)$ rewrite (15) in the form (13) given in Lemma 1,

$$\langle u, v \rangle = \sigma$$
$$\langle (u + t), v \rangle = \sigma - \langle (u + t), \tau \rangle. \quad (20)$$

From Lemma 1 for $x = v, a = u$, $b = u + t$, and $c = \langle (u + t), \tau \rangle$, $i = j = \sigma$, we have the following cases.

a) The system (20) consists of two linearly independent equations for any given $u \neq 0$ such that $u + t \neq \gamma u$ for any $\gamma \in \mathrm{GF}(q)$.

b) The system (20) is reduced to one linear equation for any $u \neq 0$ and there exists $\gamma \in \mathrm{GF}(q)$ such that

$$u + t = \gamma u \qquad \langle (u + t), \tau \rangle = \sigma(1 - \gamma). \quad (21)$$

From (21) we have $\sigma(\gamma - 1)^2 + \langle t, \tau \rangle (\gamma - 1) + \langle t, \tau \rangle = 0$, $\gamma \neq 1$, and for $p = 2$, γ exists iff $\mathrm{tr}(\sigma \langle t, \tau \rangle^{-1}) = 0$, $\langle t, \tau \rangle \neq 0$ [7].

c) If $u + t = \gamma u$, $\langle (u + t), \tau \rangle \neq \sigma(1 - \gamma)$ or $u = 0$, then (20) becomes an inconsistent system.

The above implies that there are $q^m - q$ fixations of u such that (20) consists of two linearly independent equations. If $u \neq 0$ satisfies (21) (for $p = 2$, $\mathrm{tr}(\langle t, \tau \rangle^{-1}) = 0$, $\langle t, \tau \rangle \neq 0$), then there are two fixations of u such that (20) is reduced to one linear equation.

2) Following the proof for the case of $\sigma \neq 0$, for $\sigma = 0$ and $t = \tau = 0$, $u = 0$ implies another q^m values of v satisfying (20). For $(t, \tau) \neq 0$, $\langle u, v \rangle = 0$, $\langle u + t, v + \tau \rangle = 0$, can be reduced to one linear equation if a) $u = 0$ or b) $u = -t$ or c) $u = \gamma t$ ($\gamma \neq 0, -1$) and $\langle t, \tau \rangle = T = 0$ since (20) becomes $\langle u, v \rangle = 0$ and $\langle t, v \rangle = -(\gamma - 1) T$. Hence $B_\sigma(t, \tau) = (q^m - q) q^{m-2} + 2q^{m-1} + \delta_T (q-2) q^{m-1}$. Q.E.D.

Proof of Theorem 2: Since $Q(t, \tau) = B_\sigma(t, \tau)|C|^{-1}$ and $|C| = B_\sigma(0, 0)$, (10) – (12) now follow from Lemma 2. Q.E.D.

Theorem 3: For $m=1$ and $\sigma \neq 0$, we have $(u,v) \in C$ iff $uv=\sigma$, $(u,v,\sigma \in \mathrm{GF}(q),\ q=p^s)$, and maxima of the conditional error-masking probabilities, $Q(t,\tau)$ are given by

$$\max_{(t,\tau)\neq 0} Q(t,\tau) = \frac{2}{q-1}. \tag{22}$$

For $p=2$, we have in this case optimal codes satisfying the lower bound (2) on maxima of $Q(t,\tau)$. For these codes,

$$B_\sigma(t,\tau) = \begin{cases} 2^s-1, & t=\tau=0 \\ 2, & \mathrm{tr}\left(\sigma(t\tau)^{-1}\right)=0,\ t\tau\neq 0 \\ 0, & \text{otherwise} \end{cases} \tag{23}$$

and for $(t,\tau)\neq 0$,

$$Q(t,\tau) = \begin{cases} 2(2^s-1)^{-1}, & \mathrm{tr}\left(\sigma(t\tau)^{-1}\right)=0,\ t\tau\neq 0 \\ 0, & \text{otherwise.} \end{cases} \tag{24}$$

Proof: From $uv=\sigma$ and $(u+t)(v+\tau)=\sigma$ we have $\tau u^2 + t\tau u + t\sigma = 0$, $u\neq 0$. Thus there exist at most two fixations of u such that an error (t,τ) is masked. Further, for $p=2$, (24) follows from the solvability condition for $\tau u^2 + t\tau u + t\sigma = 0$, $u\neq 0$ [7]. Q.E.D.

For codes constructed by Theorem 3, with $m=1$, the maxima of autocorrelation are equal to two, that is $\max_{e\neq 0} B_\sigma(e) = \max_{e\neq 0}\sum_x f_\sigma(x) f_\sigma(x+e) = 2$, where $e=(t,\tau)$, $x=(u,v)$, $f_\sigma(x) = 1$ iff $x\in C$, $(uv=\sigma)$.

