NASA CR-170604

ON THE PROBABILITY OF UNDETECTED ERROR FOR THE MAXIMUM DISTANCE SEPARABLE CODES

Technical Reports

to

NASA

Goddard Space Flight Center

Greenbelt, Maryland

Grant Number NAG 5-234

Principal Investigators

Daniel J. Costello, Jr.
Department of Electrical Engineering
Illinois Institute of Technology
Chicago, Illinois 60616

Shu Lin
Department of Electrical Engineering
University of Hawaii at Manoa
2540 Dole Street
Honolulu, Hawaii 96822

August 29, 1983

ON THE PROBABILITY OF UNDETECTED ERROR FOR THE MAXIMUM DISTANCE SEPARABLE CODES*

Tadao Kasami
Osaka University
Toyonaka, JAPAN 560

Shu Lin
University of Hawaii at Manoa
Honolulu, Hawaii 96822

ABSTRACT

In this paper we investigate the performance of maximum-distance-separable codes with symbols from GF(q) when they are used for pure error detection or for simultaneous error correction and detection. We show that these codes are good for symbol error detection. Their probability of undetected error is upper bounded by q^{-r} and decreases monotonically as the symbol error probability ε decreases from (q-1)/q to 0, where r is the number of parity-check symbols of a code.

*This research is partially supported by NASA Grant NAG5-234.

1. Introduction

For controlling transmission errors in data communication systems, a linear block code can be used in three different manners, namely: pure error detection, pure error correction, and simultaneous error correction and detection [1,2]. Error detection incorporated with automatic-repeat-request (ARQ) can provide virtually error-free data transmission [2]. In this paper we investigate the performance of maximum-distance-separable codes when they are used for pure error detection or for simultaneous error correction and detection.

An (n,k) linear code with symbols from a finite field of q elements, GF(q), is called a maximum-distance-separable (MDS) code if its minimum distance d is one greater than its number n-k of parity-check symbols [3,4], i.e.,

$$d = n - k + 1 .$$

An important property of MDS codes is that a shortened MDS code is also a MDS code. The most important MDS codes are q-ary Reed-Solomon (RS) codes of length $n = q-1$ [1,2,4,5] and the extended q-ary RS codes of length $n = q+1$ [4,6,7]. RS (or shortened RS) codes are widely used for error control in data communication and data storage systems. They can be used either for correcting random symbol (or character) errors or for correcting multiple bursts of errors [1,2]. In this paper we show that these codes are also very effective in detecting errors.

Consider a q-ary (n,k) code C which is used for error detection on a discrete memoryless channel (DMC) with q inputs and q outputs. We assume that any symbol which is transmitted has a probability $(1-\varepsilon)$ of being received correctly and a probability $\varepsilon/(q-1)$ of being changed into each of the q-1 other symbols. Suppose that a codeword $\overline{v} = (v_0,v_1,\ldots,v_{n-1})$ is transmitted. Let $\overline{r} = (r_0,r_1,\ldots,r_{n-1})$ be the corresponding received vector. Then the difference,

$$\overline{e} = \overline{r}-\overline{v} = (r_0-v_0,r_1-v_1,\ldots,r_{n-1}-v_{n-1}) \qquad (1)$$

is the error pattern caused by the channel noise, where "-" denotes the subtraction defined on GF(q). From (1), we see that

$$\bar{r} = \bar{v} + \bar{e}$$

where "+" denotes the addition defined on GF(q). If the error pattern $\bar{e}$ is a nonzero codeword in C, then $\bar{r}$ is also a codeword but $\bar{r} \neq \bar{v}$. In this case, the decoder assumes that $\bar{r}$ is error-free and accepts $\bar{r}$ as the transmitted codeword [1,2]. As a result, a decoding error is commited. Such an error pattern is said to be undetectable. If $\bar{e}$ is not a codeword, then $\bar{r}$ is not a codeword and the decoder would be able to detect the existence of an error. Such an error pattern is called a detectable error pattern. Let $P_{ud}(C,\varepsilon)$ denote the probability that the decoder fails to detect the existence of an error. This probability is called the probability of undetected error for C. This probability is normally used to measure the error detection performance of a code. For a code to be good in error detection, this probability should be small for all ε.

Let $C^{\perp}$ denote the dual code of C. Let A_i and B_i be the number of codewords of weight i in C and $C^{\perp}$ respectively. The sets $\{A_i: 0 \leq i \leq n\}$ and $\{B_i: 0 \leq i \leq n\}$ are called the weight distributions (or spectra) of C and $C^{\perp}$ respectively [1,2,4,8]. The probability of undetected error for C can be expressed either in terms of the weight distribution of C or in terms of the weight distribution of $C^{\perp}$ as follows:

$$P_{ud}(C,\varepsilon) = \sum_{i=1}^{n} A_i \left(\frac{\varepsilon}{q-1}\right)^i (1-\varepsilon)^{n-i} \ , \tag{2}$$

$$= q^{-(n-k)} \sum_{i=0}^{n} B_i \left(1 - \frac{q\varepsilon}{q-1}\right)^i - (1-\varepsilon)^n \ . \tag{3}$$

From (2) and (3), we see that, to compute the exact probability of undetected error for a linear code (one needs to know either the weight distribution of C or the weight distribution of its dual $C^{\perp}$. Theoretically, we can compute the weight distribution of C by examining its q^k codewords or by examining the q^{n-k} codewords of its dual $C^\perp$. For large n, k, n-k and q, the computation becomes practically impossible. Except for some short linear codes and a few small classes of linear codes [1,2,4,8], the weight distribution for many known linear codes are still unknown. Consequently, it is very difficult, if not impossible, to compute their probability of undetected error. Even if we know the weight distribution of a code and are able to compute its probability of undetected error, we still need a criterion to say whether the code is good or poor in error detection.

