More on the Decoder Error Probability for Reed-Solomon Codes

K.-M. Cheung
Communications Systems Research Section

This article is an extension of a recent paper by McEliece and Swanson dealing with the decoder error probability for Reed-Solomon codes (more generally, linear MDS codes). McEliece and Swanson offered an upper bound on $\mathrm{P_E}(\mathrm{u})$*, the decoder error probability given that* u *symbol errors occur. This upper bound is slightly greater than* Q*, the probability that a completely random error pattern will cause decoder error. In this article, by using a combinatoric technique–the principle of inclusion and exclusion–an exact formula for* $\mathrm{P_E}(\mathrm{u})$ *is derived.*

The $\mathrm{P_E}(\mathrm{u})$*'s for the (255, 223) Reed-Solomon Code used by NASA, and for the (31,15) Reed-Solomon code (JTIDS code), are calculated using the exact formula, and the* $\mathrm{P_E}(\mathrm{u})$*'s are observed to approach the* Q*'s of the codes rapidly as* u *gets large. An upper bound for the expression* $|[\mathrm{P_E}(\mathrm{u})/\mathrm{Q}] - 1|$ *is derived, and is shown to decrease nearly exponentially as* u *increases. This proves analytically that* $\mathrm{P_E}(\mathrm{u})$ *indeed approaches* Q *as* u *becomes large, and some laws of large numbers come into play.*

I. Weight Distribution Formula for Decodable Words in a Linear MDS Code

A. Introduction

We begin with the following definitions. 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, $2t \leqslant d - 1$.

The class of Reed-Solomon (RS) codes is a subclass of MDS codes. Reed-Solomon codes are used in many sectors of today's industry. Some examples are the (255, 223) 16-error correcting RS code (the NASA code) in deep space communications, the (31,15) 8-error correcting RS code (the JTIDS code) in military communications, and the Cyclic Interleaving RS Code (CIRC) in the compact disc industry. A detailed treatment of MDS codes, their properties and open questions about them is given in [1]. The weight distribution of a linear MDS code with the parameters n, k, d, t, and q was independently found by three groups of researchers: Assmus, Mattson and Turyn [2], Forney [3], and Kasami, Lin and Peterson [4].

In Section I, we rederive the weight distribution formula for a linear MDS code by using the principle of inclusion and exclusion, and then extend this method to obtain the exact weight distribution formula for "decodable words" in any linear MDS code. By decodable words, we mean all the words that lie within distance t from a codeword. If we assume the decoder to be a bounded distance decoder, then the weight distribution formula for the decodable words can be used to find the undetected error probability for linear MDS codes. This will be discussed in detail in Section II.

Section I is divided into 5 parts. Part I.A is a brief introduction. In I.B, we review some basic mathematical tools that are needed to derive the formulae. In I.C, we first derive the weight distribution formula for the number of codewords in a linear MDS code, and then we derive the weight distribution formula for the number of decodable words in a linear MDS code. In I.D, we give some numerical examples, and finally, in I.E, we end Section I of this article with some concluding remarks.

B. Some Basic Tools

In this part, we review the basic tools that are required to derive the weight distribution formulae for the number of codewords in a linear MDS code and for the number of decodable words in a linear MDS code.

Let C be an (n, k) code over $GF(q)$, not necessarily linear. If we examine any set of $k - 1$ components of the codewords, we find that there are only q^{k-1} possibilities for the q^k codewords. Thus, there must be a pair of codewords that agree on these $k - 1$ components, and so the minimum distance d of the code must satisfy $d \leqslant n - k + 1$. This upper bound on d is known as the Singleton bound, and a code for which $d = n - k + 1$ is called an MDS code. RS codes and cosets of RS codes are examples of MDS codes.

One important tool that we need is the basic combinatoric property of the MDS code. Let K be a subset of k coordinate positions of an MDS code. If two codewords were equal on K, the distance between them would be at most $n - k$. This contradicts the fact that $d = n - k + 1$. Thus, all q^k codewords are different in K. Let $\alpha = (\alpha_1, \alpha_2, \cdots, \alpha_k)$ be a k-tuple of elements from $GF(q)$. From the above argument, there exists a unique codeword whose k coordinates in K equal the k components of α. We call this important fact the basic combinatorial property of MDS codes.

Another important tool that we need is the principle of inclusion and exclusion [5]. Suppose we have N objects and a number of properties $P(1), \cdots, P(n)$. Let N_i be the number of objects with property $P(i)$, and $N_{i_1, i_2, \cdots, i_r}$ be the number of objects with properties $P(i_1), P(i_2), \cdots, P(i_r)$. The number of objects $N(0)$ with none of the properties is given by the following formula:

$$N(0) = N - \sum_{i} N_i + \sum_{i_1 < i_2} N_{i_1 i_2} + \cdots + (-1)^r \times \sum_{i_1 < i_2 \cdots < i_r} N_{i_1 i_2 \cdots i_r} + \cdots + (-1)^n N_{1 2 3 \cdots n} \qquad (1)$$

The proof can be found in [5].