The problem of constructing maximal codes for a given $\max_{e\neq 0} B_\sigma(e)$ is very difficult. We will show this for the case $\max_{e\neq 0} B_\sigma(e) = 2$. For a binary code C of length n containing $|C|$ codewords, we construct a linear code $V(C)$ such that nonzero codewords of C are columns of the check matrix for $V(C)$. Then $V(C)$ has codewords of length $|C|-1$ (we assume $0\in C$) and the number of check bits for $V(C)$ is equal to n. It is easy to show that $\max_{e\neq 0} B_\sigma(e) - 2$ for C iff $A_1 = A_2 = A_4 = 0$, where A_i is the number of codewords of weight i in $V(C)$. Thus the problem of constructing a code C with maximal $|C|$ and $\max_{e\neq 0} B_\sigma(e) = 2$ is equivalent to constructing a linear code $V(C)$ of the maximal length with a given number of check bits and $A_1 = A_2 = A_4 = 0$. This problem is very difficult. The problem of constructing double-error-correcting codes $(A_1 = A_2 = A_3 = A_4 = 0)$ of maximal length for a given number of check bits is still open [7].

We have presented quadratic codes with codewords being blocks of length $n=2m$ q-ary symbols and one redundant q-ary symbol. Quadratic codes are non-linear and nonsystematic codes (positions of redundant q-ary symbols depend on messages, see Example 1) with the transmission rate $n^{-1}\log_q|C|-1$ as $n\to\infty$, for $m>1$. From Theorem 2 one can readily see that as $n\to\infty$, we have for the conditional error-masking probabilities given error $(t,\tau)\neq 0$, $Q(t,\tau)\sim q^{-1}$ for $m>1$. Hence quadratic codes are asymptotically optimal providing an equal protection against all error patterns. In other words, characteristic functions of quadratic codes are asymptotically bent.

IV. Modified Codes

The quadratic codes developed in the previous section have limited numbers $|C|$ of codewords for a given block size $n=2ms$ symbols from $\mathrm{GF}(p)$ and the number of redundant symbols from $\mathrm{GF}(p)$, $r=s$. In this section we will develop modified quadratic codes with r redundant symbols such that $Q(t,\tau)\sim p^{-r}$, as $n\to\infty$, for any $r\leq s$. For the same block size as the original codes, modified codes will have more codewords (additional $s-r$ information symbols). However, this results in the increase in the conditional error-masking probability to $Q(t,\tau)\sim p^{-r}$.

Definition: Let C^* denote a modified quadratic code defined as a union of equivalent classes of V_{2m} over $\mathrm{GF}(p^s)$, $m>1$, partitioned by $\langle u,v\rangle = \sigma$, $\sigma\in\mathrm{GF}(p^s)$. For a given $\sigma^*\in V_r$ over $\mathrm{GF}(p)$,

$$(u,v)\in C^* \text{ iff } \langle u,v\rangle \in \Sigma, \tag{25}$$

where $\Sigma = \{\sigma:\ \sigma=(\nu,\sigma^*),\ \nu\in V_{s-r} \text{ over } \mathrm{GF}(p)\}$, $|\Sigma| = p^{s-r}$, and $u,v\in V_m$ over $\mathrm{GF}(p^s)$.

In other words,

$$\text{if } C_\sigma = \{(u,v):\langle u,v\rangle = \sigma\}, \text{ then } C^* = \bigcup_{\sigma\in\Sigma} C_\sigma. \tag{26}$$

Theorem 4: Consider modified quadratic codes C^* with codewords length $n=2m$ of symbols from $\mathrm{GF}(q)$, $q=p^s$, $m>1$, defined by (25), (26). We have for $\sigma^*\neq 0$, $|C^*| = p^{2ms-r} - p^{ms-r}$, and for $\sigma^*\neq 0$, $|C^*| = p^{2ms-r} - p^{ms-r} + p^{ms}$. Moreover, the conditional error-masking probability $Q^*(t,\tau) \triangleq B^*(t,\tau)|C^*|^{-1}$ (where $B^*(t,\tau)$ denotes the autocorrelation function for the characteristic function of C^*), is asymptotically equal to p^{-r} for any $(t,\tau)\neq 0$ as $n\to\infty$.

The following lemma will be used in the proof of Theorem 4.

Lemma 3: Let C^* be a code defined for a given $\sigma^*\in V_r$ over $\mathrm{GF}(p)$ by $(u,v)\in C^*$ iff $\langle u,v\rangle\in\Sigma$, where $u,v\in V_m$ over $\mathrm{GF}(p^s)$, provided that $m>1$, $\Sigma=\{\sigma:\ \sigma=(\nu,\sigma^*),\ \nu\in V_{s-r},\ \sigma^*\in V_r,\ \text{over } \mathrm{GF}(p)\}$. Then for a given $\sigma^*\neq 0$, the conditional error-masking probability $Q^*(t,\tau)$, $(t,\tau)\neq 0$, for C^* is bounded by

$$\frac{p^{2ms-2r} - p^{s-r}p^{ms-r}}{p^{2ms-r} - p^{ms-r}} \leq Q^*(t,\tau) \leq \frac{p^{2ms-2r} + p^{s-r}p^{ms-r}}{p^{2ms-r} - p^{ms-r}}. \tag{27}$$