Consider the ensemble Γ of all q-ary (n,k) linear codes. Let $\overline{P_{ud}(\varepsilon)}$ denote the average probability of an undetected error over the ensemble Γ. It has been proved [9] that

$$\overline{P_{ud}(\varepsilon)} = [1 - (1-\varepsilon)^k]q^{-(n-k)} \qquad (4)$$

for all n, k and ε with $0 \le \varepsilon < 1$. Therefore, there must be codes in Γ with $P_{ud}(C,\varepsilon)$ satisfying the following bound:

$$P_{ud}(C,\varepsilon) \le [1 - (1-\varepsilon)^k]q^{-(n-k)} \qquad (5)$$

Since $[1-(1-\varepsilon)^k] \le 1$, a weaker bound is that there exist codes in Γ such that

$$P_{ud}(C,\varepsilon) \le q^{-(n-k)} \qquad (6)$$

For q=2, the bound given by (5) was first proved by Korzhik [10]. The proof of the bound given by (5) is an existence proof and no general method has been found for constructing codes satisfying the bound given by (5). Only a few small classes of known binary codes [9,11-13] have been proved to satisfy the weaker bound $2^{-(n-k)}$. These are Hamming codes, distance-4 Hamming codes, double-error-correcting and some triple-error-correcting primitive BCH codes. For q>2, only a few RS codes of short length have been proved to satisfy the weaker bound $q^{-(n-k)}$ [9].

For a q-ary input and q-ary output DMC, the worst channel condition is that $\varepsilon=(q-1)/q$. In this case, each of the q symbols from the code alphabet occurs at the receiver with equal probability. Consequently [9],

$$P_{ud}[C,\frac{q-1}{q}] = q^{-(n-k)} - q^{-n} \approx q^{-(n-k)} .$$

In this paper, we only consider the case where $0\leq\varepsilon\leq(q-1)/q$. A q-ary (n,k) code C is said to be good for error detection if

$$P_{ud}(C,\varepsilon) \leq q^{-(n-k)}$$

for $0\leq\varepsilon\leq(q-1)/q$ and $P_{ud}(C,\varepsilon)$ decreases monotonically as ε decreases from $(q-1)/q$ to 0.

In this paper we investigate the error detection performance of MDS codes. First we consider the case for which MDS codes are used only for pure error detection. We will show that all MDS codes are good for error detection. Then we consider the case for which MDS codes are used for simultaneous error correction and error detection. We will study their probability of undetected error after error correction.

2. Probability of an Undetected Error for MDS Codes

In this section, we will show that the probability of undetected error for a MDS code satisfies the upper bound $q^{-(n-k)}$ for $0\leq\varepsilon\leq(q-1)/q$ and decreases monotonically as ε decreases from $(q-1)/q$ to 0. Hence, the MDS codes are good for error detection.

Consider a q-ary MDS (n,k) code C with minimum distance d=n-k+1. The number of codewords of weight i is given by

$$A_i = \binom{n}{i} \left\{ \sum_{j=0}^{i-d} (-1)^j \binom{i}{j} q^{i-j+1-d} + \sum_{j=i-d+1}^{i} (-1)^j \binom{i}{j} \right\} \qquad (7)$$

for $d\leq i\leq n$ and $A_i=0$ for $0\leq i<d$. The weight distribution of a MDS code was derived independently by Assmus, Mattson, and Turyn [14]; Forney [15]; and Kasami, Lin,

and Peterson [6]. The expression for A_i given by (7) can be rearranged into the following form:

$$A_i = \binom{n}{i} q^{-(n-k)} \left\{ (q-1)^i + \sum_{j=0}^{n-k} (-1)^{i+j} \binom{i}{j} (q^{n-k} - q^j) \right\} \tag{8}$$

for $d \leq i \leq n$. From (2) and (8) we can compute the probability $P_{ud}(C,\varepsilon)$ of undetected error for a MDS code C. However, in the following, we will derive a different expression for $P_{ud}(C,\varepsilon)$ which is more convenient to work with.

Define

$$A(X,Y) = \sum_{i=d}^{n} A_i X^i Y^{n-i} \tag{9}$$

with A_i given by (8). From (2) and (9) we see that

$$P_{ud}(C,\varepsilon) = A\left(\frac{\varepsilon}{q-1}, 1-\varepsilon\right) . \tag{10}$$

Let

$$\gamma = q - 1 . \tag{11}$$

Then A(X,Y) can be put into the following form [see Appendix A for derivation]:

$$A(X,Y) = q^{-(n-k)} \left\{ (\gamma X+Y)^n + \sum_{i=0}^{n-k-1} \binom{n}{i} (q^{n-k} - q^i) X^i (Y-X)^{n-i} - q^{n-k} Y^n \right\} \tag{12}$$

It follows from (10) and (12) that we have the following expression for $P_{ud}(C,\varepsilon)$:

$$P_{ud}(C,\varepsilon) = q^{-(n-k)} \left\{ 1 + \sum_{i=0}^{n-k-1} \binom{n}{i} (q^{n-k} - q^i) \left(\frac{\varepsilon}{q-1}\right)^i \left(1 - \frac{q\varepsilon}{q-1}\right)^{n-i} - q^{n-k} (1-\varepsilon)^n \right\} \tag{13}$$

For the worst channel condition $\varepsilon = (q-1)/q$, we have

$$P_{ud}\left(C, \frac{q-1}{q}\right) = q^{-(n-k)} - (1-\varepsilon)^n \leq q^{-(n-k)} \tag{14}$$

Next we will show that $P_{ud}(C,\varepsilon)$ decreases monotonically as ε decreases from $(q-1)/q$ to 0. This is done by examining whether the derivative of $P_{ud}(C,\varepsilon)$,