The basic combinatorial property of MDS codes and the principle of inclusion and exclusion will be referred to in the proofs in later sections.

C. Derivation of Formulae

This part is divided into three subparts. In the first, we derive the formula for the number of codewords of weight u in a linear MDS code, using the principle of inclusion and exclusion. In the second, we extend this idea by deriving a general formula for the number of decodable words of weight u. Last of all, in the third, we simplify the key formula by using some combinatoric identities.

1. **Formula for the number of codewords of weight u.** Let $\bar{c}$ be some codeword of C. Let $\bar{c}$ have a Hamming weight u, $u \geqslant d$. Let the coordinates of codeword $\bar{c}$ be indexed by $\{0, 1, 2, \cdots, n - 1\}$. Define $v = n - u$. Then $\bar{c}$ has v zeros. We now want to find the number of codewords of weight u in C having exactly v zeros at some particular v coordinates where $v = n (u = 0)$ or $v \leqslant n - d = k - 1 (u \geqslant d)$. Since the code is linear, the number of codewords of weight zero ($u = 0$) is one—the all zero codeword. The following discussion applies only to codewords with weight $u \geqslant d$.

Let V be a set of v coordinates, $|V| = v$. Let $\{i_1, i_2, \cdots, i_j\} \subset \{1, 2, \cdots, n\} - V$ be a set of j coordinates. Define $S(i_1, i_2, \cdots, i_j) = \{\bar{c} : \bar{c} \in C$ and $\bar{c}$ has zeros in V and $\{i_1, i_2, \cdots, i_j\}\}$. For $j \leqslant k - v$, the number of zeros in a codeword in $S(i_1, i_2, \cdots, i_j)$ is at least $j + v \leqslant k (j + v \leqslant k)$. By using the basic combinatorial property of MDS code, for each particular choice of $\{i_1, i_2, \cdots, i_j\}$ we can specify q^{k-v-j} codewords having zeros at V and $\{i_1, i_2, \cdots, i_j\}$. So

$$|S(i_1, i_2, \cdots, i_j)| = q^{k-v-j} \qquad 0 \leqslant j \leqslant k - v \qquad (2)$$

For $j \geqslant k - v + 1$, the number of zeros in a codeword is $j + v \geqslant k + 1$. This implies that the weight of the codeword is less than d, so $S(i_1, i_2, \cdots, i_j) = \{\bar{0}\}$. That is,

$$|S(i_1, i_2, \cdots, i_j)| = 1 \qquad k - v + 1 \leqslant j \leqslant u \qquad (3)$$

Note that we choose $i_1, i_2, \cdots, i_j$ from a set of $u = n - v$ coordinates so that for every choice of j, we have $\binom{u}{j} S(i_1, i_2, \cdots, i_j)$'s.

By the principle of inclusion and exclusion, the number of codewords with exactly v zeros at V equals

$$|S(0)| - \sum_{i_1} |S(i_1)| + \cdots + (-1)^u |S(i_1, i_2, \cdots, i_u)|$$

$$= \sum_{j=0}^{k-v-1} (-1)^j \binom{u}{j} q^{k-v-j} + \sum_{j=k-v}^{u} (-1)^j \binom{u}{j}$$

$$= \sum_{j=0}^{u-d} (-1)^j \binom{u}{j} q^{u-d-j+1} - \sum_{j=0}^{u-d} .(-1)^j \binom{u}{j}$$

$$= \sum_{j=0}^{u-d} (-1)^j \binom{u}{j} (q^{u-d-j+1} - 1)$$

We have $\binom{n}{v} = \binom{n}{u}$ ways to choose v zeros from $\{0, 1, 2, \cdots, n - 1\}$. Thus, the number of codewords of weight u, which is denoted by A_u, is given by the following expression:

$$A_u = \binom{n}{u} \sum_{j=0}^{u-d} (-1)^j \binom{u}{j} (q^{u-d-j+1} - 1) \qquad d \leqslant u \leqslant n \tag{4}$$

After deriving this relatively simple formula for the number of codewords of weight u in a linear MDS code, we proceed to derive the more complicated formula for the number of decodable words of weight u in a linear MDS code.