Proof: 1) By definition $Q^*(t,\tau) = B^*(t,\tau)/B^*(0,0)$. $B^*(t,\tau) = |\{(u,v):\ (u,v),(u+t,v+\tau)\in C^*\}|$ is the number of solutions of the following system of two quadratic equations over $\mathrm{GF}(q)$, $q=p^s$

$$\begin{aligned} \langle u,v\rangle &= i \\ \langle (u+t),(v+\tau)\rangle &= j,\ i,j\in\Sigma; \end{aligned} \tag{28}$$

that is, $B^*(t,\tau)$ is the number of $(u,v)\in C^*$ such that there exists $j\in\Sigma$ satisfying $\langle (u+t),(v+\tau)\rangle = j$.

2) $B^*(0,0) = (q^m-1)q^{m-1}p^{s-r} = p^{2ms-r} - p^{ms-r}$, since for any $u\neq 0$ there exists $q^{m-1}p^{s-r}$ values of v satisfying $\langle u,v\rangle\in\Sigma$, $|\Sigma| = p^{s-r}$.

3) Rewrite (28) in the form given in Lemma 1 $(v=x,\ u=a,\ u+t=b,\ c=\langle (u+t),\tau\rangle)$:

$$\begin{aligned} \langle u,v\rangle &= i \\ \langle (u+t),v\rangle &= j - \langle (u+t),\tau\rangle, \qquad i,j\in\Sigma. \end{aligned} \tag{29}$$

There are q fixations of u satisfying the condition $u+t=\gamma u$, for some $\gamma\in\mathrm{GF}(q)$. The system becomes inconsistent iff $\langle (u+t),\tau\rangle \neq j - i\gamma$, or one linear equation iff $\langle (u+t),\tau\rangle = j - i\gamma$. From $u+t=\gamma u$, $\langle (u+t),\tau\rangle = j - i\gamma$ we have

$$i\gamma^2 - (i+j-T)\gamma + j = 0, \qquad \gamma\neq 1, \qquad T = \langle t,\tau\rangle. \tag{30}$$

The lower bound on $Q^*(t,\tau)$ is obtained by assuming that, for some T there is no solution γ satisfying (30) for any $i,j\in\Sigma$. Hence $B^*(t,\tau)\geq (q^m-q)q^{m-2}|\Sigma|^2$. The upper bound on $Q^*(t,\tau)$ is obtained by assuming that, for some T there are two solutions γ, satisfying (30) for any $i,j\in\Sigma$. Hence $B^*(t,\tau)\leq (q^m-q)q^{m-2}|\Sigma|^2 + 2q^{m-1}|\Sigma|^2$. Q.E.D.

We note, that as in the case of nonmodified codes C, for modified codes C^* conditional error-masking probabilities $Q^*(t,\tau)$ depend only on $T=\langle t,\tau\rangle$.

Proof of Theorem 4: For the case $\sigma^*\neq 0$, we have $Q^*(t,\tau)\sim p^{-r}$ which is readily seen from Lemma 3. For the case $\sigma^*=0$, we have $0\in\Sigma$ and $|C^*|=(p^{s-r}-1)(q^{2m-1}-q^{m-1})+(q^{2m-1}-q^{m-1}+q^m)$, since C^* is a union of $p^{s-r}-1$ nonmodified codes with $\sigma\neq 0$ and one nonmodified code with $\sigma=0$. To show that $Q^*(t,\tau)\sim p^{-r}$ for $\sigma^*=0$, we observe that the main term p^{2ms-2r} still appears in the expression for $B^*(t,\tau)$. Indeed, out of q^m possible fixations of u only q fixations make the system $\langle u,v\rangle=i$ and $\langle (u+t),(v+\tau)\rangle=j$ linearly dependent. (These u are solutions of $u=\gamma(u+t)$ for any given γ). Hence, $B^*(t,\tau)$ contains the term $(q^m-q)q^{m-2}|\Sigma|^2=p^{2ms-2r}-p^{m(s+1)-2r}$. Q.E.D.

It can be easily shown that for $p-2$ and $r=1$, $f(u,v)=1$ iff $\langle u,v\rangle=\sigma$, $\sigma\in\Sigma$, the characteristic function of the code, $f(u,v)$, is a bent function.

Theorem 5: For $m=1$ and $\sigma^*\neq 0$ we have for modified codes

$$Q^*(t,\tau)\le 2p^{2s-2r}|C^*|^{-1},\ |C^*|=p^{2s-r}-p^{s-r}. \qquad (31)$$

Proof: Since C^* is a union of $C_\sigma=\{uv:\ uv=\sigma\}$ for all $\sigma\in\Sigma$, for $m=1$ and $\sigma^*\neq 0$ we have $|C^*|=(q-1)p^{s-r}$, $|\Sigma|=p^{s-r}$. From $uv=i$ and $(u+t)(v+\tau)=j$, $i,j\in\Sigma$, $0\notin\Sigma$, we have, $\tau u^2+(t\tau+i-j)u+ti=0$. The upper bound (31) is obtained by assuming the existence of two solutions, $u\neq 0$, for any $i,j\in\Sigma$. Q.E.D.

