ISIT'2013 1569718847

Incorrigible Set Distributions and Unsuccessful Decoding Probability of Linear Codes

Yong Jiang, Shu-Tao Xia, Xin-Ji Liu
Graduate School at Shenzhen, Tsinghua University
Shenzhen, Guangdong 518055, P. R. China
Email: {jiangy, xiast}@sz.tsinghua.edu.cn

Fang-Wei Fu
Chern Institute of Mathematics and LPMC, Nankai University
Tianjin 300071, P. R. China
Email: fwfu@nankai.edu.cn

***Abstract*—On a binary erasure channel (BEC) with erasing probability ϵ, the performance of a binary linear code is determined by the incorrigible sets of the code. The incorrigible set distribution (ISD) $\{I_i\}_{i=0}^n$ enumerates the number of incorrigible sets with size i of the code. The probability of unsuccessful decoding under optimal decoding for the code could be formulated by the ISD and ϵ. In this paper, we determine the ISDs for the Simplex codes, the Hamming codes, the first order Reed-Muller codes, and the extended Hamming codes, which are some Reed-Muller codes or their shortening or puncturing versions. Then, we show that the probability of unsuccessful decoding under optimal decoding for any binary linear code is monotonously non-decreasing on ϵ in the interval $[0, 1]$.**

I. Introduction

The performance of optimal decoding for binary linear codes over a binary erasure channel (BEC) depends on the incorrigible sets of this code [1]. Alike the weight distribution of a linear code for error detection over a binary symmetric channel, the so-called *incorrigible set distribution* characterizes the probability of unsuccessful decoding of linear codes under optimal decoding over the BEC.

Let C be a binary $[n, k, d]$ linear code with length n, dimension k and minimum distance d. Let $W(x) = \sum_{i=0}^n A_i x^i$ denote the *weight enumerator* of C, where A_i is the number of codewords with weight i. Suppose a codeword $\mathbf{c} = (c_1, c_2, \ldots, c_n) \in C$ is transmitted over the BEC with erasing probability ϵ. The *support* of $\mathbf{c}$ is defined by the set of its non-zero positions. Let $\mathbf{r} = (r_1, r_2, \ldots, r_n)$ be the received word. The erasure set is defined by $E_{\mathbf{r}} = \{j : r_j \neq 0, 1\}$. The received word $\mathbf{r}$ can be decoded successfully if and only if it matches exactly one codeword of C on $\bar{E}_{\mathbf{r}} = \{1, 2, \ldots, n\} \setminus E_{\mathbf{r}}$. When C is linear, this is equivalent to the condition that $E_{\mathbf{r}}$ does not contain the support of a nonzero codeword. An *incorrigible set* of C is an erasure set which contains the support of a non-zero codeword of C. A decoder is said to be *optimal* if it can achieve successful decoding whenever the erasure set is not incorrigible. Clearly, the exhaustive decoder is an optimal decoder with highest decoding complexity. Let $I(x) = \sum_{i=1}^n I_i x^i$ denote the *incorrigible set enumerator* of C, where I_i is the number of incorrigible sets of C with size i. $\{I_i\}_{i=1}^n$ is called the *incorrigible set distribution* (ISD) of C. Let $H = (\mathbf{h}_1, \ldots, \mathbf{h}_n)$ be an $m \times n$ parity-check matrix of C. Clearly, the columns $\{\mathbf{h_i}, i \in E\}$ are linearly dependent if and only if E contains the support a non-zero codeword, which gives the following result.

Proposition 1: Let C be a binary linear code with $m \times n$ parity-check matrix $H = (\mathbf{h}_1, \ldots, \mathbf{h}_n)$. Let E be a non-empty erasure set. Then E is incorrigible if and only if the columns $\{\mathbf{h_i}, i \in E\}$ are linearly dependent.

