A Lower Bound for the Decoder Error Probability of the Linear MDS Code

K.-M. Cheung
Communications Systems Research Section

In this article, a lower bound for the decoder error probability ($P_E[u]$) of a linear maximum distance separable (MDS) code is derived by counting the dominant types of decoding words around code words. It is shown that the lower bound derived in this article is similar in form, and close numerically, to the upper bound derived in [2].

I. Introduction

Let C be a linear code of length n, dimension k, and minimum distance d. Let q be a positive power of a prime. An (n,k,d) linear code C over $GF(q)$ is *maximum distance separable* (MDS) if the Singleton bound is achieved; that is, $d = n - k + 1$. A code is t-error correcting if for some integer t, $2t \leqslant d - 1$.

In [1], by repeated use of the inclusion and exclusion principle, an exact expression for D_u, the number of decodable words of weight u, is derived. Also in [1], the exact decoding error probability $P_E(u)$ of a linear MDS code is evaluated. However, the formulas derived in [1] are complicated and clumsy, and offer no mathematical insight. In this article, by assuming that $q \geqslant n$, the lower bounds of $P_E(u)$ and $D(u)$ are derived from a completely different approach—simply by counting the dominant types of decoding words around code words. In Sections II and III the lower bound derived in this article is shown to be similar in form, and close numerically, to the upper bound derived in [2]. In Section IV, with the assumption that $q \geqslant n$, the lower bound of $P_E(u)$ as a function of u is shown to achieve its minimum value at $u = d - t$. Thus, the lower bound for $u = d - t$ is the overall lower bound of $P_E(u)$. For $q < n$, this may not be true.

II. Lower Bound of the Number of Code Words of Weight w

Let A_w denote the number of code words of weight w. A lower bound of A_w is given by the following theorem:

Theorem 1:

$$A_w \geqslant C \binom{n}{w} q^{-d+1} (q-1)^w \qquad d \leqslant w \leqslant n \qquad (1)$$

where

$$C = 1 - \frac{\binom{d}{2} q^{d-2}}{(q-1)^d}$$

Proof: From [1], A_w is given by the following expression:

$$A_w = \binom{n}{w}(q-1)\sum_{i=0}^{w-d}(-1)^i\binom{w-1}{i}q^{w-d-i}$$

$$= \binom{n}{w}(q-1)q^{-d+1}\sum_{i=0}^{w-d}(-1)^i\binom{w-1}{i}q^{w-1-i}$$

$$= \binom{n}{w}(q-1)q^{-d+1}\left[(q-1)^{w-1} - \sum_{i=w-d+1}^{w-1}(-1)^i\binom{w-1}{i}q^{w-1-i}\right]$$

Consider the second term of the above expression. Since $q \geqslant n$,

$$\binom{w-1}{i}q^{w-1-i} \geqslant \binom{w-1}{i+1}q^{w-1-i-1}$$

for $d \leqslant w \leqslant n$ and $w-d+1 \leqslant i \leqslant w-1$. It is not hard to see that the following inequalities are obtained:

$$A_w \geqslant \binom{n}{w}q^{-d+1}(q-1)^w \tag{2}$$

$$A_w \leqslant \binom{n}{w}q^{-d+1}(q-1)^w\left[1+\frac{\binom{w-1}{w-d+1}q^{d-2}}{(q-1)^{w-1}}\right]$$

$$w = d, d+2, d+4, \ldots \tag{3}$$

and

$$A_w \leqslant \binom{n}{w}q^{-d+1}(q-1)^w \tag{4}$$

$$A_w \geqslant \binom{n}{w}q^{-d+1}(q-1)^w\left[1-\frac{\binom{w-1}{w-d+1}q^{d-2}}{(q-1)^{w-1}}\right]$$

$$w = d+1, d+3, d+5, \ldots \tag{5}$$

Consider the bracketed term in Eq. (5). Since $q \geqslant n$, it is an ascending function of w. So if we denote