2. General formula for the number of decodable words of weight u. Let D be the set of decodable words in an MDS code. Let V be a set of v coordinates, $|V| = v$. Let $\{i_1, i_2, \cdots, i_j\}$ be a set of j coordinates, where $\{i_1, i_2, \cdots, i_j\} \subset \{0, 1, 2, \cdots, n - 1\} - V$. Define $S(i_1, i_2, \cdots, i_j) = \{\bar{d} : \bar{d} \in D$ and $\bar{d}$ has zeros in V and $\{i_1, i_2, \cdots, i_j\}\}$. We proceed to derive the weight distribution formula for the number of decodable words of weight u in a linear MDS code by using the principle of inclusion and exclusion. Our problem is now reduced to finding the cardinality of $S(i_1, i_2, \cdots, i_j)$ for all j subjected to a given V. This problem is solved with the help of the following theorems.

Theorem 1:

$$|S(i_1, i_2, \cdots, i_j)| = q^{u-d+1-j} V_n(t) \qquad 0 \leqslant j \leqslant u - d \tag{5}$$

where

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

Proof: The argument here is similar to the derivation given in I.C.1, above. We note that each coset of a linear MDS code is also an MDS code. Also, since all words lying within the Hamming spheres (with volume $V_n(t)$) that surround codewords are decodable words, we have $V_n(t)$ disjoint cosets that contain decodable words. From the basic combinatorial property of the MDS code we can, for each particular choice of $\{i_1, i_2, \cdots, i_j\}$, specify $q^{k-v-j} = q^{u-d+1-j}$ decodable words to each of these cosets. Thus, we have altogether $q^{u-d+1-j} V_n(t)$ decodable words having zeros at V and $\{i_1, i_2, \cdots, i_j\}$. This completes the proof. ■

Theorem 2:

$$|S(i_1, i_2, \cdots, i_j)| = \sum_{w=d-u+j}^{t} \binom{n-u+j}{w} \times \sum_{i=0}^{w-d+u-j} (-1)^i \binom{w}{i} (q^{w-d+u-j-i+1} - 1) \times \sum_{s=w}^{t} \binom{u-j}{s-w} (q-1)^{s-w} + \sum_{i=0}^{t} \binom{u-j}{i} (q-1)^i \tag{6}$$

for $u - d + 1 \leqslant j \leqslant u - d + t$.

Proof: For $u - d + 1 = k - v \leqslant j$, the number of zeros in a decodable word is equal to $v + j \geqslant k$. Since $\bar{d}$ is a decodable word, $\bar{d}$ can be uniquely decomposed into a codeword $\bar{c}$ and an error pattern $\bar{e}$ with weight that is less than or equal to t. If we "project" $\bar{c}$ onto $V \cup \{i_1, i_2, \cdots, i_j\}$, then the result will be a certain $(v + j, k)$ code. Since the parent code has a minimum distance $d = n - k + 1$, the new code must have a minimum distance $d' \geqslant d - (n - v - j) = (v + j) - k + 1$. Since it is impossible for d' of the $(v + j, k)$ code to be greater than

$(v + j) - k + 1$ (because of the Singleton bound), d' must be equal to $d - (n - v - j) = (v + j) - k + 1$.

If $\bar{c} + \bar{e}$ vanishes on $V \cup \{i_1, i_2, \cdots, i_j\}$, then $\bar{c}$ must have weight that is less than or equal to t on $V \cup \{i_1, i_2, \cdots, i_j\}$. Let w be the weight of $\bar{c}$ on $V \cup \{i_1, i_2, \cdots, i_j\}$. From the above argument we also know that C, when restricted to $V \cup \{i_1, i_2, \cdots, i_j\}$, is a linear $(v + j, k)$ MDS code with a minimum distance $d - (n - v - j) = (v + j) - k + 1$. Thus, w is either 0 (in the case of the all-zero codeword) or between $d - u + j$ and t. So the number of codewords of weight w in the $(v + j, k)$ MDS code is (by using Eq. (4))

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

for $d - u + j \leqslant w \leqslant t$ and 1 for $w = 0$. For each codeword $\bar{c}$ with weight w in $V \cup \{i_1, i_2, \cdots, i_j\}$, where $d' \leqslant w \leqslant t$ ($d' = v + j - k + 1$), we must count the number of $\bar{e}$'s such that $\bar{c} + \bar{e}$ vanishes on $V \cup \{i_1, i_2, \cdots, i_j\}$. Suppose that $\bar{e}$ has weight $s \geqslant w$. $\bar{e}$ must match $\bar{c}$ exactly on $V \cup \{i_1, i_2, \cdots, i_j\}$, but the $s - w$ other nonzero components can be arbitrarily placed outside $V \cup \{i_1, i_2, \cdots, i_j\}$. Then the total number of $\bar{e}$'s for a given $\bar{c}$ of weight w on $V \cup \{i_1, i_2, \cdots, i_j\}$ is

$$\sum_{s=w}^{t} \binom{u-j}{s-w} (q-1)^{s-w}$$

When $w = 0$, all components of $\bar{e}$ must lie outside the set $V \cup \{i_1, i_2, \cdots, i_j\}$. So there are

$$\sum_{i=0}^{t} \binom{u-j}{i} (q-1)^i$$

$\bar{e}$'s for the case $w = 0$. Combining the above results, we obtain the theorem. ■

Theorem 3:

$$|S(i_1, i_2, \cdots, i_j)| = \sum_{i=0}^{t} \binom{u-j}{i} (q-1)^i \qquad (7)$$

for $u - d + t + 1 \leqslant j \leqslant u - t - 1$.