Furthermore, Weber and Abdel-Ghaffar [1] show that

$$I_i = \begin{cases} 0, & \text{if } 1 \leq i \leq d-1, \\ A_i, & \text{if } i = d, \\ \binom{n}{i}, & \text{if } n-k+1 \leq i \leq n. \end{cases} \quad (1)$$

For a binary linear code C over the BEC with erasing probability ϵ, it is known [1] that the probability of unsuccessful decoding for an optimal decoder is

$$P_{ud}(C, \epsilon) = \sum_{i=d}^n I_i \epsilon^i (1-\epsilon)^{n-i}. \quad (2)$$

Hence, this probability is determined by the ISD of C.

While the exhaustive decoding often suffers from high decoding complexity, iterative decoding attracts many attentions recently. It is well known that the performance of iterative decoding for the linear code C over the BEC depends on certain combinatorial structures, called *stopping sets*, of the parity-check matrix of the code [2]. Stopping sets and stopping set distributions of linear codes have been studied recently by a number of researchers, e.g., see [3]-[17]. In order to explicitly show the dependency of the performance on the stopping sets, Weber and Abdel-Ghaffar [1] introduced the notion of dead-end sets and obtained the probability of unsuccessful decoding of iterative decoding. Furthermore, they show that the iterative decoding is equivalent to the optimal decoding when the dead-end sets coincide with the incorrigible sets. Let H^* be formed by rows which are all the non-zero codewords of $C^\perp$. It is known from [1] and [8] that the dead-end set distribution of H^* is the same with the ISD of C. Hence, the iterative decoder could be an optimal decoder and may have lower decoding complexity than the exhaustive decoder.

If the binary linear $[n, k, d]$ code C is used for error detection on a binary-symmetric channel with symbol error probability p, the probability of undetected errors is given by (see, e.g., [19])

$$P_{ue}(C, p) = \sum_{i=1}^n A_i p^i (1-p)^{n-i}.$$

Comparing it to (2), it is easy to see that the ISD is substituted to the weight distribution in the form. Similar to the probability of undetected errors, on a BEC, it is desirable that the probability $P_{ud}(C, \epsilon)$ of unsuccessful decoding for an optimal decoder is monotonously non-decreasing on ϵ in the interval $[0, 1]$.

In this paper, we determine the ISDs for the Simplex codes, the Hamming codes, the first order Reed-Muller codes, and the extended Hamming codes, which are some Reed-Muller

codes or their shortening or puncturing versions. Then, we show that the probability of unsuccessful decoding under optimal decoding over the BEC for any binary linear code is monotonously non-decreasing on ϵ in the interval $[0,1]$, i.e., $P'_{ud}(C,\epsilon) \geq 0$ when $0 \leq \epsilon \leq 1$. The rest of this paper is arranged as follows. Section II gives some preliminaries. In Section III, the ISDs for these codes are obtained. In Section IV, we show that the probability of unsuccessful decoding under optimal decoding over the BEC for any binary linear code is monotonously non-decreasing on ϵ in the interval $[0,1]$. Finally, conclusions are given in Section V.

II. Preliminaries

A. Finite Geometries

Let $\mathbb{F}_q$ be a finite field of q elements and $\mathbb{F}_q^m$ be the m-dimensional vector space over $\mathbb{F}_q$, where $m \geq 2$. Let $EG(m,q)$ be the m-dimensional Euclidean geometry over $\mathbb{F}_q$ [20, pp. 692-702]. $EG(m,q)$ has q^m points, which are vectors of $\mathbb{F}_q$. The μ-flat in $EG(m,q)$ is a μ-dimensional subspace of $\mathbb{F}_q^m$ or its coset. Let $PG(m,q)$ be the m-dimensional projective geometry over $\mathbb{F}_q$. $PG(m,q)$ is defined in $\mathbb{F}_q^{m+1} \setminus \{\mathbf{0}\}$. Two nonzero vectors $\mathbf{p}, \mathbf{p}' \in \mathbb{F}_q^{m+1}$ are said to be equivalent if there is $\lambda \in \mathbb{F}_q$ such that $\mathbf{p} = \lambda \mathbf{p}'$. All equivalent classes of $\mathbb{F}_q^{m+1} \setminus \{\mathbf{0}\}$ form $(q^{m+1}-1)/(q-1)$ points of $PG(m,q)$. The μ-flat in $PG(m,q)$ is simply the set of equivalent classes in a $(\mu+1)$-dimensional subspace of $\mathbb{F}_q^{m+1}$.