$$\frac{d}{d\varepsilon} P_{ud}(C,\varepsilon)$$

is positive for $0<\varepsilon<(q-1)/q$. From (13), we have

$$\begin{aligned}
\frac{d}{d\varepsilon} P_{ud}(C,\varepsilon) = {} & q^{-(n-k)} \left\{ \gamma^{-1} \sum_{i=0}^{n-k} i\binom{n}{i}(q^{n-k}-q^{i})\left(\frac{\varepsilon}{\gamma}\right)^{i-1}\left(1-\frac{q\varepsilon}{\gamma}\right)^{n-i} \right. \\
& \left. -q\gamma^{-1} \sum_{i=0}^{n-k}(n-i)\binom{n}{i}(q^{n-k}-q^{i})\left(\frac{\varepsilon}{\gamma}\right)^{i}\left(1-\frac{q\varepsilon}{\gamma}\right)^{n-1-i} \right\} \\
& + n(1-\varepsilon)^{n-1} \\
= {} & q^{-(n-k)} \left\{ \gamma^{-1} \sum_{i=1}^{n-k} n\binom{n-1}{i-1}(q^{n-k}-q^{i})\left(\frac{\varepsilon}{\gamma}\right)^{i-1}\left(1-\frac{q\varepsilon}{\gamma}\right)^{n-i} \right. \\
& \left. -q\gamma^{-1} \sum_{i=0}^{n-k} n\binom{n-1}{i}(q^{n-k}-q^{i})\left(\frac{\varepsilon}{\gamma}\right)^{i}\left(1-\frac{q\varepsilon}{\gamma}\right)^{n-1-i} \right\} \\
& + n(1-\varepsilon)^{n-1} \\
= {} & nq^{-(n-k)}\gamma^{-1} \left\{ \sum_{i=0}^{n-k-1} \binom{n-1}{i}(q^{n-k}-q^{i+1})\left(\frac{\varepsilon}{\gamma}\right)^{i}\left(1-\frac{q\varepsilon}{\gamma}\right)^{n-1-i} \right. \\
& \left. -q \sum_{i=0}^{n-k-1} \binom{n-1}{i}(q^{n-k}-q^{i})\left(\frac{\varepsilon}{\gamma}\right)^{i}\left(1-\frac{q\varepsilon}{\gamma}\right)^{n-1-i} \right\} \\
& + n(1-\varepsilon)^{n-1} \\
= {} & nq^{-(n-k)}\gamma^{-1} \left\{ -\gamma q^{n-k} \sum_{i=0}^{n-k-1} \binom{n-1}{i}\left(\frac{\varepsilon}{\gamma}\right)^{i}\left(1-\frac{q\varepsilon}{\gamma}\right)^{n-1-i} \right\} \\
& + n(1-\varepsilon)^{n-1} \\
= {} & n(1-\varepsilon)^{n-1} - n \sum_{i=0}^{n-k-1} \binom{n-1}{i}\left(\frac{\varepsilon}{\gamma}\right)^{i}\left(1-\frac{q\varepsilon}{\gamma}\right)^{n-1-i} \\
= {} & n \sum_{i=n-k}^{n-1} \binom{n-1}{i}\left(\frac{\varepsilon}{\gamma}\right)^{i}\left(1-\frac{q\varepsilon}{\gamma}\right)^{n-1-i} \qquad (15)
\end{aligned}$$

From (15) we see that

$$\frac{d}{d\varepsilon} P_{ud}(C,\varepsilon) > 0 \qquad (16)$$

for $0<\varepsilon<\gamma/q = (q-1)/q$. Note that, from (15),

$$\left.\frac{d}{d\varepsilon} P_{ud}(C,\varepsilon)\right|_{\varepsilon=(q-1)/q} = 0 \qquad (17)$$

From (14), (16) and (17), we conclude that $P_{ud}(C,\varepsilon)$ for a q-ary (n,k) MDS code satisfies the bound $q^{-(n-k)}$ and decreases monotonically as ε decreases from $(q-1)/q$ to 0. Hence MDS codes are good for error detection.

3. Probability of an Undetected Error after Error Correction for MDS Codes

Consider a q-ary (n,k) code C with minimum distance d. Let t be a non-negative integer such that $t < d/2$. Suppose that code C is used to correct all error patterns with t or fewer symbol errors. Let $P_{ud}(C,t,\varepsilon)$ denote the probability of undetected error after error correction. An error pattern is undetectable if it is in a coset of weight t or less but not the coset leader [1,2]. Such an error pattern will cause a decoding error. In this section, we will investigate the error probability $P_{ud}(C,t,\varepsilon)$ for a MDS code, and will show that $P_{ud}(C,t,\varepsilon)$ decreases monotonically as ε decreases from $(q-1)/q$ to 0. Note that, for t=0,

$$P_{ud}(C,0,\varepsilon) = P_{ud}(C,\varepsilon) .$$

Let $\gamma = q-1$. Let $\{A_i:\ 0 \le i \le n\}$ be the weight distribution of C. Define the following polynomial:

$$A(X+Y+(\gamma-1)XY,\ 1+\gamma XY) = \sum_{h=d}^{n} A_h (X+Y+(\gamma-1)XY)^n (1+\gamma XY)^{n-h} . \tag{18}$$

If we expand each term in the summation of (18), $A(X+Y+(\gamma-1)XY,\ 1+\gamma XY)$ can be put into the following form:

$$A(X+Y+(\gamma-1)XY,\ 1+\gamma XY) = \sum_{h=0}^{n} Q_h(X) Y^h \tag{19}$$

where $Q_h(X) = \sum_{\ell=0}^{n} Q_{h,\ell} X^{\ell}$. MacWilliams [16] proved that $Q_{h,\ell}$ is the number of vectors of weight ℓ in the cosets of weight h, excluding the coset leaders.

Let

$$P_h(\varepsilon) = (1-\varepsilon)^n Q_h\left(\frac{\varepsilon}{\gamma(1-\varepsilon)}\right) \tag{20}$$

which is the probability that an undetectable error pattern in a coset of weight h occurs for $0 \leq h \leq t$. Then

$$P_{ud}(C,t,\varepsilon) = \sum_{h=0}^{t} P_h(\varepsilon) \ . \tag{21}$$

Now suppose that C is a q-ary (n,k) MDS code with minimum distance d=n-k+1 and weight distribution given by (8). It follows from (9), (12) and (18) that

$$\begin{aligned}
&A(X+Y+(\gamma-1)XY,\ 1+\gamma XY)\\
&\quad = q^{-(n-k)}\Big\{(1+\gamma X)^n(1+\gamma Y)^n\\
&\qquad + \sum_{i=0}^{n-k-1}\binom{n}{i}(q^{n-k}-q^i)[X+(1+(\gamma-1)X)Y]^i(1-X-Y+XY)^{n-i}\\
&\qquad - q^{n-k}(1+\gamma XY)^n\Big\}\\
&\quad = q^{-(n-k)}(1+\gamma X)^n(1+\gamma Y)^n\\
&\qquad + \sum_{i=0}^{n-k-1}\binom{n}{i}(1-q^{-(n-k)+i})(1-X)^{n-i}[X+(1+(\gamma-1)X)Y]^i(1-Y)^{n-i}\\
&\qquad - (1+\gamma XY)^n \ .
\end{aligned} \tag{22}$$