$$C = \left[1-\frac{\binom{w-1}{w-d+1}q^{d-2}}{(q-1)^{w-1}}\right]_{w=d+1}$$

$$= 1-\frac{\binom{d}{2}q^{d-2}}{(q-1)^d}$$

we have

$$A_w \geqslant C\binom{n}{w}q^{-d+1}(q-1)^w \qquad d \leqslant w \leqslant n$$

where C is a scaling factor very close to 1. ■

III. Derivation of Lower Bound

Let $\bar{d}$ be a decodable word. Then $\bar{d}$ can be expressed uniquely as a sum $\bar{c}+\bar{e}$, where $\bar{c}$ is a code word and $\bar{e}$ is an error pattern of weight less than or equal to t. Let $\bar{d}$ have weight u and $\bar{e}$ have weight s, $s \leqslant t$. The weight of $\bar{c}$ is then confined within a certain set of values, depending on the value of u and s. The main idea of deriving the lower bound of the number of decodable words of weight u is to count a certain "dominant" subset of code words that, when added to appropriate error patterns, gives rise to decodable words of weight u. Let us define

$B_{u,s}$ = {w: w is the weight of a code word that is at a distance s from a decodable word of weight u}

We then have the following expression for $B_{u,s}$ depending on the value of u and s:

(1) If $d-t \leqslant u \leqslant d-1 \leqslant n-t$,
then $B_{u,s} = \{w: d \leqslant w \leqslant u+s\}$

(2) If $d \leqslant u \leqslant d+t-1 \leqslant n-t$,
then $B_{u,s} = \{w: d \leqslant w \leqslant u+s\}$

(3) If $d+t \leqslant u \leqslant n-t$,
then $B_{u,s} = \{w: u-s \leqslant w \leqslant u+s\}$

(4) If $n-t+1 \leqslant u \leqslant n$:

If $u+s \leqslant n$, then $B_{u,s} = \{w: u-s \leqslant w \leqslant u+s\}$

If $u+s > n$, then $B_{u,s} = \{w: u-s \leqslant w \leqslant n\}$

We can then express D_u as follows:

$$D_u = \sum_s \sum_{w \in B_{u,s}} A_w \times \{\#\text{ of error patterns of weight } s \text{ that give rise to a decodable word of weight } u \text{ from a code word of weight } w\} \quad (6)$$

We see that in the case $d - t \leqslant u \leqslant d - 1$, an allowable error pattern must be of weight $s \in \{d - u, \ldots, t\} \subset \{0, 1, \ldots, t\}$. In the case $d \leqslant u \leqslant n$, an allowable error pattern must be of weight $s \in \{0, 1, \ldots, t\}$.

We also observe that for a linear MDS code, if $q \geqslant n$ and q is large, then

$$\frac{A_w}{A_{w-1}} \gg 1 \qquad \text{for most } d \leqslant w \leqslant n$$

Thus, for the purpose of finding a lower bound of D_u, we do not need to consider all $w \in B_{u,s}$. We need only count those w's that give rise to most decodable words of weight u. It is then logical to consider only those $w \in B'_{u,s} \subseteq B_{u,s}$ where $B'_{u,s}$ is a subset of $B_{u,s}$ ($B'_{u,s}$ consists of the larger numbers in $B_{u,s}$), instead of all $w \in B_{u,s}$. We now define $B'_{u,s}$ as follows:

(1) If $d - t \leqslant u \leqslant d - 1 \leqslant n - t$,
then $B'_{u,s} = \{w : d \leqslant w \leqslant u + s\}$

(2) If $d \leqslant u \leqslant d + t - 1 \leqslant n - t$,
then $B'_{u,s} = \{w : u \leqslant w \leqslant u + s\}$

(3) If $d + t \leqslant u \leqslant n - t$
then $B'_{u,s} = \{w : u \leqslant w \leqslant u + s\}$

(4) If $n - t + 1 \leqslant u \leqslant n$:

If $u + s \leqslant n$, then $B'_{u,s} = \{w : u \leqslant w \leqslant u + s\}$

If $u + s > n$, then $B'_{u,s} = \{w : u \leqslant w \leqslant n\}$

Before we proceed, we want to categorize the decodable words according to the following definition.