Modified quadratic codes C^* were shown in Theorem 4 (for the case $m>1$) to be asymptotically optimal; that is, characteristic functions of modified codes are asymptotically bent. Codewords of C^* are blocks of $n=2ms$ p-ary symbols ($q=p^s$) where the number of redundant p-ary symbols $r\le s$. The number of codewords in C^* can be readily obtained from the number of codewords in the nonmodified codes C, that is, $|C^*|=|C|p^{s-r}$, since C^* is a union of disjoint $C_\sigma=\{\langle u,v\rangle=\sigma\}$, $\sigma\in\Sigma$, where $\Sigma=\{\sigma:\ \sigma=(\nu,\sigma^*),\ r\le s,\ \nu\in V_{s-r},\ \sigma^*\in V_r,\ \text{over GF}(p)\}$, $|\Sigma|=p^{s-r}$. For the case $m=1$ and $\sigma^*\neq 0$ as $n\to\infty$, $n=2s$ p-ary symbols and from (31) we have $Q^*(t,\tau)\lesssim 2p^{-r}$, $r\le s$. Moreover, for $p=2$, $m=1$ and $r=1$ the characteristic function of C^* is bent.

V. Encoding and Decoding Procedures for Quadratic Codes

In presenting encoding and decoding procedures for quadratic codes, without loss of generality, we consider only the case of nonmodified and modified codes over GF(2^s) and describe the encoding and decoding procedures by means of the following example.

Example 2: Let $C=\{(u,v):\ \langle u,v\rangle=1\}$, $u,v\in V_4$ over GF(2^4), $1\in$ GF(2^4), $(u,v)=(u_3,u_2,u_2,u_1,u_0,v_3,v_2,v_1,v_0)\in C$ iff $u_3v_3+u_2v_2+u_1v_1+u_0v_0=1$, where addition and multiplication are defined in GF(2^4).

Encoding: Let the message be denoted by $M=(M_0,M_1,M_2,M_3,M_4,M_5,M_6)$, $M_i\in GF(2^4)$. If $M_0\neq 0$, the redundant symbol ρ can be obtained by letting $M_i=u_i$, $i=0,1,2,3$, $M_i=v_{i-3}$, $i=4,5,6$, and $v_0=\rho=(1+u_1v_1+u_2v_2+u_3v_3)u_0^{-1}$. If $M_0=0$, $M_1\neq 0$, we let $M_4=v_0$, $M_5=v_2$, $M_6=v_3$, and $V_1=\rho=(1+u_2v_2+u_3v_3)u_1^{-1}$. If $M_0=M_1=0$, $M_2\neq 0$, then $v_2=\rho=(1+u_3v_3)u_2^{-1}$. Last, if $M_0=M_1=M_2=0$, $M_3\neq 0$, then $V_3=\rho=u_3^{-1}$. Several examples of messages and the corresponding codewords are given in Table III. The redundant symbols in the codewords shown in Table III are in boldface. (In this example GF(2^4) is constructed by x^4+x+1 over GF(2)).

TABLE III
Examples Describing Encoding Procedure

Messages							Codewords							
M_0	M_1	M_2	M_3	M_4	M_5	M_6	u_0	u_1	u_2	u_3	v_0	v_1	v_2	v_3
α	1	α^{12}	α^5	α^3	0	α^7	α	1	α^{12}	α^5	α^{10}	α^3	0	α^7
α^3	0	α^{10}	α^{12}	α^8	α^9	α^{10}	α^3	0	α^{10}	α^{12}	α^{11}	α^8	α^9	α^{10}
0	α	α^2	0	α^4	α^5	α^6	0	α	α^2	0	α^4	α^8	α^5	α^6
0	0	α^{11}	α^{14}	α^2	α^{13}	α	0	0	α^{11}	α^{14}	α^2	α^{13}	**0**	α
0	0	0	α^8	α	α^7	1	0	0	0	α^8	α	α^7	1	α^7

Next, we consider an example of an encoding procedure for modified codes. Let $r=2$; then a message consists of seven GF(2^4) symbols and the new additional two bits ($s-r=2$) are denoted by $\nu_0,\nu_1\in$ GF(2). Consider, the modified code defined by $C^*=\{(u,v):\ \langle u,v\rangle=(\nu_0,\nu_1,0,1)\}$, $\sigma^*=(0,1)$. The encoding procedure is the same as for the nonmodified code described earlier except the redundant symbol ρ is computed based on $\langle u,v\rangle=(\nu_0,\nu_1,0,1)$. For example, let $M=(\alpha,\alpha^{14},0,\alpha^5,\alpha^9,\alpha^2,1)$ and $\nu_0=1$, $\nu_1=1$, $(\nu_0,\nu_1\in$ GF(2)). Since $M_0=u_0=\alpha\neq 0$, we have $v_0=\rho=[\alpha^{13}+(\alpha^{23}+0+\alpha^5)]\alpha^{-1}=\alpha^{10}$, $\alpha^{13}=(1,1,0,1)=(\nu,\sigma^*)$, and the encoded message is $(u,v)=(\alpha,\alpha^{14},0,\alpha^5,\alpha^{10},\alpha^9,\alpha^2,1)$.