From (22), we find that

$$\begin{aligned}
Q_h(X) &= q^{-(n-k)}(1+\gamma X)^n\binom{n}{h}\gamma^h\\
&\quad + \sum_{i=0}^{n-k-1}\binom{n}{i}(1-q^{-n+k+i})(1-X)^{n-i} \ \cdot\\
&\quad \sum_{j=\max(0,h+i-n)}^{\min(i,h)}(-1)^{h-j}\binom{i}{j}\binom{n-i}{h-j}X^{i-j}[1+(\gamma-1)X]^j\\
&\quad - \binom{n}{h}\gamma^h X^h
\end{aligned} \tag{23}$$

Since

$$\binom{n}{i}\binom{i}{j}\binom{n-i}{h-j} = \binom{n}{h}\binom{n-h}{i-j}\binom{h}{j} \ ,$$

we have

$$Q_h(X) = \binom{n}{h}\Big[\gamma^h q^{-(n-k)}(1+\gamma X)^n - \gamma^h X^h + \sum_{i=0}^{n-k-1}\ \sum_{j=\max(0,h+i-n)}^{\min(i,h)} (-1)^{h-j}\binom{n-h}{i-j}\binom{h}{j}(1-q^{-n+k+i})(1-X)^{n-i}X^{i-j}[1+(\gamma-1)X]^j\Big] \tag{24}$$

It follows from (20) and (24) that

$$P_h(\varepsilon) = \binom{n}{h}\Big\{ q^{-(n-k)}\gamma^h - \varepsilon^h(1-\varepsilon)^{n-h} + \sum_{i=0}^{n-k-1}\ \sum_{j=\max(0,h+i-n)}^{\min(i,h)} (-1)^{h-j}\binom{n-h}{i-j}\binom{h}{j}(1-q^{-n+k+i})(\tfrac{\varepsilon}{\gamma})^{i-j}(1 - \tfrac{\varepsilon}{\gamma})^j(1 - \tfrac{q\varepsilon}{\gamma})^{n-i}\Big\} \tag{25}$$

The summation

$$\sum_{i=0}^{n-k-1}\ \sum_{j=\max(0,h+i-n)}^{\min(i,h)}$$

in (25) can be rewritten as

$$\sum_{\ell=0}^{\min(n-k-1,n-h)}\ \sum_{j=0}^{\min(n-k-1-\ell,h)}$$

where $\ell = i-j$. As a result, $P_h(\varepsilon)$ can be put into the following form:

$$P_h(\varepsilon) = \binom{n}{h}\Big\{ q^{-(n-k)}\gamma^h - \varepsilon^h(1-\varepsilon)^{n-h} + \sum_{\ell=0}^{\min(n-k-1,n-h)} \binom{n-h}{\ell}(\tfrac{\varepsilon}{\gamma})^{\ell}(1 - \tfrac{q\varepsilon}{\gamma})^{n-h-\ell}R_{h,\ell}(\varepsilon)\Big\} \tag{26}$$

where

$$R_{h,\ell}(\varepsilon) = \sum_{j=0}^{\min(n-k-1-\ell,h)} (-1)^{h-j}\binom{h}{j}(1-q^{-n+k+\ell+j})(1 - \tfrac{\varepsilon}{\gamma})^j(1 - \tfrac{q\varepsilon}{\gamma})^{h-j} \tag{27}$$

for $0 \le \ell < n-k$. Combining (21) and (26), we have

$$P_{ud}(C,t,\varepsilon) = \sum_{h=0}^{t}\binom{n}{h}\Big[q^{-(n-k)}\gamma^h - \varepsilon^h(1-\varepsilon)^{n-h} + \sum_{\ell=0}^{\min(n-k-1,n-h)} \binom{n-h}{\ell}(\tfrac{\varepsilon}{\gamma})^{\ell}(1 - \tfrac{q\varepsilon}{\gamma})^{n-h-\ell} R_{h,\ell}(\varepsilon)\Big] \tag{28}$$

It is easy to check that $P_{ud}(C,\varepsilon)$ given by (13) can be obtained from $P_{ud}(C,t,\varepsilon)$ by setting $t=0$. For any t, we can compute the probability of undetected error after error correction for a q-ary (n,k) MDS code for (28). For the worst channel condition $\varepsilon = (q-1)/q$, we have

$$P_{ud}(C,t,\tfrac{q-1}{q}) = \sum_{h=0}^{t} \binom{n}{h} \left[q^{-(n-k)}(q-1)^{h} - \varepsilon^{h}(1-\varepsilon)^{n-h}\right] \tag{29}$$

Next we will show that $P_{ud}(C,t,\varepsilon)$ for a MDS code decreases monotonically from $P_{ud}(C,t,\frac{q-1}{q})$ as ε decreases from $(q-1)/q$ to 0. From (28), we can show [see Appendix B] that

$$\frac{d}{d\varepsilon} P_{ud}(C,t,\varepsilon) = n\binom{n-1}{t}\left\{\varepsilon^{t} \sum_{\ell=n-k}^{n-1-t} \binom{n-1-t}{\ell}\left(\frac{\varepsilon}{\gamma}\right)^{\ell}\left(1-\frac{q\varepsilon}{\gamma}\right)^{n-1-t-\ell} + N_t(\varepsilon)\right\} \tag{30}$$

where

$$N_t(\varepsilon) = \sum_{\ell=n-k-t}^{\min(n-k-1,n-1-t)} \binom{n-1-t}{\ell}\left(\frac{\varepsilon}{\gamma}\right)^{\ell}\left(1-\frac{q\varepsilon}{\gamma}\right)^{n-1-t-\ell} \cdot \sum_{j=0}^{\ell-n+k+t} (-1)^{j}\binom{t}{j}\left(1-\frac{\varepsilon}{\gamma}\right)^{t-j}\left(1-\frac{q\varepsilon}{\gamma}\right)^{j} , \tag{31}$$

and

$$N_0(\varepsilon) = 0 .$$

For $t=0$, it follows from (30) that

$$\frac{d}{d\varepsilon} P_{ud}(C,0,\varepsilon) = h \sum_{\ell=n-k}^{n-1} \binom{n-1}{\ell}\left(\frac{\varepsilon}{\gamma}\right)^{\ell}\left(1-\frac{q\varepsilon}{\gamma}\right)^{n-1-\ell} > 0 \tag{32}$$

for $0<\varepsilon<\gamma/q$.