Definition 1:

Let $\bar{d}$ be a decodable word which can be expressed in the form $\bar{d} = \bar{c} + \bar{e}$. Let $T_{\bar{c}}$ denote the set of nonzero coordinates of $\bar{c}$ and $T_{\bar{e}}$ denote the set of nonzero coordinates of $\bar{e}$.

(1) $\bar{d}$ is defined to be of type A if $T_{\bar{e}} \subset T_{\bar{c}}$.

(2) $\bar{d}$ is defined to be of type B if it is not of type A.

It can be shown that for a given u, the number of type-A decodable words of weight u is usually much greater than the number of type-B decodable words of weight u for most u. However, an explanation of the above claim is complicated and clumsy, and it is very hard to present a formal proof. A crude and oversimplified explanation is that type-A decodable words lie within Hamming spheres of code words of weights up to $u + t$, whereas type-B decodable words lie in the Hamming sphere of code words of weights only up to $u + t - 2$. As was mentioned before, $A_w \gg A_{w-1}$ for most w. This partly explains why the number of type-A decodable words is much greater than the number of type-B decodable words of weight u.

Summing up the above results, a lower bound of the number of decodable words of weight u is given by the following expression:

$$D_u \geqslant \sum_s \sum_{w \in B'_{u,s}} A_w \times \{\#\text{ of error patterns of weight } s \text{ that give rise to a type-A decodable word of weight } u \text{ from a code word of weight } w\} \quad (7)$$

We have four cases to consider, depending on the value of u.

(1) $d - t \leqslant u \leqslant d - 1$

In this case, $s \in \{d - u, \ldots, t\}$ and $w \in B'_{u,s} = \{d, d + 1, \ldots, u + s\}$. There are $\binom{w}{s}$ ways of choosing s coordinates that give rise to type-A decodable words. But in order to have a type-A decodable word of weight u, the $w - u$ nonzero coordinates in $\bar{c}$ must match with the corresponding $w - u$ nonzero coordinates in $\bar{e}$ to give $w - u$ zeros in these coordinates. The remaining $s - (w - u)$ coordinates of $\bar{e}$ must also match the corresponding $s - (w - u)$ coordinates of $\bar{c}$ to give a nonzero value in each of the $s - (n - w)$ coordinates. There are $(q - 2)^{s - (u - w)}$ ways to do so.

Thus, the number of decodable words of weight u, where $d - t \leqslant u \leqslant d - 1$, is lower bounded as follows:

$$D_u \geqslant \sum_{s=d-u}^{t} \sum_{w \in B'_{u,s}} A_w \binom{w}{s} \binom{s}{w-u} (q-2)^{s-(w-u)}$$

We then substitute the lower bound of A_w in Eq. (1) for the above expression, and we have a lower bound of D_u as follows:

$$D_u \geqslant \sum_{s=d-u}^{t} \sum_{w=d}^{u+s} C \binom{n}{w} q^{-d+1} (q-1)^w \times \binom{w}{s} \binom{s}{w-u} (q-2)^{s-(w-u)}$$

We see that

$$\binom{n}{w}\binom{w}{s}\binom{s}{w-u}$$

can be expressed as

$$\binom{n}{u}\binom{n-u}{w-u}\binom{u}{s-(w-u)}$$

Let $\lambda = w - u$. The above expression can be rewritten as

$$D_u \geqslant \sum_{s=d-u}^{t} \sum_{\lambda=d-u}^{s} C\left(\frac{q-1}{q}\right)^{d-1}\left(\frac{q-2}{q-1}\right)^{s-w+u}$$