Decoding: First the decoder checks whether the received codeword $(\tilde u,\tilde v)$ satisfies $\langle\tilde u,\tilde v\rangle=\sigma$ for the nonmodified codes, or $\langle\tilde u,\tilde v\rangle\in\Sigma$ for modified codes. If errors are detected ($\langle\tilde u,\tilde v\rangle\neq\sigma$ or $\langle\tilde u,\tilde v\rangle\notin\Sigma$), the decoder requests the retransmission of the message. If no errors are detected, the decoder identifies the redundant symbol using the following rule: if i is the smallest integer such that $u_i\neq 0$, the redundant symbol is v_i. For our example of the modified code given above, let $(\tilde u,\tilde v)=(\alpha,\alpha^{14},0,\alpha^5,\alpha^{10},\alpha^9,\alpha^2,1)$, the decoder checks that $\langle\tilde u,\tilde v\rangle=\alpha^{11}+\alpha^{23}+0+\alpha^5=\alpha^{13}=(1,1,0,1)$, $\sigma^*=(0,1)$, and errors are not detected. Moreover, the message is $(\alpha,\alpha^{14},0,\alpha^5,\alpha^9,\alpha^2,1)$ and $(\nu_0,\nu_1)=(1,1)$, $\nu_0,\nu_1\in$ GF(2).

VI. Conclusion

Quadratic codes are asymptotically optimal (as $n\to\infty$) with respect to the lower bound on the maxima of the conditional error-masking probability. In other words, these codes provide for an equal protection against all error patterns (characteristic functions of these codes are asymptotically bent), and total error-masking probabilities are independent of the distribution of errors in the channel. We presented quadratic codes for a wide range of numbers of codewords and values of error-masking probabilities. A table of error-masking probabilities attained by quadratic codes for block size $n=4,\cdots,16$ can be found in the Appendix.

Acknowledgment

The authors would like to thank Professor Lev B. Levitin of Boston University, Boston, MA, for many helpful discussions.

APPENDIX
TABLE OF QUADRATIC CODES

Table IV is the table of quadratic codes, both nonmodified (NM) and modified (M), with minimal $\max_{e\neq 0} Q(e)$, for $p=2$, and block sizes $n=4, 6, 8, 12, 14$, and 16 bits and the lower bound on $\max_{e\neq 0} Q(e)$ for given n and $|C|$ constructed by Theorem 1. The table also includes 1) complemented codes $\bar{C}$ having characteristic functions $f_{\bar{C}}(x)=1-f_C(x)$ where $f_C(x)$ is the characteristic function of a quadratic code C (the conditional error-masking probability for $\bar{C}$ is given by $Q_{\bar{C}}(e)=1-(|C|-B(e))(q^n-|C|)^{-1}$; note that C is optimal iff $\bar{C}$ is optimal); 2) the nonmodified codes with the codeword of all zeros added.