Now we consider the case for which $0<t<d/2$. For $d\geq 3$, we can show that

$$N_t(\varepsilon) > 0 \tag{33}$$

for $0<\varepsilon<\gamma/q$ [see Appendix C]. Consequently, it follows from (30) and (33) that, for $d\geq 3$, $0<t<d/2$ and $0<\varepsilon<\gamma/q$,

$$\frac{d}{d\varepsilon} P_{ud}(C,t,\varepsilon) > 0 . \tag{34}$$

Combining (32) and (34), we have

$$\frac{d}{d\varepsilon} P_{ud}(C,t,\varepsilon) > 0 , \tag{35}$$

for $0\leq t<d/2$ and $0<\varepsilon<(q-1)/q$.

Summarizing the above results, we have the following theorem.

Theorem: Consider a q-ary (n,k) MDS code C with minimum distance $d=n-k+1$. Let t be a nonnegative integer such that $t<d/2$. Suppose the code is used to correct t or fewer errors over a DMC with symbol error probability ε. Then the probability $P_{ud}(C,t,\varepsilon)$ of undetected error after decoding for the code decreases monotonically from

$$P(C,t,\frac{q-1}{q}) = \sum_{h=0}^{t} \binom{n}{h} \left[q^{-(n-k)}(q-1)^h - \varepsilon^h(1-\varepsilon)^{n-h}\right]$$

as ε decreases from $(q-1)/q$ to 0.

4. Conclusion

In this paper we have investigated the error-detection performance of maximum-distance-separable codes over a discrete memoryless channel with symbol error probability ε. We have shown that the probability of undetected error for these codes, no matter for pure error detection or for simultaneous error correction and detection, decreases monotonically from the value at the worst channel condition $\varepsilon = (q-1)/q$ as ε decreases from $(q-1)/q$ to 0. This behavior indicates that maximum-distance-separable codes are effective for pure error detection or simultaneous error correction and detection.

APPENDIX A

Derivation of (12)

Substituting (8) into (9), we have

$$A(X,Y) = \sum_{i=n-k+1}^{n} \binom{n}{i} q^{-(n-k)} \left[\gamma^i + \sum_{j=0}^{n-k} (-1)^{i+j} \binom{i}{j} (q^{n-k}-q^j) \right] X^i Y^{n-i}$$

$$= q^{-(n-k)} \left\{ \sum_{i=n-k+1}^{n} \binom{n}{i} (\gamma X)^i Y^{n-i} + F(X,Y) \right\}$$

$$= q^{-(n-k)} \left\{ (\gamma X+Y)^n - \sum_{i=0}^{n-k} \binom{n}{i} (\gamma X)^i Y^{n-i} + F(X,Y) \right\} \qquad \text{(A-1)}$$

where

$$F(X,Y) = \sum_{i=n-k+1}^{n} \sum_{j=0}^{n-k} (-1)^{i+j} \binom{n}{i} \binom{i}{j} (q^{n-k}-q^j) X^i Y^{n-i} \qquad \text{(A-2)}$$

Using the equality

$$\binom{n}{i}\binom{i}{j} = \binom{n}{j}\binom{n-j}{i-j} ,$$

we have

$$F(X,Y) = \sum_{i=n-k+1}^{n} \sum_{j=0}^{n-k} (-1)^{i+j} \binom{n}{j} \binom{n-j}{i-j} (q^{n-k}-q^j) X^i Y^{n-i}$$

$$= \sum_{j=0}^{n-k} \binom{n}{j} (q^{n-k}-q^j) X^j \sum_{i=n-k+1}^{n} (-1)^{i-j} \binom{n-j}{i-j} X^{i-j} Y^{n-j-(i-j)}$$

$$= \sum_{j=0}^{n-k} \binom{n}{j} (q^{n-k}-q^j) X^j \sum_{\ell=n-k+1-j}^{n-j} (-1)^{\ell} \binom{n-j}{\ell} X^{\ell} Y^{n-j-\ell}$$

$$= \sum_{j=0}^{n-k} \binom{n}{j} (q^{n-k}-q^j) X^j \left[(Y-X)^{n-j} - \sum_{\ell=0}^{n-k-j} (-1)^{\ell} \binom{n-j}{\ell} X^{\ell} Y^{n-j-\ell} \right]$$

$$= \sum_{j=0}^{n-k} \binom{n}{j} (q^{n-k}-q^j) X^j (Y-X)^{n-j}$$

$$- \sum_{j=0}^{n-k} \sum_{\ell=0}^{n-k-j} (-1)^{\ell} \binom{n}{j} \binom{n-j}{\ell} (q^{n-k}-q^j) X^{j+\ell} Y^{n-j-\ell}$$

$$= \sum_{j=0}^{n-k} \binom{n}{j} (q^{n-k}-q^j) X^j (Y-X)^{n-j} - \sum_{i=0}^{n-k} \sum_{j=0}^{i} (-1)^{i-j} \binom{n}{j} \binom{n-j}{i-j} (q^{n-k}-q^j) X^i Y^{n-i} \qquad \text{(A-3)}$$

Note that

$$\sum_{j=0}^{i} (-1)^{i-j}\binom{n}{j}\binom{n-j}{i-j}q^{j} = P_i(0) = \binom{n}{i}\gamma^{i} \qquad \text{(A-4)}$$

where $P_i(z)$ is the Krawtchouk polynomial [4, p. 151]. By letting q=1 in (A-4) which holds for any q, we have that

$$\sum_{j=0}^{i} (-1)^{i-j}\binom{n}{j}\binom{n-j}{i-j} = \begin{cases} 0, & \text{for } 1 \le i \le n \\ 1, & \text{for } i = 0 \end{cases} \qquad \text{(A-5)}$$

It follows from (A-3), (A-4) and (A-5) that

$$F(X,Y) = \sum_{j=0}^{n-k} \binom{n}{j}(q^{n-k}-q^{j})X^{j}(Y-X)^{n-j} + \sum_{i=0}^{n-k} \binom{n}{i}(\gamma X)^{i}Y^{n-i} - q^{n-k}Y^{n} \qquad \text{(A-6)}$$

Combining (A-1) and (A-6), we obtain the expression (12).