$$\times \binom{n}{u}\binom{n-u}{\lambda}\binom{u}{s-\lambda}(q-1)^{u+s-d+1}$$

Next, it is not hard to see that for the given ranges of u, s and w,

$$\left(\frac{q-2}{q-1}\right)^{s-w+u} > \left(\frac{q-2}{q-1}\right)^{t}$$

Also, for the purpose of consistency with the equations that follow, the lower limit of the first summation on the RHS of the above expression can be replaced with 0 and thus our final expression is

$$D_u \geqslant C\left(\frac{q-1}{q}\right)^{d-1}\left(\frac{q-2}{q-1}\right)^{t}\binom{n}{u}(q-1)^{u-d+1}$$

$$\times \sum_{s=0}^{t} \sum_{\lambda=d-u}^{s} \binom{n-u}{\lambda}\binom{u}{s-\lambda}(q-1)^{s}$$

where

$$C = 1 - \frac{\binom{d}{2} q^{d-2}}{(q-1)^{d}}$$

(2) $d \leqslant u \leqslant d + t$

In this case $s \in \{0, 1, \ldots, t\}$ and $w \in \{u, u+1, \ldots, u+s\}$. The derivation of lower bound of the number of decodable words of weight u is very similar to case 1, and the details of derivation are omitted. Since the smallest value of the code word weights that are involved in counting is u, the scaling factor of the lower bound is now

$$C' = 1 - \frac{\binom{u-1}{u-d+1} q^{d-2}}{(q-1)^{u-1}}$$

which is closer to 1 than C. The lower bound of D_u is then given by

$$D_u \geqslant C'\left(\frac{q-1}{q}\right)^{d-1}\left(\frac{q-2}{q-1}\right)^{t}\binom{n}{u}(q-1)^{u-d+1}$$

$$\times \sum_{s=0}^{t} \sum_{\lambda=0}^{s} \binom{n-u}{\lambda}\binom{u}{s-\lambda}(q-1)^{s}$$

The lower bound can again be simplified by recalling the famous combinatoric identity

$$\sum_{\lambda=0}^{s} \binom{n-u}{\lambda}\binom{u}{s-\lambda} = \binom{n}{s}$$

and the final expression for this case is

$$D_u \geqslant C'\left(\frac{q-1}{q}\right)^{d-1}\left(\frac{q-2}{q-1}\right)^{t}\binom{n}{u}(q-1)^{u-d+1}$$

$$\times \sum_{s=0}^{t}\binom{n}{s}(q-1)^{s}$$

$$= C'\left(\frac{q-1}{q}\right)^{d-1}\left(\frac{q-2}{q-1}\right)^{t}\binom{n}{u}(q-1)^{u-d+1}$$

$$\times V_n(t) \qquad d \leqslant u \leqslant d+t$$

(3) $d + t + 1 \leqslant u \leqslant n - t$

In this case, $s \in \{0, \ldots, t\}$ and $w \in \{u, \ldots, u+s\}$. The derivation is exactly the same as in case 2, and the lower bound is given by

$$D_u \geqslant C'\left(\frac{q-1}{q}\right)^{d-1}\left(\frac{q-2}{q-1}\right)^{t}\binom{u}{u}(q-1)^{u-d+1}$$

$$\times V_n(t) \qquad d+t+1 \leqslant u \leqslant n-t$$

(4) $n - t + 1 \leqslant u \leqslant n$

In this case, if $u + s \leqslant n$ then $w \in \{u, \ldots, u + s\}$, and if $u + s > n$ then $w \in \{u, \ldots, n\}$. The derivation of the lower bound is slightly different from those of cases 2 and 3, but the final expression turns out to be the same. That is,

$$D_u \geqslant C' \left(\frac{q-1}{q}\right)^{d-1} \left(\frac{q-2}{q-1}\right)^{t} \binom{n}{u} (q-1)^{u-d+1} \times V_n(t) \qquad n - t + 1 \leqslant u \leqslant n$$