TABLE IV
QUADRATIC CODES

				Maximum Probability of Masking		
	$\|C\|$	m	s	Lower Bound	Upper Bound	Remarks
$n=4$	6	2	1	0.3333	0.3333	bent $\sigma\neq 0$, optimal
	5	2	1	0.4000	0.4000	$\bar{C}$, optimal
	7	2	1	0.2857	0.5714	$\hat{C}$
	9	1	2	0.6666	0.6666	$\bar{C}$, optimal
	10	2	1	0.6000	0.6000	bent $\sigma=0$, optimal
	11	2	1	0.7272	0.7272	$\hat{\bar{C}}$, optimal
	13	1	2	0.9231	0.9231	$\bar{C}$, optimal
$n=6$	8	1	3	0.2500	0.2500	$\hat{\bar{C}}$, optimal
	27	3	1	0.4444	0.4444	$\bar{C}$, optimal
	28	3	1	0.4286	0.4286	bent $\sigma\neq 0$, optimal
	29	3	1	0.5000	0.5000	$\hat{C}$, optimal
	36	3	1	0.5555	0.5555	bent $\sigma=0$, optimal
	35	3	1	0.5714	0.5714	$\bar{C}$, optimal
	37	3	1	0.5946	0.5946	$\hat{\bar{C}}$, optimal
	42	1	3	0.6666	0.7143	$\bar{C}$
	49	1	3	0.7755	0.8571	$\bar{C}$
	50	1	3	0.8000	0.8400	$\bar{C}$
	56	1	3	0.8928	0.8928	$\bar{C}$, optimal
	57	1	3	0.9123	0.9123	$\bar{C}$, optimal
$n=8$	15	1	4	0.1333	0.1333	NM $\sigma\neq 0$, optimal
	30	1	4	0.1333	0.2666	M $\sigma\neq 0$
	46	1	4	0.2174	0.3913	M $\sigma=0$
	60	2	2	0.2333	0.3333	NM $\sigma\neq 0$
	76	1	4	0.3158	0.3684	M $\sigma=0$
	120	4	1	0.4667	0.4667	bent $\sigma\neq 0$, optimal
	136	4	1	0.5294	0.5294	bent $\sigma=0$, optimal
	180	1	4	0.7111	0.7333	$\bar{C}$
	196	2	2	0.7653	0.7959	$\bar{C}$
	210	1	4	0.8286	0.8666	$\bar{C}$
	226	1	4	0.8850	0.9026	$\bar{C}$
	241	1	4	0.9460	0.9460	$\bar{C}$, optimal
$n=10$	32	1	5	0.0625	0.0625	$\hat{C}$, optimal
	62	1	5	0.0645	0.1290	M $\sigma\neq 0$
	124	1	5	0.0645	0.2258	M $\sigma\neq 0$
	156	1	5	0.1538	0.2820	M $\sigma=0$
	248	1	5	0.2419	0.2903	M $\sigma\neq 0$
	280	1	5	0.2786	0.3143	M $\sigma=0$
	496	1	5	0.4839	0.4839	bent $\sigma\neq 0$, optimal
	528	1	5	0.5151	0.5151	bent $\sigma=0$, optimal
	744	1	5	0.7285	0.7419	$\bar{C}$
	775	1	5	0.7587	0.7716	$\bar{C}$
	776	1	5	0.7577	0.7732	$\bar{C}$
	868	1	5	0.8479	0.8710	$\bar{C}$
	900	1	5	0.8800	0.8933	$\bar{C}$
	962	1	5	0.9397	0.9439	$\bar{C}$
	992	1	5	0.9698	0.9698	$\bar{C}$, optimal
	993	1	5	0.9707	0.9707	$\bar{C}$, optimal
$n=12$	63	1	6	0.0317	0.0317	NM $\sigma\neq 0$, optimal
	126	1	6	0.0317	0.0635	M $\sigma\neq 0$
	252	1	6	0.0635	0.0952	M $\sigma\neq 0$
	505	2	3	0.1228	0.1426	$\hat{C}$
	568	2	3	0.1408	0.2113	NM $\sigma=0$
	1008	2	3	0.2460	0.2698	M $\sigma\neq 0$
	1072	2	3	0.2631	0.2836	M $\sigma=0$
	2016	3	1	0.4921	0.4921	bent $\sigma\neq 0$, optimal
	2080	3	1	0.5077	0.5077	bent $\sigma=0$, optimal

TABLE IV
CONTINUED

				Maximum Probability of Masking		
	$\|C\|$	m	s	Lower Bound	Upper Bound	Remarks
	3024	2	3	0.7388	0.7460	$\bar{C}$
	3088	2	3	0.7539	0.7617	$\bar{C}$
	3528	2	3	0.8617	0.8730	$\bar{C}$
	3591	2	3	0.8772	0.8794	$\bar{C}$
	3844	1	6	0.9386	0.9407	$\bar{C}$
	3970	1	6	0.9693	0.9703	$\bar{C}$
	4033	1	6	0.9849	0.9849	$\bar{C}$, optimal
$n=14$	128	1	7	0.0156	0.0156	$\hat{C}$, optimal
	254	1	7	0.0157	0.0315	M $\sigma\neq 0$
	508	1	7	0.0315	0.0551	M $\sigma\neq 0$
	1016	1	7	0.0623	0.0756	M $\sigma\neq 0$
	2032	1	7	0.1240	0.1496	M $\sigma\neq 0$
	2160	1	7	0.1324	0.1704	M $\sigma=0$
	4064	1	7	0.2480	0.2598	M $\sigma\neq 0$
	4192	1	7	0.2562	0.2672	M $\sigma=0$
	8128	1	7	0.4961	0.4961	bent $\sigma\neq 0$, optimal
	8256	1	7	0.5039	0.5039	bent $\sigma=0$, optimal
	12192	1	7	0.7443	0.7480	$\bar{C}$
	12320	1	7	0.7520	0.7558	$\bar{C}$
	14224	1	7	0.8683	0.8740	$\bar{C}$
	14352	1	7	0.8760	0.8800	$\bar{C}$
	15368	1	7	0.9381	0.9391	$\bar{C}$
	15876	1	7	0.9690	0.9698	$\bar{C}$
	16130	1	7	0.9845	0.9847	$\bar{C}$
	16256	1	7	0.9922	0.9922	$\bar{C}$, optimal
	16257	1	7	0.9923	0.9923	$\bar{C}$, optimal
$n=16$	255	1	8	0.0078	0.0078	NM $\sigma\neq 0$, optimal
	510	1	8	0.0078	0.0157	M $\sigma\neq 0$
	1020	1	8	0.0157	0.0274	M $\sigma\neq 0$
	2040	1	8	0.0314	0.0431	M $\sigma\neq 0$
	4080	2	4	0.0622	0.0667	NM $\sigma\neq 0$
	4336	2	4	0.0664	0.1144	NM $\sigma=0$
	8160	2	4	0.1245	0.1333	M $\sigma\neq 0$
	8416	2	4	0.1286	0.1483	M $\sigma=0$
	16320	4	2	0.2490	0.2549	NM $\sigma\neq 0$
	16576	4	2	0.2530	0.2587	NM $\sigma=0$
	32640	8	1	0.4980	0.4980	bent $\sigma\neq 0$, optimal
	32896	8	1	0.5019	0.5019	bent $\sigma=0$, optimal
	48960	4	2	0.7471	0.7490	$\bar{C}$
	49216	4	2	0.7510	0.7529	$\bar{C}$
	57120	2	4	0.8716	0.8751	$\bar{C}$
	57376	2	4	0.8755	0.8767	$\bar{C}$
	61200	2	4	0.9338	0.9372	$\bar{C}$
	61456	2	4	0.9377	0.9380	$\bar{C}$
	63496	1	8	0.9686	0.9693	$\bar{C}$
	64516	1	8	0.9844	0.9846	$\bar{C}$
	65026	1	8	0.9922	0.9923	$\bar{C}$
	65281	1	8	0.9961	0.9961	$\bar{C}$, optimal

