# New Class of Nonlinear Systematic Error Detecting Codes

Mark Karpovsky, *Fellow, IEEE,* and Alexander Taubin, *Senior Member, IEEE*

***Abstract*— We will say that code $C$ detects error $e$ with probability $1-Q(e)$, if $Q(e)$ is a fraction of codewords $y$ such that $y, y+e \in C$. We present a class of optimal nonlinear $q$-ary systematic $(n,k)$-codes (robust codes) minimizing over all $(n,k)$- codes maxima of $Q(e)$ over all $e \neq 0$. We will also show that any linear $(n,k)$-code $V$ with $n \leq 2k$ can be modified into a nonlinear $(n,k)$-code $C_V$ with simple encoding and decoding procedures, such that set $E = \{e \,|Q(e) = 1\}$ of undetected errors for $C_V$ is a $(k-r)-$ dimensional subspace of $V$ ($|E|=q^{k-r}$ instead of $q^k$ for $V$). For the remaining $q^n$-$q^{k-r}$ nonzero errors $Q(e) \leq q^{-r}$ for $q \geq 3$ and $Q(e) \leq 2^{-r+1}$ for $q = 2$.**

***Index Terms*— nonlinear systematic error detecting codes, minimax criterion for error detection, robust error detection**

## I. INTRODUCTION

We present a construction for optimal systematic error-detecting codes for the case where distributions of errors in the channel are not known or 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 these codes. We will use the following probability as the measure for the error-detection capability of a code.

Let $C \subseteq GF(q^n)$ be a systematic $(n,k)$- code and $e \in GF(q^n)$. We define the error-detecting probability given error $e$ (where $e \neq 0$) for the code $C$ as:

$$1 - Q(e) = 1 - q^{-k} \left| \{ y \,| y, y+e \in C \} \right|. \qquad (1)$$

(We assume that all the codewords have the same probability of being transmitted).

The following lower bounds for error-masking probability $Q(e)$ have been proven in [1] for any $q$-ary code $C$ of length $n$ and any error $e$:

$$Q(e) \geq |C|^{-1} \left\lceil (q^n - 1)^{-1} |C| \left( |C| - 1 \right) \right\rceil \; for \; q \geq 3 \qquad (2)$$

and

$$Q(e) \geq 2 \, |C|^{-1} \left\lceil 0.5 \, |C| \left( |C| - 1 \right) (2^n - 1)^{-1} \right\rceil \; for \; q = 2. \qquad (3)$$

For a given block size $n$ and number of information digits $k$ our goal is to construct an optimal code such that maxima of $Q(e)$ over all $e \neq 0$ are minimal. The problem can be formulated as follows. For given $n, k, q$ construct a code based on $\min_{C \in C(n,k,q)} \max_{e \neq 0} Q(e)$, where $C(n,k,q)$ denotes the set of all $q$-ary $(n,k)$-codes.

Manuscript received , 2003; revised December 19, 2003.

M. Karpovsky and A.Taubin are with Reliable Computing Laboratory, Boston University, E-mails: markkar@bu.edu, taubin@bu.edu

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 [5]. This criterion was used for error detection in computation channels (VLSI chips), where the distributions of errors (errors are manifestations of faults at the outputs of the chips) are difficult to characterize [3]. Hence the presented codes are applicable in the design of fault-tolerant devices. In the area of computer hardware testing, optimal compression of test responses based on the minimax approach was described in [2].

We present the solution of this problem for the cases $n = 2k$ and $n = 2k-1$ for $q = 2$ and $n = 2k$ for $q \geq 3$.

We note that asymptotically optimal codes of length $n = 2m$ containing $q^{2m-1} - q^{m-1}$ codewords and detecting any error with probability at least $1 - (q^{2m-1} - q^{m-1})^{-1} (q^{2m-2} + q^{m-1})$ were described in [1]. But these codes are not systematic and have rather complicated encoding and decoding procedures.

Let $V$ be a linear $q$-ary $(n,k)-$code ($q$ is a prime) with $n \leq 2k$ and check matrix $H = [P \,| I]$ where $P$ is an $(n-k) \times k$ matrix of rank $r = n-k$ over $GF(q)$ and $I$ is the $r \times r$ identity matrix.

We will also show in this paper that linear $(n,k)$-code $V$ can be modified into a nonlinear $(n,k)-$code $C_V$ with simple encoding and decoding procedures, such that set $E = \{e \,| Q(e) = 1\}$ of undetected errors for $C_V$ is a $(k-r)-$dimensional subspace of $V (|E| = q^{k-r}$ instead of $q^k$ for $V)$. For the remaining $q^n - q^{k-r}$ nonzero errors $Q(e) \leq q^{-r}$ for $q \geq 3$ and $Q(e) \leq 2^{-r+1}$ for $q = 2$.