APPENDIX B

Derivation of (30)

From (21), we have

$$\frac{d}{d\varepsilon} P(C,t,\varepsilon) = \sum_{h=0}^{t} \frac{d}{d\varepsilon} P_h(\varepsilon) \tag{B-1}$$

Using the expression of (26) for $P_h(\varepsilon)$, we obtain

$$\begin{aligned}\frac{d}{d\varepsilon} P_h(\varepsilon) = &- \binom{n}{h} h\varepsilon^{h-1}(1-\varepsilon)^{n-h} + \binom{n}{h}(n-h)\varepsilon^{h}(1-\varepsilon)^{n-h-1}\\ &+ \binom{n}{h}\Bigg\{\frac{1}{\gamma}\sum_{\ell=0}^{\min(n-k-1,n-h)} \ell\binom{n-h}{\ell}\left(\frac{\varepsilon}{\gamma}\right)^{\ell-1}\left(1-\frac{q\varepsilon}{\gamma}\right)^{n-h-\ell}R_{h,\ell}(\varepsilon)\\ &- \frac{q}{\gamma}\sum_{\ell=0}^{\min(n-k-1,n-h)} (n-h-\ell)\binom{n-h}{\ell}\left(\frac{\varepsilon}{\gamma}\right)^{\ell}\left(1-\frac{q\varepsilon}{\gamma}\right)^{n-h-\ell-1}R_{h,\ell}(\varepsilon)\\ &+ \sum_{\ell=0}^{\min(n-k-1,n-h)} \binom{n-h}{\ell}\left(\frac{\varepsilon}{\gamma}\right)^{\ell}\left(1-\frac{q\varepsilon}{\gamma}\right)^{n-h-\ell} \frac{d}{d\varepsilon} R_{h,\ell}(\varepsilon) \Bigg\}\end{aligned} \tag{B-2}$$

Let

$$\begin{aligned} L_0(h,\varepsilon) &= n\binom{n-1}{h}\varepsilon^{h}(1-\varepsilon)^{n-1-h}, \quad \text{for } h \geq 0\\ L_0(-1,\varepsilon) &= 0\end{aligned} \tag{B-3}$$

Then

$$\begin{aligned}\frac{d}{d\varepsilon} P_h(\varepsilon) = &-L_0(h-1,\varepsilon) + L_0(h,\varepsilon)\\ &+ \binom{n}{h}\Bigg\{\frac{1}{\gamma}\sum_{\ell=1}^{\min(n-k-1,n-h)} \ell\binom{n-h}{\ell}\left(\frac{\varepsilon}{\gamma}\right)^{\ell-1}\left(1-\frac{q\varepsilon}{\gamma}\right)^{n-h-1-(\ell-1)}R_{h,\ell-1+1}(\varepsilon)\\ &- \frac{q}{\gamma}\sum_{\ell=0}^{\min(n-k-1,n-h-1)} (n-h-\ell)\binom{n-h}{\ell}\left(\frac{\varepsilon}{\gamma}\right)^{\ell}\left(1-\frac{q\varepsilon}{\gamma}\right)^{n-h-1-\ell}R_{h,\ell}(\varepsilon)\\ &+ \sum_{\ell=0}^{\min(n-k-1,n-h)} \binom{n-h}{\ell}\left(\frac{\varepsilon}{\gamma}\right)^{\ell}\left(1-\frac{q\varepsilon}{\gamma}\right)^{n-h-\ell} \frac{d}{d\varepsilon} R_{h,\ell}(\varepsilon)\Bigg\}\\ = &-L_0(h-1,\varepsilon) + L_0(h,\varepsilon)\\ &+ \binom{n}{h}(n-h)\Bigg[\frac{1}{\gamma}\sum_{\ell=0}^{\min(n-k-2,n-h-1)} \binom{n-h-1}{\ell}\left(\frac{\varepsilon}{\gamma}\right)^{\ell}\left(1-\frac{q\varepsilon}{\gamma}\right)^{n-h-1-\ell}R_{h,\ell+1}(\varepsilon)\end{aligned}$$

$$- \frac{q}{\gamma} \sum_{\ell=0}^{\min(n-k-1,n-h-1)} \binom{n-h-1}{\ell} \left(\frac{\varepsilon}{\gamma}\right)^{\ell} \left(1 - \frac{q\varepsilon}{\gamma}\right)^{n-h-1-\ell} R_{h,\ell}(\varepsilon) \Big]$$

$$+ \binom{n}{h} \sum_{\ell=0}^{\min(n-k-1,n-h)} \binom{n-h}{\ell} \left(\frac{\varepsilon}{\gamma}\right)^{\ell} \left(1 - \frac{q\varepsilon}{\gamma}\right)^{n-h-\ell} \frac{d}{d\varepsilon} R_{h,\ell}(\varepsilon) \qquad \text{(B-4)}$$

From (27) we can rewrite $R_{h,\ell}(\varepsilon)$ as follows:

$$R_{h,\ell}(\varepsilon) = \sum_{j=0}^{\min(n-k-\ell,h)} (-1)^{h-j} \binom{h}{j} (1 - q^{-n+k+\ell+j}) \left(1 - \frac{\varepsilon}{\gamma}\right)^{j} \left(1 - \frac{q\varepsilon}{\gamma}\right)^{h-j} \qquad \text{(B-5)}$$

Note that $R_{h,n-k}(\varepsilon) = 0$. Then (B-4) can be rewritten as follows:

$$\frac{d}{d\varepsilon} P_h(\varepsilon) = -L_0(h-1,\varepsilon) + L_0(h,\varepsilon)$$

$$- n\binom{n-1}{h} \sum_{\ell=0}^{\min(n-k-1,n-1-h)} \binom{n-1-h}{\ell} \left(\frac{\varepsilon}{\gamma}\right)^{\ell} \left(1 - \frac{q\varepsilon}{\gamma}\right)^{n-1-h-\ell} \Big[\frac{q}{\gamma} R_{h,\ell}(\varepsilon)$$

$$- \frac{1}{\gamma} R_{h,\ell+1}(\varepsilon)\Big]$$

$$+ \binom{n}{h} \sum_{\ell=0}^{\min(n-k-1,n-1-(h-1))} \binom{n-1-(h-1)}{\ell} \left(\frac{\varepsilon}{\gamma}\right)^{\ell} \left(1 - \frac{q\varepsilon}{\gamma}\right)^{n-1-(h-1)-\ell} \frac{d}{d\varepsilon} R_{h,\ell}(\varepsilon)$$

$$\text{(B-6)}$$

From (27) and (B-5) we have that

$$\frac{q}{\gamma} R_{h,\ell}(\varepsilon) - \frac{1}{\gamma} R_{h,\ell+1}(\varepsilon)$$