Proof: For $k - v + t \leqslant j \leqslant u - t - 1$, the number of zeros in a decodable word is greater than or equal to $k + t$ but less than or equal to $n - t - 1$. Thus any decodable words in $S(i_1, i_2, \cdots, i_j)$ have weight that is less than or equal to $d - t - 1$. It is not hard to see that the element of $S(i_1, i_2, \cdots, i_j)$ cannot be decoded into a codeword of weight other than $\bar{0}$. Therefore, $S(i_1, i_2, \cdots, i_j)$ contains all words having weight that is less than or equal to t in the coordinates $\{0, 1, \cdots, n-1\} - (V \cup \{i_1, i_2, \cdots, i_j\})$. This completes the proof. ■

Theorem 4:

$$|S(i_1, i_2, \cdots, i_j)| = q^{u-j} \qquad \text{for } u - t \leqslant j \leqslant u \qquad (8)$$

Proof: Since j is greater than or equal to $u - t$, the number of zeros is equal to $v + j$ and is greater than or equal to $n - t$. Therefore, the number of nonzero components is less than or equal to t. Thus, all words with zeros on $V \cup \{i_1, i_2, \cdots, i_j\}$ are decodable and this completes the proof. ■

As in I.C.1, we choose $i_1, i_2, \cdots, i_j$ from $v = n - u$ coordinates. Thus, for every choice of j, we have $\binom{u}{j} S(i_1, i_2, \cdots, i_j)$'s. Denote $N_j = \binom{u}{j} \; | S(i_1, i_2, \cdots, i_j) |$. Again, by the principle of inclusion and exclusion, we see that the number of decodable words which have exactly $v = n - u$ zeros at V equals

$$\sum_{j=0}^{u} (-1)^j N_j$$

However, we have $\binom{n}{u} = \binom{n}{v}$ ways to choose v zeros from $0, 1, \cdots, n-1$. Thus, the number of decodable words of weight u is given by

$$D_u = \binom{n}{u} \sum_{j=0}^{u} (-1)^j N_j \qquad \text{for } d - t \leqslant u \leqslant n \qquad (9)$$

3. Simplification of the key formula. The weight enumerator formula that we have just derived is complicated and clumsy. There are four different expressions for N_j's, and these expressions are combined together by the inclusion and exclusion formula. The following theorem will show that the weight distribution formula for the number of decodable words in a linear MDS code can be simplified, and that there are only two expressions for the N_j's.

Theorem 5:

$$A = \sum_{j=0}^{u-t-1} (-1)^j \binom{u}{j} \sum_{i=0}^{t} \binom{u-j}{i} (q-1)^i + \sum_{j=u-t}^{u} (-1)^j \binom{u}{j} q^{u-j} = 0 \qquad (10)$$

Proof:

$$A = \sum_{j=0}^{u-t-1} (-1)^j \binom{u}{j} \left[q^{u-j} - \sum_{i=t+1}^{u-j} \binom{u-j}{i} (q-1)^i \right]$$

$$+ \sum_{j=u-t}^{u} (-1)^j \binom{u}{j} q^{u-j}$$

$$= \sum_{j=0}^{u} (-1)^j \binom{u}{j} q^{u-j}$$

$$- \sum_{j=0}^{u-t-1} (-1)^j \binom{u}{j} \sum_{i=t+1}^{u-j} \binom{u-j}{i} (q-1)^i$$

$$= (q-1)^u - \sum_{i=t+1}^{u} (q-1)^i \sum_{j=0}^{u-i} \binom{u-j}{i} \binom{u}{j} (-1)^j$$

$$= (q-1)^u - (q-1)^u$$

$$- \sum_{i=t+1}^{u-1} (q-1)^i \sum_{j=0}^{u-i} \binom{u-j}{i} \binom{u}{j} (-1)^j$$

Notice that

$$\binom{u}{j} \binom{u-j}{i} = \binom{u}{i} \binom{u-i}{j}$$

and

$$\sum_{j=0}^{u-i} \binom{u-i}{j} (-1)^j = 0$$

then

$$\sum_{j=0}^{u-i} \binom{u-j}{i} \binom{u}{j} (-1)^j = \binom{u}{i} \sum_{j=0}^{u-i} \binom{u-i}{j} (-1)^j = 0$$

for $t + 1 \leqslant i \leqslant u - 1$.