In this paper, in order to present a unified approach, we use $FG(m,q)$ to denote either $EG(m,q)$ or $PG(m,q)$. 0-flat, 1-flat, and $(m-1)$-flat are called point, line and hyperplane respectively. Let n denote the number of points of $FG(m,q)$ and all points $\mathbf{p}_1, \mathbf{p}_2, \ldots, \mathbf{p}_n$ of $FG(m,q)$ are indexed from 1 to n. We will use i to denote the i-th point $\mathbf{p}_i$ of $FG(m,q)$ for convenience if there is no confusion. For a set of points, $\Pi \subseteq FG(m,q)$, let $\chi(\Pi) = (x_1, x_2, \ldots, x_n)$ denote the *incidence vector* of Π, i.e., x_i=1 if $i \in \Pi$ and $x_i = 0$ otherwise. For $u > 0$, a *u-set* means a set of u points of $FG(m,q)$. For a non-empty subset S of $FG(m,q)$, define $\langle S \rangle$ as the flat generated by the points in S, i.e., $\langle S \rangle$ is the flat containing S with the minimum dimension.

For $0 \leq \mu_1 < \mu_2 \leq m$, there are $N(\mu_2,\mu_1)$ μ_1-flats contained in a given μ_2-flat and $A(\mu_2,\mu_1)$ μ_2-flats containing a given μ_1-flat, where for $EG(m,q)$ and $PG(m,q)$ respectively (see [18])

$$N_{EG}(\mu_2,\mu_1) = q^{\mu_2-\mu_1} \prod_{i=1}^{\mu_1} \frac{q^{\mu_2-i+1}-1}{q^{\mu_1-i+1}-1}, \quad (3)$$

$$N_{PG}(\mu_2,\mu_1) = \prod_{i=0}^{\mu_1} \frac{q^{\mu_2-i+1}-1}{q^{\mu_1-i+1}-1}, \quad (4)$$

$$A_{EG}(\mu_2,\mu_1) = A_{PG}(\mu_2,\mu_1) = \prod_{i=\mu_1+1}^{\mu_2} \frac{q^{m-i+1}-1}{q^{\mu_2-i+1}-1}. \quad (5)$$

B. Gaussian binomial coefficients

For non-negative integers $m \leq n$, let

$$\begin{bmatrix} n \\ m \end{bmatrix}_q = \prod_{i=0}^{m-1} \frac{q^{n-i}-1}{q^{m-i}-1} \quad (6)$$

denote the q-binomial coefficient or Gaussian binomial coefficient [20, pp.443-444]. In this paper, we will omit the subscript q when $q = 2$.

From now on, we will always assume that $q = 2$. As usual, we define $\binom{0}{0} = 1$, $\binom{i_2}{i_1} = 0$, $\begin{bmatrix} 0 \\ 0 \end{bmatrix} = 1$, $\begin{bmatrix} i_2 \\ i_1 \end{bmatrix} = 0$, $\sum_{i=i_1}^{i_2} a_i = 0$ and $\prod_{i=i_1}^{i_2} a_i = 1$ if $i_1 > i_2$. We also note tat

$$N_{PG}(\mu_2,\mu_1) = \begin{bmatrix} \mu_2+1 \\ \mu_1+1 \end{bmatrix}, \quad (7)$$

$$N_{EG}(\mu_2,\mu_1) = 2^{\mu_2-\mu_1} \begin{bmatrix} \mu_2 \\ \mu_1 \end{bmatrix}, \quad (8)$$

$$A(\mu_2,\mu_1) = \begin{bmatrix} m-\mu_1 \\ \mu_2-\mu_1 \end{bmatrix}. \quad (9)$$

C. Generators in Finite Geometries

We will introduce the concepts of generators in finite geometries, and then give some enumeration results in [17]. Let $S \subseteq FG(m,2)$ be non-empty. For any $j \in S$, denote $S_j = S \setminus \{j\}$. A point i is said to be *independent* to S if $i \notin \langle S \rangle$. S is said to be *independent* if for any $j \in S$, j is independent to $\langle S_j \rangle$. The empty set $\emptyset$ is defined as an independent set.