$$= \frac{q}{\gamma} \sum_{j=0}^{\min(n-k-1-\ell,h)} (-1)^{h-j} \binom{h}{j} (1 - q^{-n+k+\ell+j}) \left(1 - \frac{\varepsilon}{\gamma}\right)^{j} \left(1 - \frac{q\varepsilon}{\gamma}\right)^{h-j}$$

$$- \frac{1}{\gamma} \sum_{j=0}^{\min(n-k-1-\ell,h)} (-1)^{h-j} \binom{h}{j} (1 - q^{-n+k+\ell+j+1}) \left(1 - \frac{\varepsilon}{\gamma}\right)^{j} \left(1 - \frac{q\varepsilon}{\gamma}\right)^{h-j}$$

$$= \sum_{j=0}^{\min(n-k-1-\ell,h)} (-1)^{h-j} \binom{h}{j} \left(1 - \frac{\varepsilon}{\gamma}\right)^{j} \left(1 - \frac{q\varepsilon}{\gamma}\right)^{h-j} \qquad \text{(B-7)}$$

$$\frac{d}{d\varepsilon} R_{h,\ell}(\varepsilon) = -\frac{1}{\gamma} \sum_{j=0}^{\min(n-k-\ell,h)} (-1)^{h-j}\binom{h}{j} j(1-q^{-n+k+\ell+j})(1-\frac{\varepsilon}{\gamma})^{j-1}(1-\frac{q\varepsilon}{\gamma})^{h-j}$$

$$-\frac{q}{\gamma} \sum_{j=0}^{\min(n-k-1-\ell,h)} (-1)^{h-j}\binom{h}{j}(h-j)(1-q^{-n+k+\ell+j})(1-\frac{\varepsilon}{\gamma})^{j}(1-\frac{q\varepsilon}{\gamma})^{h-j-1}$$

$$= -\frac{1}{\gamma} \sum_{j=0}^{\min(n-k-\ell,h)} (-1)^{h-j} h\binom{h-1}{j-1}(1-q^{-n+k+\ell+j})(1-\frac{\varepsilon}{\gamma})^{j-1}(1-\frac{q\varepsilon}{\gamma})^{h-j}$$

$$-\frac{q}{\gamma} \sum_{j=0}^{\min(n-k-1-\ell,h)} (-1)^{h-j} h\binom{h-1}{j}(1-q^{-n+k+\ell+j})(1-\frac{\varepsilon}{\gamma})^{j}(1-\frac{q\varepsilon}{\gamma})^{h-j-1}$$

$$= -\frac{h}{\gamma} \sum_{j=0}^{\min(n-k-1-\ell,h-1)} (-1)^{h-1-j}\binom{h-1}{j}(1-q^{-n+k+1+\ell+j})(1-\frac{\varepsilon}{\gamma})^{j}(1-\frac{q\varepsilon}{\gamma})^{h-1-j}$$

$$+\frac{qh}{\gamma} \sum_{j=0}^{\min(n-k-1-\ell,h-1)} (-1)^{h-1-j}\binom{h-1}{j}(1-q^{-n+k+\ell+j})(1-\frac{\varepsilon}{\gamma})^{j}(1-\frac{q\varepsilon}{\gamma})^{h-1-j}$$

$$= h \sum_{j=0}^{\min(n-k-1-\ell,h-1)} (-1)^{h-1-j}\binom{h-1}{j}(1-\frac{\varepsilon}{\gamma})^{j}(1-\frac{q\varepsilon}{\gamma})^{h-1-j} \tag{B-8}$$

It follows from (B-3), (B-6), (B-7) and (B-8) that

$$\frac{d}{d\varepsilon} P_h(\varepsilon) = -L_0(h-1,\varepsilon) + L_0(h,\varepsilon) + L_1(h-1,\varepsilon) - L_1(h,\varepsilon) \tag{B-9}$$

where

$$L_1(h,\varepsilon) = n\binom{n-1}{h} \sum_{\ell=0}^{\min(n-k-1,n-1-h)} \binom{n-1-h}{\ell}(\frac{\varepsilon}{\gamma})^{\ell}(1-\frac{q\varepsilon}{\gamma})^{n-1-h-\ell} M_{h,\ell}(\varepsilon) \tag{B-10}$$

$$L_1(-1,\varepsilon) = 0 \tag{B-11}$$

$$M_{h,\ell}(\varepsilon) = \sum_{j=0}^{\min(n-k-1-\ell,h)} (-1)^{h-j}\binom{h}{j}(1-\frac{\varepsilon}{\gamma})^{j}(1-\frac{q\varepsilon}{\gamma})^{h-j} \tag{B-12}$$

From (21) and (B-9), we obtain

$$\frac{d}{d\varepsilon} P_{ud}(C,t,\varepsilon) = L_0(t,\varepsilon) - L_1(t,\varepsilon) \tag{B-13}$$

Combining (B-3), (B-10), (B-12) and (B-13), we have that

$$\frac{d}{d\varepsilon} P_{ud}(C,t,\varepsilon) = n\binom{n-1}{t}\left\{\varepsilon^{t} \sum_{\ell=n-k}^{n-1-t} \binom{n-1-t}{\ell}\left(\frac{\varepsilon}{\gamma}\right)^{\ell}\left(1-\frac{q\varepsilon}{\gamma}\right)^{n-1-t-\ell} + \sum_{\ell=0}^{\min(n-k-1,n-1-t)} \binom{n-1-t}{\ell}\left(\frac{\varepsilon}{\gamma}\right)^{\ell}\left(1-\frac{q\varepsilon}{\gamma}\right)^{n-1-t-\ell}\left[\varepsilon^{t}-M_{t,\ell}(\varepsilon)\right]\right\} \qquad \text{(B-14)}$$

Note that

$$\varepsilon^{t} - M_{t,\ell}(\varepsilon) = \begin{cases} 0\,, & \text{for } 0 \le \ell \le n-k-t-1\,, \\ \displaystyle\sum_{j=0}^{\ell-n+k+t} (-1)^{j}\binom{t}{j}\left(1-\frac{\varepsilon}{\gamma}\right)^{t-j}\left(1-\frac{q\varepsilon}{\gamma}\right)^{j}, & \text{otherwise.} \end{cases} \qquad \text{(B-15)}$$

From (B-14) and (B-15), we obtain the expression of (30).