Thus, $A = 0$ and the theorem is proved. ■

With Theorem 5 and Eqs. (5), (6), (7), (8), and (9), the weight enumerator formula can be simplified as follows:

$$D_u = \binom{n}{u} \sum_{j=0}^{u-d+t} (-1)^j N_j \tag{11}$$

for $d - t \leqslant u \leqslant n$

$$N_j = \binom{u}{j} \left[q^{u-d+1-j} V_n(t) - \sum_{i=0}^{t} \binom{u-j}{i} (q-1)^i \right] \tag{12}$$

for $0 \leqslant j \leqslant u - d$

$$N_j = \binom{u}{j} \left[\sum_{w=d-u+j}^{t} \binom{n-u+j}{w} \right.$$

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

$$\left. \times \sum_{s=w}^{t} \binom{u-j}{s-w} (q-1)^{s-w} \right] \tag{13}$$

for $u - d + 1 \leqslant j \leqslant u - d + t$.

Examples will be found in Tables 1 and 2.

D. Remarks

The formula for the number of decodable words of weight u, where $d - t \leqslant u \leqslant n$, has been derived in the previous parts of this section. If we set $t = 0$, then we get back the weight enumerator for linear MDS code–Eq. (4). In the case of $u = d - t$, for example, we have

$$D_{d-t} = \binom{n}{d} \binom{d}{t} (q-1)$$

and the answer is consistent with the result derived in [6].

The formula is a bit clumsy, but can be easily implemented by computer program.

II. Decoder Error Probability of a Linear MDS Code

A. Number of Decodable Words vs. Decoder Error Probability

Let C be an (n, k, d) linear code capable of correcting t errors. When a codeword $\bar{c} \in C$ is transmitted over a communication channel, channel noise may corrupt the transmitted signals. As a result, the receiver receives the corrupted version of the transmitted codeword $\bar{c} + \bar{e}$, where $\bar{e}$ is an error pattern of some weight u. If $u \leqslant t$, then a bounded distance decoder on the receiver's end detects and corrects the error $\bar{e}$ and recovers $\bar{c}$. If $u > t$, then the decoder fails and does one of two things:

(1) It detects the presence of the error pattern but is unable to correct it.

(2) It misinterprets (miscorrects) the received pattern $\bar{c} + \bar{e}$ for some other codeword $\bar{c}'$ if the received pattern falls into the radius t Hamming sphere of $\bar{c}'$.

Case (2) is, in most cases, more serious than case (1). This can occur (with a nonzero probability) when an error pattern $\bar{e}$ is of weight $u \geqslant d - t$. Let us further assume that all error patterns of weight u are equally probable, and let us use $P_E(u)$ [7] to denote the decoder error probability given that an error pattern of weight u occurs. It is not hard to see that $P_E(u)$ is given by the following expression:

$$P_E(u) = \frac{D_u}{\binom{n}{u}(q-1)^u} \qquad \text{for } d - t \leqslant u \leqslant n \qquad (14)$$

That is, $P_E(u)$ is the ratio of the number of decodable words of weight u to the number of words of weight u in the whole vector space. Thus, the problem of finding the $P_E(u)$'s is essentially the same as the problem of finding the weight distribution of the set of decodable words. Equations (11), (12) and (13) of Section I and Eq. (14) of Section II together enable us to find the exact decoder error probability of a linear MDS code.

Let the probability that a completely random error pattern will cause decoder error be denoted by Q. It is the ratio of the number of decodable words to the cardinality of the whole vector space. That is,

$$Q = \frac{(q^k - 1)\, V_n(t)}{q^n} \cong q^{-r}\, V_n(t) \qquad (15)$$

where $r = n - k$ is the code's redundancy and

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

is the volume of a Hamming sphere of radius t. It is shown in the next part of this section that if $q \geqslant n$, which is generally true, then $P_E(u)$ approaches Q very rapidly as u increases.

B. Examples and Observations

Two well-known examples of linear MDS codes–the NASA code and the JTIDS code–are tabulated in Table 3 and Table 4, respectively. In these two examples, we observe that $P_E(u)$ approaches the constant Q as u increases. In fact, $P_E(u)$ approaches Q rapidly for $u \ll n$. In the case of large q and $q \geqslant n$, $P_E(u)$ approaches Q even for $u < d$. The $P_E(u)$ and Q of the NASA code agree to eight significant digits for $u \geqslant 26$ ($d = 33$). If $P_E(u)$ and Q are interpreted combinatorically as ratios, then we have the following relationship:

$$\frac{\text{\# of decodable words of weight } u}{\text{\# of vectors of weight } u} \rightarrow \frac{\text{\# of decodable words}}{\text{\# of words in vector space}}$$

This astonishing relationship cited above implies that a linear MDS code, which possesses rigid algebraic and combinatoric structures, behaves (in some sense) like a random code with no structure at all. Some laws of large number come into play somehow.