For an integer $0 \leq l \leq m$, let $F^{(l)}$ denote an l-flat of $FG(m,2)$. $F^{(l)}$ has $N(l,0)$ points. Let $u \geq 1$, if a u-set generates $F^{(l)}$, we call it a *u-generator* of $F^{(l)}$. Define $B(u,l)$ as the number of u-generators of $F^{(l)}$, i.e, for $u \geq 1$ and $l \geq 0$,

$$B(u,l) = |\{S \subseteq F^{(l)} : |S| = u,\ \langle S \rangle = F^{(l)}\}|. \quad (10)$$

Define $B(u,l) = 0$ if $u \leq 0$ or $l < 0$. Clearly,

$$B(u,l) = 0 \quad \text{if } u \leq l. \quad (11)$$

Lemma 1: [17, Lemma 11] For any $u \geq 1$ and $l \geq 0$, $B(u,l)$ satisfies the following recursive equation

$$B(1,0) = 1, \quad B(u,0) = 0 \quad \text{if } u \geq 2, \quad (12)$$

$$\binom{N(l,0)}{u} = \sum_{i=0}^{l} N(l,i)\, B(u,i),\ l \geq 0. \quad (13)$$

By solving the recursive equation in the above lemma, the next lemma gives the enumeration formulas of $B(u,l)$ for projective geometry and Euclidean geometry, respectively.

Lemma 2: [17, Lemma 7] Let $u \geq l+1$. Then

$$B_{PG}(u,l) = \sum_{j=0}^{l} (-1)^j 2^{j(j-1)/2} \begin{bmatrix} l+1 \\ j \end{bmatrix} \binom{2^{l-j+1}-1}{u}, \quad (14)$$

$$B_{EG}(u,l) = \sum_{j=0}^{l} (-1)^j 2^{j(j+1)/2} \begin{bmatrix} l \\ j \end{bmatrix} \binom{2^{l-j}}{u}. \quad (15)$$

III. Incorrigible Set Distributions

Let $RM(m,r)$ be the r-th order binary Reed-Muller code [20, Ch. 13]. By puncturing a fix coordinate from all codewords of $RM(m,r)$, we obtain the punctured Reed-Muller code $RM(m,r)^*$. It is well known that $RM(m,m-2)$ is a $[2^m, 2^m-m-1, 4]$ extended Hamming code, which is also denoted by $\hat{\mathcal{H}}(m)$; $RM(m,1)$ is the dual code of $\hat{\mathcal{H}}(m)$ and has parameters $[2^m, m+1, 2^{m-1}]$; $RM(m,m-2)^*$ is a $[2^m-1, 2^m-m-1, 3]$ Hamming code, which is denoted by $\mathcal{H}(m)$; The shortened $RM(m,1)$, or simplex code $\mathcal{S}(m)$, is the dual code of $\mathcal{H}(m)$ and has parameters $[2^m-1, m, 2^{m-1}]$.

The points of $PG(m-1,2)$ are simply the nonzero vectors of $\mathbb{F}_2^m$. A μ-flat of $PG(m-1,2)$ is simply the nonzero linear combination of $\mu+1$ linearly independent points. The points of $EG(m,2)$ are simply the vectors of F_2^m. A μ-flat of $EG(m,2)$ is simply μ-dimensional subspace or its coset.

A. Simplex Codes and the First Order Reed-Muller Codes

By (4), $PG(m-1,2)$ has 2^m-1 points and 2^m-1 hyperplanes. For the Simplex code $\mathcal{S}(m)$ and any hyperplane P of $PG(m-1,2)$, $\chi(\bar{P})$ is the support of a non-zero codeword and vice versa [17]. The next lemma gives a necessary and sufficient condition that an erasure set is corrigible.