APPENDIX C

Proof of (33)

For $n-k-t \leq \ell \leq \min(n-k-1, n-1-t)$ and $0 \leq j \leq \ell-n+k+t$, let

$$U_{t,\ell,j}(\varepsilon) = (-1)^j \binom{n-1-t}{\ell}\binom{t}{j}\left(\frac{\varepsilon}{\gamma}\right)^{\ell}\left(1-\frac{q\varepsilon}{\gamma}\right)^{n-1-t-\ell+j}\left(1-\frac{\varepsilon}{\gamma}\right)^{t-j} \qquad \text{(C-1)}$$

which is simply a term in the double summation of $N_t(\varepsilon)$ given by (31). Consequently,

$$\begin{aligned} N_t(\varepsilon) &= \sum_{\ell=n-k-t}^{\min(n-k-1,n-1-t)} \sum_{j=0}^{\ell-n+k+t} U_{t,\ell,j}(\varepsilon) \\ &= \sum_{i=0}^{\lfloor t/2 \rfloor -1} \sum_{\ell=n-k-t+2i}^{\min(n-k-2,n-2-t)} (U_{t,\ell,2i} + U_{t,\ell+1,2i+1}) \\ &\quad + \sum_{i=0}^{\lfloor (t-1)/2 \rfloor} U_{t,\min(n-k-1,n-1-t),2i}(\varepsilon) \end{aligned} \qquad \text{(C-2)}$$

where $\lfloor x \rfloor$ denotes the largest integer not greater than x. In the following, we want to show that, for $0<t<d/2$, $N_t(\varepsilon)>0$. Then, from (30), $\frac{d}{d\varepsilon} P_{ud}(C,t,\varepsilon) > 0$. First, we note that

$$U_{t,\ell,2i}(\varepsilon) > 0 \qquad \text{(C-3)}$$

for $0 < \varepsilon < \gamma/q$. For $n-k-t+2i \leq \ell < \min(n-k-1, n-1-t)$ and $0 \leq i \leq (t-1)/2$, we have

$$\begin{aligned} -\frac{U_{t,\ell+1,2i+1}(\varepsilon)}{U_{t,\ell,2i}(\varepsilon)} &= \frac{n-1-t-\ell}{\ell+1} \cdot \frac{t-2i}{2i+1} \cdot \frac{\varepsilon}{\gamma} \cdot \frac{1}{1-\frac{\varepsilon}{\gamma}} \\ &< \frac{(k-1)t}{(n-k-t)(q-1)} \\ &\leq \frac{k-1}{q-1} \end{aligned} \qquad \text{(C-4)}$$

for $0 < \varepsilon < \gamma/q$ and $0 < t < d/2$. For $d \geq 3$, since the code is a MDS code, we have

$$n-2 \geq k .$$

It follows from Corollary 7 [4, p. 321] that

$$q - 1 \geq k \ . \qquad \text{(C-5)}$$

From (C-4) and (C-5), we see that

$$U_{t,\ell,2i}(\varepsilon) + U_{t,\ell+1,2i+1}(\varepsilon) > 0 \qquad \text{(C-6)}$$

for $0 < \varepsilon < \gamma/q$. It follows from (C-2), (C-3) and (C-6) that

$$N_t(\varepsilon) > 0$$

for $0 < \varepsilon < \gamma/q$.

REFERENCES

1. W.W. Peterson and E.J. Weldon, Jr., Error-Correcting Codes, 2nd Ed., MIT Press, Cambridge, Mass., 1972.

2. S. Lin and D.J. Costello, Jr., Error Control Coding: Fundamentals and Applications, Prentice-Hall, New Jersey, 1983.

3. R.C. Singleton, "Maximum Distance q-nary Codes," IEEE Transactions on Information Theory, Vol. IT-10, pp. 116-118, 1964.

4. F.J. MacWilliams and N.J.A. Sloane, Theory of Error-Correcting Codes, North Holland, Amsterdam, 1977.

5. I.S. Reed and G. Solomon, "Polynomial Codes Over Certain Finite Fields," J. SIAM, 8, pp. 300-304, 1960.

6. T. Kasami, S. Lin and W.W. Peterson, "Some Results on Weight Distributions of BCH Codes," IEEE Transactions on Information Theory, Vol. IT-12, p. 274, 1966.

7. J.K. Wolf, "Adding Two Information Symbols to Certain Nonbinary BCH Codes and Some Applications, Bell System Technical Journal, No. 48, pp. 2405-2424, 1969.

8. E.R. Berlekamp, Algebraic Coding Theory, McGraw-Hill, New York, 1968.

9. J.K. Wolf, A.M. Michelson, and A.H. Levesque, "On the Probability of Undetected Error for Linear Block Codes," IEEE Transactions on Communications, Vol. COM-30, No. 2, pp. 317-324, February, 1982.

10. V.I. Korzhik, "Bounds on Undetected Error Probability and Optimum Group Codes in a Channel with Feedback," Radiotecknika, 20, Vol. 1, pp. 27-33, 1965. (English translation: Telecommunications and Radio Engineering, 2, pp. 87-92, January, 1965.)

11. S.K. Leung-Yan-Cheong and M.E. Hellman, "Concerning a Bound on Undetected Error Probability," IEEE Transactions on Information Theory, Vol. IT-22, No. 2, pp. 235-237, March, 1976.

12. S.K. Leung-Yan-Cheong, E.R. Barnes, and D.U. Friedman, "Some Properties of Undetected Error Probability of Linear Codes," IEEE Transactions on Information Theory, Vol. IT-25, No. 1, pp. 110-112, January 1979.

13. T. Kasami, T. Kløve, and S. Lin, "Error Detection with Linear Block Codes," IEEE Transactions on Information Theory, Vol. IT-29, No. 1, January, 1983.

14. E.F. Assmus, Jr., H.F. Mattson, Jr., and R.J. Turyn, Cyclic Codes, AFCRL-65-332, Air Force Cambridge Research Labs, Bedford, Mass., 1965.

15. G.D. Forney, Jr., Concatenated Codes, MIT Press, Cambridge, MA, 1966.

16. F.J. MacWilliams, "A Theorem on the Distribution of Weights in a Systematic Code," Bell System Technical Journal, No. 42, pp. 79-94, 1963.