In order to describe analytically how fast $P_E(u)$ approaches Q when u is large, an upper bound on the expression $|[P_E(u)/Q] - 1|$ is derived in the following paragraphs. This upper bound is denoted by $\mathrm{U}(u)$, where $u \geqslant d$. It will be shown that $\mathrm{U}(u)$ approaches a very small number ϵ as u increases.

As in Section I, let D_u denote the exact number of decodable words of weight u. Let N_j's be the corresponding terms in the inclusion and exclusion formula of D_u as expressed in Eqs. (11), (12), and (13) of Section I. Let $\hat{D}_u$ denote the estimated number of decodable words of weight u. Let $\hat{N}_j$'s be the corresponding terms in the inclusion and exclusion formula of $\hat{D}_u$. The expression of $\hat{N}_j$, $0 \leqslant j \leqslant u$ is constructed by extrapolating the first term on the right-hand side of Eq. (12) of Section I from $0 \leqslant j \leqslant u - d$ to $0 \leqslant j \leqslant u$. We now have the following equations for $\hat{D}_u$ and $\hat{N}_j$:

$$\hat{D}_u = \binom{n}{u} \sum_{j=0}^{u} (-1)^j \hat{N}_j \qquad d - t \leqslant u \leqslant n \qquad (16)$$

$$\hat{N}_j = \binom{u}{j} q^{u-d+1-j}\, V_n(t) \qquad 0 \leqslant j \leqslant u \qquad (17)$$

Now we want to find an upper bound, denoted by U_j, for N_j in Eq. (13) of Section I for $u - d + 1 \leqslant j \leqslant u - d + t$.

$$N_j = \binom{u}{j} \sum_{w=d-u+j}^{t} \binom{n-u+j}{w}$$

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

$$\times \sum_{s=w}^{t} \binom{u-j}{s-w} (q-1)^{s-w}$$

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

$$\times \left[\sum_{i=0}^{w-d+u-j} (-1)^i \binom{w-1}{i} q^{w-d+u-j-i} \right]$$

$$\times \sum_{s=w}^{t} \binom{u-j}{s-w} (q-1)^{s-w}$$

$$\leqslant \binom{u}{j} \sum_{w=d-u+j}^{t} \binom{n-u+j}{w} (q-1)\, q^{-d+u-j}\, q^{w}$$

$$\times \sum_{s=w}^{t} \binom{u-j}{s-w} (q-1)^{s-w}$$

$$= \binom{u}{j} \sum_{w=d-u+j}^{t} \binom{n-u+j}{w} q^{u-j-d+1} \left(\frac{q}{q-1}\right)^{w-1} (q-1)^{w}$$

$$\times \sum_{s=w}^{t} \binom{u-j}{s-w} (q-1)^{s-w}$$

$$\leqslant q^{u-j-d+1} \left(\frac{q}{q-1}\right)^{t-1} \binom{u}{j} \sum_{w=d-u+j}^{t} \binom{n-u+j}{w} (q-1)^{w}$$

$$\times \sum_{s=w}^{t} \binom{u-j}{s-w} (q-1)^{s-w}$$

$$= q^{u-j-d+1} \left(\frac{q}{q-1}\right)^{t-1} \binom{u}{j}$$

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

$$< q^{u-j-d+1} \left(\frac{q}{q-1}\right)^{t-1} \binom{u}{j} V_n(t)$$

$$= \left(\frac{q}{q-1}\right)^{t-1} \hat{N}_j \overset{\text{def}}{=} U_j$$

Note that $\binom{u}{j} q^{u-d+1-j} V_n(t) = \hat{N}_j < U_j$, and so $U_j \geqslant \max \{N_j, \hat{N}_j\}$. Also, with the additional assumption that $q \geqslant n$, which is generally true, U_j is a descending function of j.