Lemma 3: For the Simplex code $\mathcal{S}(m)$, a non-empty erasure set E is a corrigible set if and only if $\bar{E} = PG(m-1,2) \setminus E$ is a $(2^m-1-|E|)$-generator of $PG(m-1,2)$.

Proof: Let $E \subseteq PG(m-1,2)$ be a non-empty erasure set. Thus $|\bar{E}| = 2^m-1-|E|$. Note that for the support S of any non-zero codeword of $\mathcal{S}(m)$, $\bar{S}$ is a hyperplane of $PG(m-1,2)$, and vice versa. Hence, by the definition of corrigible sets, it is easy to see that

$$\begin{aligned} & E \text{ is a corrigible set} \\ \iff & \text{for any non-zero codeword support } S,\ S \not\subseteq E \\ \iff & \text{for any non-zero codeword support } S,\ \bar{E} \not\subseteq \bar{S} \\ \iff & \text{for any hyperplane } P \text{ of } PG(m-1,2)\ ,\ \bar{E} \not\subseteq P \\ \iff & \langle \bar{E} \rangle = PG(m-1,2), \end{aligned}$$

or $\bar{E}$ is a $(2^m-1-|E|)$-generator of $PG(m-1,2)$. ∎

The ISD of the Simplex code $\mathcal{S}(m)$ is obtained by Lemma 3 as follows.

Theorem 1: For the Simplex code $\mathcal{S}(m)$ and $i = 1,2,\ldots,2^m-1$,

$$I_i = \binom{2^m-1}{i} - B_{PG}(2^m-1-i, m-1) \quad (16)$$

$$= \sum_{j=1}^{m-1} (-1)^{j-1} 2^{j(j-1)/2} \begin{bmatrix} m \\ j \end{bmatrix} \binom{2^{m-j}-1}{2^m-1-i}. \quad (17)$$

Proof: The number of i-sets of $PG(m-1,2)$ is $\binom{2^m-1}{i}$. By Lemma 3, the corrigible sets with size i are 1-1 corresponding to the (2^m-1-i)-generators of $PG(m-1,2)$, which implies that the number of corrigible sets with size i is $B_{PG}(2^m-1-i, m-1)$. Hence, by (14), the number of incorrigible sets with size i is

$$\begin{aligned} I_i &= \binom{2^m-1}{i} - B_{PG}(2^m-1-i, m-1) \\ &= \binom{2^m-1}{i} - \sum_{j=0}^{m-1} (-1)^j 2^{j(j-1)/2} \begin{bmatrix} m \\ j \end{bmatrix} \binom{2^{m-j}-1}{2^m-1-i} \\ &= \sum_{j=1}^{m-1} (-1)^{j-1} 2^{j(j-1)/2} \begin{bmatrix} m \\ j \end{bmatrix} \binom{2^{m-j}-1}{2^m-1-i}. \end{aligned}$$

∎

Remark 1: By (17), when $1 \le i \le 2^{m-1}-1$, $\binom{2^{m-j}-1}{2^m-1-i} = 0$ and $I_i = 0$; when $i = 2^{m-1}$, $I_i = \begin{bmatrix} m \\ 1 \end{bmatrix} = 2^m-1$. By (11) and (16), when $2^m-m \le i \le 2^m-1$, $B_{PG}(2^m-1-i, m-1) = 0$ and $I_i = \binom{2^m-1}{i}$. Hence,

$$I_i = \begin{cases} 0, & 1 \le i \le 2^{m-1}-1, \\ 2^m-1, & i = 2^{m-1}, \\ \binom{2^m-1}{i}, & 2^m-m \le i \le 2^m-1. \end{cases} \quad (18)$$

Note that for the Simplex code $\mathcal{S}(m)$, the length $n = 2^m-1$, the minimum distance $d = 2^{m-1}$, the dimension $k = m$, and $A_d = 2^m-1$. Thus, (18) coincides with (1).