In summary, the lower bound of the number of decodable words is given by the following equations:

$$D_u \geqslant C \left(\frac{q-1}{q}\right)^{d-1} \left(\frac{q-2}{q-1}\right)^{t} \binom{n}{u} (q-1)^{u-d+1} \times \sum_{s=0}^{t} \sum_{\lambda=d-u}^{s} \binom{n-u}{\lambda} \binom{u}{s-\lambda} (q-1)^{s}$$

$$d - t \leqslant u \leqslant d - 1 \tag{8}$$

$$D_u \geqslant C' \left(\frac{q-1}{q}\right)^{d-1} \left(\frac{q-2}{q-1}\right)^{t} \binom{n}{u} (q-1)^{u-d+1} \times V_n(t) \qquad n - t + 1 \leqslant u \leqslant n \tag{9}$$

where

$$C = 1 - \frac{\binom{d}{2} q^{d-2}}{(q-1)^{d}}$$

and

$$C' = 1 - \frac{\binom{u-1}{u-d+1} q^{d-2}}{(q-1)^{u-1}}$$

We have shown in [1] that the decoder error probability is related to the number of decodable words via Eq. (2) and thus the decoder error probability $P_E(u)$ is lower bounded as follows:

$$P_E(u) \geqslant C q^{-d+1} \left(\frac{q-2}{q-1}\right)^{t} \sum_{s=0}^{t} \sum_{\lambda=d-u}^{s} \binom{n-u}{\lambda} \binom{u}{s-\lambda} (q-1)^{s}$$

$$d - t \leqslant u \leqslant d - 1 \tag{10}$$

$$P_E(u) \geqslant C' q^{-d+1} \left(\frac{q-2}{q-1}\right)^{t} V_n(t) \qquad d \leqslant u \leqslant n \tag{11}$$

where

$$C = 1 - \frac{\binom{d}{2} q^{d-2}}{(q-1)^{d}}$$

and

$$C' = 1 - \frac{\binom{u-1}{u-d+1} q^{d-2}}{(q-1)^{u-1}}$$

IV. Overall Lower Bound of $P_E(u)$

In this section, an overall lower bound of $P_E(u)$ for all u is given by the following theorem and corollary.

Theorem 2:

If $q \geqslant n$, then the lower bound of $P_E(u)$ in Eqs. (10) and (11) is smallest for $u = d - t$.

Proof: First of all, it is not hard to see that the lower bound in Eq. (10) is always smaller than the lower bound in Eq. (11) because $\binom{n}{s}$ is always greater than the incomplete Vandermonde convolution $\sum_{\lambda=d-u}^{t} \binom{n-u}{\lambda} \binom{u}{t-\lambda}$. Also, the scaling factor C' in Eq. (11) is always greater than the scaling factor C in Eq. (10). Thus, to prove the theorem, we need only consider the lower bound of $P_E(u)$ for $d - t \leqslant u \leqslant d - 1$. It is not hard to see that a sufficient condition is to show that

$$\sum_{s=0}^{t} \sum_{\lambda=d-u}^{s} \binom{n-u}{\lambda} \binom{u}{s-\lambda} (q-1)^{s} \geqslant \binom{n-d+t}{t} (q-1)^{t}$$

$$d - t \leqslant u \leqslant d - 1$$

It is obvious that

$$\sum_{s=0}^{t} \sum_{\lambda=d-u}^{s} \binom{n-u}{\lambda} \binom{u}{s-\lambda} (q-1)^{s} \geqslant \sum_{\lambda=d-u}^{t} \binom{n-u}{\lambda} \binom{u}{t-\lambda} (q-1)^{t}$$

We now proceed to show that

$$\sum_{\lambda=d-u}^{t} \binom{n-u}{\lambda}\binom{u}{t-\lambda}(q-1)^t \geq \binom{n-d+t}{t}(q-1)^t$$

Let $l = t - d + u$ and $m = t - \lambda$; we have

$$\sum_{\lambda=d-u}^{t} \binom{n-u}{\lambda}\binom{u}{t-\lambda}(q-1)^t = \sum_{m=0}^{l} \binom{n-d+t-l}{t-m} \times \binom{d-t+l}{m}(q-1)^t$$