Now let us consider the second term on the right-hand side of Eq. (12) of Section I, and denote it by $\Theta(u)$. We want to find an upper bound for $\Theta(u)$.

$$\Theta(u) = \sum_{j=0}^{u-d} (-1)^j \binom{u}{j} \sum_{i=0}^{t} \binom{u-j}{i} (q-1)^i$$

$$= \sum_{j=0}^{u-d} (-1)^j \sum_{i=0}^{t} \binom{u}{i} \binom{u-i}{j} (q-1)^i$$

$$= \sum_{i=0}^{t} \binom{u}{i} (q-1)^i \sum_{j=0}^{u-d} (-1)^j \binom{u-i}{j}$$

$$\leqslant \sum_{i=0}^{t} \binom{u}{i} (q-1)^i \sum_{j=0}^{u-d} \binom{u-i}{j}$$

$$\leqslant \sum_{i=0}^{t} \binom{u}{i} (q-1)^i \sum_{j=0}^{u-i} \binom{u-i}{j}$$

$$= \sum_{i=0}^{t} \binom{u}{i} (q-1)^i\, 2^{u-i}$$

$$= 2^u \sum_{i=0}^{t} \binom{u}{i} \left(\frac{q-1}{2}\right)^i$$

$$= 2^u\, V_u^*(t)$$

where

$$V_u^*(t) = \sum_{i=0}^{t} \binom{u}{i} \left(\frac{q-1}{2}\right)^i$$

We then want to find an upper bound of $|D_u - \widehat{D}_u|$, where $d \leqslant u \leqslant n$. We have

$$|D_u - \widehat{D}_u| = \left| \binom{n}{u} \left[\sum_{j=0}^{u-d+t} (-1)^j N_j - \sum_{j=0}^{u} (-1)^j \widehat{N}_j \right] \right|$$

$$\leqslant \binom{n}{u} \left[\left| \sum_{j=u-d+1}^{u-d+t} (-1)^j N_j \right.\right.$$

$$\left.\left. - \sum_{j=u-d+1}^{u} (-1)^j \widehat{N}_j \right| + \Theta(t) \right]$$

$$= \binom{n}{u} \left[\left| \sum_{j=u-d+1}^{u} (-1)^j (N_j - \widehat{N}_j) \right| + \Theta(u) \right]$$

(set $N_j = 0$ for $u - d + t + 1 \leqslant j \leqslant u$)

$$\leqslant \binom{n}{u} \left[\sum_{j=u-d+1}^{u} \left| N_j - \widehat{N}_j \right| + \Theta(u) \right]$$

$$\leqslant \binom{n}{u} \left[\sum_{j=u-d+1}^{u} \max \{N_j, \widehat{N}_j\} + \Theta(u) \right]$$

$$\leqslant \binom{n}{u} \left[\sum_{j=u-d+1}^{u} U_j + \Theta(u) \right]$$

$$\leqslant \binom{n}{u} \; [dU_{u-d+1} + \Theta(u)]$$

(U_j is a descending function)

$$= \binom{n}{u} \left[d \left(\frac{q}{q-1} \right)^{t-1} \binom{u}{d-1} V_n(t) + 2^u \, V_u^*(t) \right]$$

We are finally ready to derive an upper bound for $|[P_E(u)/Q] - 1|$. By the definition of $\widehat{D}_u$ in Eqs. (16) and (17), it is not hard to see that

$$\widehat{D}_u = \binom{n}{u} \sum_{j=0}^{u} (-1)^j \binom{u}{j} q^{u-d+1-j} \, V_n(t)$$

$$= \binom{n}{u} V_n(t) \, q^{-d+1} \, (q-1)^u$$

Now for $d \leqslant u \leqslant n$,

$$\left| \frac{P_E(u)}{Q} - 1 \right| = \left| \frac{q^n D_u}{\binom{n}{u} (q-1)^u q^k \, V_n(t)} - 1 \right|$$

$$= \left| \frac{q^n (D_u - \widehat{D}_u)}{\binom{n}{u} (q-1)^u q^k \, V_n(t)} \right|$$

$$= \frac{q^n |D_u - \widehat{D}_u|}{\binom{n}{u} (q-1)^u \, \mathrm{q}^k \, V_n(t)}$$

$$\leqslant \left(\frac{q}{q-1} \right)^{t-1} \frac{q^{d-1} \binom{u}{d-1} d}{(q-1)^u}$$

$$+ \frac{q^{d-1} \, 2^u}{(q-1)^u} \, \frac{V_u^*(t)}{V_n(t)} \overset{\text{def}}{=} \mathrm{U}(u)$$

where

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

and

$$V_u^*(t) = \sum_{i=0}^{t} \binom{u}{i} \left(\frac{q-1}{2}\right)^i$$

Thus, the upper bound U(u) of $|[P_E(u)/Q] - 1|$, which is a function of u for $d \leqslant u \leqslant n$, is given by the following equation:

$$\left|\frac{P_E(u)}{Q} - 1\right| \leqslant \left(\frac{q}{q-1}\right)^{t-1} \frac{q^{d-1} \binom{u}{d-1} d}{(q-1)^u}$$

$$+ \frac{q^{d-1}\, 2^u}{(q-1)^u} \frac{V_u^*(t)}{V_n(t)} = \mathrm{U}(u)$$

The upper bounds of $|[P_E(u)/Q] - 1|$ of the NASA code and the JTIDS code are tabulated in Table 5 and Table 6, respectively.