## II. NONBINARY CODES.

We will start with a nonbinary case since in this case the construction is simpler.

Let $V$ be a linear $q$-ary $(n,k)-$code ($q \geq 3$ is a prime) with $n \leq 2k$ and check matrix $H = [P \,| I]$ with $rank(P) = n-k$.

*Theorem 1:*
Let $C_V = \left\{ (x,w) \,\middle|\, x \in GF(q^k),\, w = (Px)^2 \in GF(q^r) \right\}$. Then for $C_V$ the set $E = \{e \,| Q(e) = 1\}$ of undetected errors is a $(k-r)-$ dimensional subspace of $V$, $q^k - q^{k-r}$ errors are detected with probability 1 and remaining $q^n - q^k$ errors are detected with probability $1 - q^{-r}$.

*Proof:* Error $e = (e_x, e_w)$ is not detected by $C_V$ when message $(x, (Px)^2)$ is transmitted iff

$$(P(x + e_x))^2 = (Px)^2 + e_w. \qquad (4)$$

From (4) we have

$$2(Px)\,(Pe_x)\ + (Pe_x)^2 - e_w = 0. \tag{5}$$

Equation (5) is satisfied for all $x$ iff $Pe_x = e_w = 0$. Since $[P\,|I]$ is the check matrix for $V$ and $rank(P) = r$, the number of errors $e = (e_x, e_w)$ (including $e = 0$) satisfying (5) is $q^{k-r}$, and these errors form $(k-r)$-dimensional subspace $E$in $V = \{(x,\, w)\,|w = Px\}$ .

If $Pe_x = 0$ and $e_w \neq 0$, then (5) is not satisfied for any $x$. The number of these errors is equal to $q^k - q^{k-r}$.

If $Pe_x \neq 0$, then for any $e = (e_x,\, e_w)$ there exists a unique $Px$ satisfying (5). The probability that for a given $e$ such that $Pe_x \neq 0$ randomly selected $x \in GF(q^k)$is not satisfying (5) is $1 - q^{-r}$, and the number of errors $e = (e_x,\ e_w)$, such that $Pe_x \neq 0$ is $q^n - q^k$. ∎

For the case $k = r$ the proposed codes are *robust*, i.e. have the same probability, $Q(e) = q^{-r}$, for the detection of any nonzero error $e$. Comparing these codes with codes proposed in [1], one can see that $C_V$ has more simple encoding and decoding procedures and for the same size of a code has a twice smaller maximal probability of not detecting an error.

We will show now that the proposed codes are optimal for the minimax error detection and rate $1/2$, i.e. these codes minimize maxima of error-masking probability $Q(e),\ \ e \neq 0$, defined by (1).

*Corollary 1:* Codes $C_V$ are optimal for rate $1/2$ and any $q \geq 3$.

*Proof: Corollary 1* follows from *Theorem* 1 and (2), since for codes $C_V$ with rate $1/2$ we have $Q(e) = q^{-k}$ for all $e \neq 0$. ∎

We note also that encoding and decoding procedures for code $C_V$ require multiplication by $P$ over $GF(q)$ and computing $(Px)^2$ in $GF(q^r)$. This last operation requires not more than $O(r^2)$ additions and multiplications $\bmod q$.

*Example 1:* Let $q = 3$, $n = 3$, $k = 2$ and $P = [21]$. Then $C_V$ =$\{$000, 011, 021, 101, 110, 121, 201, 211, 220$\}$. The following $3^{k-3} = 3$ errors are not detected by $C_V$: 000, 110 and 220. ( For these errors $Pe_x = e_w = 0$). Errors 001, 002, 111, 112, 221, 222 are detected for any message. (For these errors $Pe_x = 0$ and $e_w \neq 0$). Any one of the remaining $3^n - 3^k$ =18 errors with $Pe_x \neq 0$ is detected with probability $1 - 3^{-r} = 2/3$. For example, error 121 is detected when any one of the following 6 (out of 9 possible) messages are transmitted: 011, 021, 101, 121, 201 and 220.

## III. Binary Codes

For the binary case we will slightly modify our construction for $C_V$.

Let $V$ be a binary linear $(n,k)-$code with $n \leq 2k$ and check matrix $H = [P\,|I]$ with $rank(P) = n - k$.

*Theorem 2:*
Let $C_V = \{(x,w)\,\big|x \in GF(2^k),\ w = (Px)^3 \in GF(2^r)\}$. Then the set $E = \{e\,|Q(e) = 0\}$of undetected errors for $C_V$ is a $(k-r)-$dimensional subspace of $V$, and from the remaining $2^n - 2^{k-r}$errors $2^{n-1} + 2^{k-1} - 2^{k-r}$are detected with probability 1 and $2^{n-1} - 2^{k-1}$ are detected with probability $1 - 2^{-r+1}$.