Since $d \geq 2t + 1$ and $0 \leq l \leq t - 1$,

$$\binom{d-t+l}{m} \geq \binom{l}{m}$$

Thus,

$$\sum_{m=0}^{l} \binom{n-d+t-l}{t-m}\binom{d-t+l}{m}(q-1)^t$$

$$\geq \sum_{m=0}^{l} \binom{n-d+t-l}{t-m}\binom{l}{m}(q-1)^t = \binom{n-d+t}{t}(q-1)^t$$

and the theorem is proved. ■

Corollary:

An overall lower bound of $P_E(u)$ for all u is

$$P_E(u) \leq C\left(\frac{q-2}{q-1}\right)^t \left(\frac{q-1}{q}\right)^{d-1} P_E(d-t)$$

$$= C\left(\frac{q-2}{q-1}\right)^t q^{-d+1}\binom{n-d+t}{t}(q-1)^t$$

where

$$C = 1 - \frac{\binom{d}{2}q^{d-2}}{(q-1)^d}$$

Proof: A direct result from Theorem 2. ■

V. Remarks

For $q \geq n$, the upper bound and lower bound of $P_E(u)$ give a good estimation of $P_E(u)$. The upper bounds [2], lower bounds, and exact values of the $P_E(u)$'s of the NASA code and the JTIDS code are tabulated in Table 1 and Table 2, respectively. We observe that the estimated values (upper bound and lower bound) are more or less of the same order of magnitude as the exact value in each case.

Also, we have shown that with the assumption that $q \geq n$, an overall lower bound of $P_E(u)$ (for all u) is given by

$$C\left(\frac{q-2}{q-1}\right)^t P_E(d-t)$$

For $q < n$, this may not be true.

References

[1] K.-M. Cheung, "More on the Decoder Error Probability for Reed-Solomon Codes," *TDA Progress Report 42-91*, vol. July–September 1987, Jet Propulsion Laboratory, Pasadena, California, pp. 213–221, November 15, 1987.

[2] R. J. McEliece and L. Swanson, "On the Decoder Error Probability for Reed-Solomon Codes," *IEEE Tran. Inform. Theory*, vol. IT-32, pp. 701–703, 1986.

Table 1. Decoder error probability of the NASA code*

Weight	Lower bound	Actual value	Upper bound
17	7.769×10^{-15}	9.464×10^{-15}	2.956×10^{-14}
18	1.665×10^{-14}	1.913×10^{-14}	2.957×10^{-14}
19	2.171×10^{-14}	2.401×10^{-14}	2.957×10^{-14}
20	2.361×10^{-14}	2.660×10^{-14}	2.957×10^{-14}
21	2.414×10^{-14}	2.602×10^{-14}	2.957×10^{-14}
22	2.425×10^{-14}	2.608×10^{-14}	2.957×10^{-14}
.	.	.	.
.	.	.	.
.	.	.	.
37	2.450×10^{-14}	2.609×10^{-14}	2.957×10^{-14}
.	.	.	.
.	.	.	.

*NASA code (255, 223); $q = 256$; $t = 16$.

Table 2. Decoder error probability of the JTIDS code*

Weight	Lower bound	Actual value	Upper bound
9	1.340×10^{-6}	3.750×10^{-6}	9.250×10^{-6}
10	5.741×10^{-6}	1.439×10^{-6}	9.349×10^{-6}
11	1.310×10^{-6}	2.951×10^{-6}	9.350×10^{-6}
12	2.123×10^{-6}	4.329×10^{-6}	9.350×10^{-6}
13	2.767×10^{-6}	5.189×10^{-6}	9.350×10^{-6}
14	3.140×10^{-6}	5.547×10^{-6}	9.350×10^{-6}
.	.	.	.
.	.	.	.
.	.	.	.
25	4.328×10^{-6}	5.626×10^{-6}	9.350×10^{-6}
.	.	.	.
.	.	.	.

*RS code (31, 15); $q = 32$; $t = 8$.