C. Remarks

With the assumptions that q is greater than or equal to n and that u is large compared to d, Eq. (18) shows that the upper bound of $|[P_E(u)/Q] - 1|$ is dominated by the denominator term $(q - 1)^u$. Thus, the upper bound of $|[P_E(u)/Q] - 1|$ decays nearly exponentially as a function of u. This upper bound is not a very tight bound, but it is sufficient to illustrate the point that $P_E(u)$ approaches Q very rapidly as u increases.

References

[1] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, Amsterdam, The Netherlands: North-Holland, 1983.

[2] E. F. Assmus, H. F. Mattson, Jr., and R. J. Turyn, *Cyclic Codes*, AFCRL-65-332, Air Force Cambridge Research Labs, Bedford, Massachusetts, 1965.

[3] G. D. Forney, Jr., *Concatenated Codes*, Cambridge, Massachusetts: The MIT Press, 1966.

[4] T. Kasami, S. Lin, and W. W. Peterson, "Some Results on Weight Distributions of BCH codes," *IEEE Trans. Inform. Theory*, vol. IT-12, p. 274, April 1966.

[5] M. Hall, *Combinatorial Theory*, Waltham, Massachusetts: Blaisdell, 1967.

[6] E. R. Berlekamp and J. L. Ramsey, "Readable Erasures Improve the Performance of Reed-Solomon Codes," *IEEE Trans. Inform. Theory*, vol. IT-24, pp. 632–633, September 1978.

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

Table 1. (4,2) MDS code over $GF(5)$ with $t = 1$

Weight	Number of decodable words	Upper bound [6]
0	1	–
1	16	–
2	48	48
3	192	272
4	168	272

Total number of decodable words = $q^k V_n(t) = 425$.

Table 2. (6,3) MDS code over $GF(4)$ with $t = 1$

Weight	Number of decodable words	Upper bound [6]
0	1	–
1	18	–
2	0	–
3	180	180
4	405	855
5	378	1026
6	234	513

Total number of decodable words = $q^k V_n(t) = 1216$.

Table 3. NASA Code: (255,223); RS code: $q = 256$, $t = 16$

$$P_E(17) = 9.4641648 \times 10^{-15}$$
$$P_E(18) = 1.9130119 \times 10^{-14}$$
$$P_E(19) = 2.4010995 \times 10^{-14}$$
$$P_E(20) = 2.6598044 \times 10^{-14}$$
$$P_E(21) = 2.6017177 \times 10^{-14}$$
$$P_E(22) = 2.6076401 \times 10^{-14}$$
$$P_E(23) = 2.6087596 \times 10^{-14}$$
$$P_E(24) = 2.6088773 \times 10^{-14}$$
$$P_E(25) = 2.6088880 \times 10^{-14}$$
$$P_E(26) = 2.6088888 \times 10^{-14}$$
$$P_E(27) = 2.6088888 \times 10^{-14}$$
$$P_E(28) = 2.6088888 \times 10^{-14}$$
$$P_E(29) = 2.6088888 \times 10^{-14}$$
$$P_E(30) = 2.6088888 \times 10^{-14}$$
$$\vdots \qquad \vdots$$

Table 4. JTIDS Code: (31,15); RS code: q = 32, t = 8

$P_E(9) = 3.7493431 \times 10^{-7}$

$P_E(10) = 1.4392257 \times 10^{-6}$

$P_E(11) = 2.9507015 \times 10^{-6}$

$P_E(12) = 4.3287703 \times 10^{-6}$

$P_E(13) = 5.1888955 \times 10^{-6}$

$P_E(14) = 5.5466000 \times 10^{-6}$

$P_E(15) = 5.6291887 \times 10^{-6}$

$P_E(16) = 5.6296979 \times 10^{-6}$

$P_E(17) = 5.6255686 \times 10^{-6}$

$P_E(18) = 5.6256673 \times 10^{-6}$

$P_E(19) = 5.6259065 \times 10^{-6}$

$P_E(20) = 5.6258313 \times 10^{-6}$

$P_E(21) = 5.6258455 \times 10^{-6}$

$P_E(22) = 5.6258434 \times 10^{-6}$

$P_E(23) = 5.6258437 \times 10^{-6}$

$P_E(24) = 5.6258437 \times 10^{-6}$

• •

• •

• •

Table 5. NASA Code: (255,223); RS code: q = 256, t = 16

u	U(u)
33	5.133
34	0.3422
35	0.0157
36	5.526×10^{-4}
37	1.512×10^{-5}
•	•
•	•
•	•

Table 6. JTIDS Code: (31,15); RS code: q = 32, t = 8

u	U(u)
17	19.35
18	5.618
19	1.148
20	0.1851
21	0.02508
•	•
•	•
•	•