*Proof:* Error $e = (e_x,\, e_w)$ is not detected for message $(x,\, (Px)^3)$ from $C_V$ iff

$$(P(x + e_x))^3 = (Px)^3 + e_w \tag{6}$$

or

$$(Px)^2(Pe_x) + (Px)(Pe_x)^2 + (Pe_x)^3 + e_w. \tag{7}$$

It follows from (7) that $e = (e_x,\, e_w)$ is not detected for any $x$ iff $Pe_x = e_w = 0$, and $E = \{(e_x,\, e_w)\,|Pe_x = e_w = 0\}$ is a $(k-r)-$dimensional subspace in $V = \{(x,\, w)\,|w = Px\}$.

If $Pe_x = 0$ and $e_w \neq 0$, then $e$ is detected by $C_V$ for any $x$. There are

$$N_1 = 2^k - 2^{k-r} \tag{8}$$

errors, satisfying this condition.

For any given $e = (e_x,\, e_w)$ such that $Pe_x \neq 0$ quadratic equation (7) has 2 solutions for $Px$ iff

$$Tr((Pe_x)^{-3}\,((Px)^3 + e_w)) = Tr(1) + Tr((Pe_x)^{-3}\,e_w) = 0 \tag{9}$$

and has 0 solutions iff

$$Tr(1) + Tr((Pe_x)^{-3}\,e_w) = 1, \tag{10}$$

where $Tr(y)$ is the trace of $y \in GF(2^r)$ [4].

Since out of $2^n - 2^k$ errors $e = (e_x,\, e_w)$ such that $Pe_x \neq 0$

$$N_2 = 2^{n-1} - 2^{k-1} \tag{11}$$

satisfy (10), we have from (8) and (11) for a number, $N$, of errors which are detected for any $x$

$$N = N_1 + N_2 = 2^{n-1} + 2^{k-1} - 2^{k-r}.$$

Finally, the remaining $2^{n-1} - 2^{k-1}$errors satisfying (9) are detected with probability $1 - 2^{-r+1}$. ∎

*Example 2:* Consider (7,4) Hamming code $V$ with $P = \begin{bmatrix} 0111 \\ 1011 \\ 1101 \end{bmatrix}$. Then the corresponding (7,4)-code $C_V$does not detect only one nonzero error 1110000. Errors $0000w_0w_1w_2$ and $1110w_0w_1w_2$ , where $w_0w_1w_2 \neq 000$ are detected with probability 1, and , since in this case $Tr(1) = 1$, we have by (9), (10) that out of remaining 112 errors 56 errors $(e_x,\, e_w)$ with $Tr((Pe_x)^{-3}\,e_w) = 0$ are also detected with probability 1 and 56 errors with $Tr((Pe_x)^{-3}\,e_w) = 1$ are detected with probability 0.75.

*Example 3:* Consider $(2k,k)$ repetition codes $V$ with $P = I$. For these codes, which are widely used in fault-tolerant computing, error $e = (e_x,\, e_w)$ is not detected iff $e_x = e_w$. (This may be the case when both copies of the device have a common source of errors, such as variation in power supply, temperature, etc.).

The corresponding nonlinear $(2k, k)$-codes $C_V$ detect all nonzero errors, $2^{2k-1} + 2^{k-1} - 1$ of them are detected with probability 1 and the remaining $2^{2k-1} - 2^{k-1}$ with probability $1 - 2^{-k+1}$.

*Corollary 2:* Binary codes $C_V$ are optimal for $r = k - 1$ and $r = k$.

*Proof:* *Corollary* 2 follows from *Theorem* 2 and (3) since for $r = k - 1$ and $r = k$ we have $|C_V|\,(|C_V| - 1) \leq 2(2^n - 1)$. ■

## REFERENCES

[1] M.G. Karpovsky and P. Nagvajara. Optimal codes for the minimax criterion on error detection. *IEEE Transactions on Information Theory*, 35(6):1299–1305, November 1989.

[2] M.G. Karpovsky and P. Nagvajara. Optimal robust compression of test response. *IEEE Transactions on Computers*, 39(1):138–141, January 1990.

[3] P. K. Lala. *Self-Checking and Fault-Tolerant Digital Design*. Academic Press, 2000.

[4] F.J. McWilliams and N.J.A. Sloane. *The Theory of Error-Correcting Codes*. North Holland, 1978.

[5] S.Verdu and V.H. Poor. Minimax robust discrete-time match filters. *IEEE Transactions on Communications*, 31:208–216, February 1983.