For $0\notin C$ denote $\hat{C}=C\cup 0$. Let $B_{\hat{C}}(e)$ and $B_C(e)$ be the autocorrelation functions for the characteristic functions $f_{\hat{C}}$ and f_C of $\hat{C}$ and C, respectively. Since $f_{\hat{C}}(x)=f_C(x)+\delta_x$, where $\delta_x=1$ if $x=0$ and $\delta_x=0$, otherwise, we have

$$B_{\hat{C}}(e)=\sum_x f_{\hat{C}}(x)f_{\hat{C}}(x+e)=B_C(e)+2f_C(e). \tag{32}$$

Moreover, $e=(t,\tau)\in C$ iff $\langle t,\tau\rangle=\sigma$. If s is odd, then for $(t,\tau)\in C$, $\mathrm{tr}\,(\sigma\langle t,\tau\rangle^{-1})=\mathrm{tr}\,(1)=1$ and by (17), $\max_{e\neq 0} B_{\hat{C}}(e)=\max_{e\neq 0} B_C(e)$.

REFERENCES

[1] S. Verdu and V. H. Poor, "Minimax robust discrete-time matched filters," *IEEE Trans. Commun.*, vol. COM-31, pp. 208–216, Feb. 1983.

[2] J. E. Smith, "Measure of effectiveness of fault signature analysis," *IEEE Trans. Comput.*, vol. C-30, pp. 510–514, Jun. 1980.

[3] M. G. Karpovsky and P. Nagvajara, "Optimal time and space compression for VLSI devices," in *Proc. IEEE Int. Test Conf.*, 1987, pp. 523–529.

[4] D. K. Pradhan, Ed., *Fault-Tolerant Computing: Theory and Techniques*, vols. 1 and 2. Englewood Cliffs, NJ: Prentice-Hall, 1986.

[5] M. G. Karpovsky, *Finite Orthogonal Series in The Design of Digital Devices*. New York: Wiley, 1976.
[6] M. G. Karpovsky and L. A. Tractenberg, "Statistical and computational performances of Wiener filters," *IEEE Trans. Information Theory*, vol. IT-32, no. 2, pp. 303–307, Mar. 1986.
[7] F. J. McWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1978.
[8] O. S. Rothaus, "On 'bent' functions," *J. Comb. Theory*, ser. A20, pp. 300–305, 1976.
[9] R. L. McFarland, "A family of difference sets in non-cyclic groups," *J. Comb. Theory*, ser. A15, pp. 1–10, 1976.
[10] J. D. Olsen, R. A. Scholtz, and L. R. Welch, "Bent-function sequences," *IEEE Trans. Inform. Theory*, vol. IT-28, no. 6, pp. 858–864, Nov. 1982.
[11] A. Lempel and M. Cohn, "Maximal families of bent sequences," *IEEE Trans. Inform. Theory*, vol. IT-28, no. 6, pp. 865–868, Nov. 1982.
[12] A. Lempel and M. Cohn, "Design of universal test sequences for VLSI," *IEEE Trans. Inform. Theory*, vol. IT-31, pp. 10–17, Jan. 1985.

The Construction of Some Bit and Byte Error Control Codes Using Partial Steiner Systems

W. EDWIN CLARK, LARRY A. DUNNING, MEMBER, IEEE, AND D. G. ROGERS

***Abstract*—A design theoretic approach to binary linear codes that are single-error-correcting (SEC) and double-error-detecting (DED) with the capability of detecting any error within a single byte (BED) of even width w is developed. A construction of SEC–BED–DED codes from ordinary binary linear codes utilizing partial Steiner systems is given. The construction produces some codes with higher rates than known previously. The codes constructed may inherit special properties from the Steiner systems they are derived from. In particular, some rotational odd-weight-column codes are obtained.**

I. Introduction

We consider binary linear codes of length n and redundancy r in which the codewords are partitioned into m consecutive bytes of width w. Such a code is *single-error-correcting* (SEC) if any single bit error can be corrected, *double-error-detecting* (DED) if any error pattern of up to two bit errors can be detected, and *byte-error-detecting* (BED) if any pattern of bit errors confined to a single byte can be detected. Several authors [1], [2], [4], [5], [9], [10], [13] have constructed SEC–BED–DED codes, i.e., codes that are simultaneously SEC, BED, and DED.

Codes providing a combination of byte and random error protection can be used for error correction, error detection or a combination of the two. As with codes for ordinary random errors, this trade-off exists even when the code to be used is fixed. For example, a SEC–BED–DED code could also be used to detect error patterns consisting of three random errors and error patterns consisting of a single byte error together with a single random error. The *minimum distance profile* as defined in [12], [14] measures the error protection capability of a code providing a combination of byte and random error protection independently of whether the code is used for correction or detection. The minimum distance profile can be regarded as the analog of minimum distance for codes providing byte and random error protection. We shall not need to employ the minimum distance profile in this work. The definition of minimum distance profile of a code and the details of its relation to combinations of levels of error correction and error detection available when using that code can be found in van Gils and Boly [14]. For those who may wish to consult this reference, we note that the minimum distance profile of a SEC–BED code is (3,2) and that the minimum distance profile of a SEC–BED–DED code is (4,2).

In this correspondence we adopt a design-theoretic approach to SEC–BED–DED codes with even byte width w by focusing on the syndromes of error patterns of weight $w-1$ confined to a single byte and showing that, through a matrix of these syndromes, we can obtain a partial Steiner system (Theorem 1). In the opposite direction, we show that, starting from a matrix of potential syndromes and a partial Steiner system with appropriate properties, we may construct a SEC–BED–DED code (Theorem 2). From these results we obtain the codes with the improved rates shown in Table I.

TABLE I
COMPARISON OF SEC–BED–DED CODES

w	r	v	m	m^*
4	7	8	$14^{(\alpha)}$	12
4	12	24	$498^{(\beta)}$	496
6	11	12	$132^{(\gamma)}$	75
8	15	16	≥ 1164	567
10	14	14	91	84
10	15	15	≥ 222	180
10	16	16	≥ 592	372
10	17	17	≥ 1320	756
10	18	18	≥ 2760	1524
10	19	20	≥ 10536	3060
12	16	16	140	98
12	17	17	≥ 424	210
12	18	18	≥ 1260	434
12	19	19	≥ 3024	882
12	20	20	≥ 7112	1778
12	21	21	≥ 15143	3570
12	22	22	≥ 32442	7154
12	23	24	≥ 124052	4322
≥ 18	$w+3$	$w+3$	$A(v,4,w)^{(\delta)}$	$m^* < m$
≥ 12	$2w-1 > r = v \geq w+4$		$A(v,4,w)^{(\delta)}$	$m^* < m$
≥ 8	$2w-1$	$2w$	$A(v,4,w)^{(\delta)}$	$2m^* < m$
6	>11		$2^a \cdot 132^{(\epsilon)}$	$1.65m^* < m$
≥ 8	$> 2w-1$		$2^a A(2w,4,w)^{(\epsilon)}$	$2m^* < m$

w Byte width (always even).
r Redundancy.
v Number of byte syndromes of weight $w-1$.
m Code length in bytes $= A(v,4,w)$ except (ϵ).
m^* Longest previously known length in bytes.
a $r-2w+1$, check bits added by Theorem 4.

Properties of the ingredients in our construction are reflected in the codes constructed. Consequently, we are able to comment further on the optimality, uniqueness and rotational presentation of some of these codes. In Table I the entries (α) and (γ) come from full Steiner systems and trivial codes, whereas entry (β) is derived from the extended (24,12,8) binary Golay code. We show that the code indicated by (α) is unique as well as length optimal. With the aid of an automorphism of the (3,4,8)-Steiner system used in its construction, we show that the code (α) has a parity check matrix in the rotational form

$$H = \begin{pmatrix} H_1 & H_2 & RH_1 & RH_2 & R^2H_1 & R^2H_2 \cdots R^6H_1 & R^6H_2 \end{pmatrix} \quad (1)$$

Manuscript received May 20, 1988; revised February 26, 1989. This work was supported in part by the Center for Microelectronics Design and Test, University of South Florida, Tampa, FL.

W. E. Clark is with the Department of Mathematics, University of South Florida, Tampa, FL 33620.
L. A. Dunning is with the Department of Computer Science, Bowling Green State University, Bowling Green, OH 43403-0214.
D. G. Rogers is temporarily at P.O. Box 8011, Honolulu, Hawaii 96830-0011. His permanent address is Fernley House, The Green, Croxley Green, United Kingdom, WD3 3HT.

IEEE Log Number 8931673.