By (3), $EG(m,2)$ has 2^m points and $2^{m+1}-2$ hyperplanes. By using totally similar arguments, it is easy to obtain the following results for $EG(m,2)$ and $RM(m,1)$.

Lemma 4: For the first order Reed-Muller code $RM(m,1)$, a non-empty erasure set E is corrigible set if and only if $\bar{E} = EG(m,2) \setminus E$ is a $(2^m-|E|)$-generator of $EG(m,2)$.

Theorem 2: For the first order Reed-Muller code $RM(m,1)$ and $i = 1,\ldots,2^m$,

$$I_i = \binom{2^m}{i} - B_{EG}(2^m-i, m) \quad (19)$$

$$= \sum_{j=1}^{m} (-1)^{j-1} 2^{j(j+1)/2} \begin{bmatrix} m \\ j \end{bmatrix} \binom{2^{m-j}}{2^m-i}. \quad (20)$$

Remark 2: It is well known from [20] that shortening $RM(m,1)$ at any position yields the simplex code $\mathcal{S}(m)$. From this fact it can be shown that

$$2^m \cdot I_i(\mathcal{S}(m)) = (2^m-i) \cdot I_i(RM(m,1)).$$

which gives another simple proof of Theorem 2 from Theorem 1.

Remark 3: It is easy to check by Theorem 2 that

$$I_i = \begin{cases} 0, & 1 \le i \le 2^{m-1}-1, \\ 2^{m+1}-2, & i = 2^{m-1}, \\ \binom{2^m}{i}, & 2^m-m \le i \le 2^m. \end{cases} \quad (21)$$

which coincides with (1).

Example 1: By Theorems 1 and 2, we can easily calculate respectively the ISDs of $\mathcal{S}(m)$ and $RM(m,1)$, e.g., for $\mathcal{S}(3)$,

$$I(x) = 7x^4 + 21x^5 + 7x^6 + x^7,$$

for $\mathcal{S}(4)$,

$$\begin{aligned} I(x) = {} & 15x^8 + 105x^9 + 315x^{10} + 525x^{11} \\ & + 455x^{12} + 105x^{13} + 15x^{14} + x^{15}, \end{aligned}$$

for $\mathcal{S}(5)$,

$$\begin{aligned} I(x) = {} & 31x^{16} + 465x^{17} + 3255x^{18} + 14105x^{19} \\ & + 42315x^{20} + 93093x^{21} + 155155x^{22} \\ & + 199485x^{23} + 199175x^{24} + 152985x^{25} \\ & + 86583x^{26} + 31465x^{27} + 4495x^{28} \\ & + 465x^{29} + 31x^{30} + x^{31}. \end{aligned}$$

for $RM(3,1)$,

$$I(x) = 14x^4 + 56x^5 + 28x^6 + 8x^7 + x^8,$$

and for $RM(4,1)$,

$$\begin{aligned} I(x) = {} & 30x^8 + 240x^9 + 840x^{10} + 1680x^{11} \\ & + 1820x^{12} + 560x^{13} + 120x^{14} \\ & + 16x^{15} + x^{16}. \end{aligned}$$

B. Hamming Codes and the Extended Hamming Codes

Recall that $PG(m-1,2)$ has $n=2^m-1$ points $\mathbf{p}_1,\ldots,\mathbf{p}_n$, where $\mathbf{p}_i$ is a binary m-dimensional column vector. Note that $(\mathbf{p}_1,\ldots,\mathbf{p}_n)$ is exact the parity-check matrix of the Hamming code $\mathcal{H}(m)$. By the definition of independent set, the next lemma follows immediately from Proposition 1.

Lemma 5: For the Hamming code $\mathcal{H}(m)$, a non-empty erasure set E is corrigible if and only if E is independent in $PG(m-1,2)$.

By Lemma 5, we obtain the ISD of $\mathcal{H}(m)$ as follows.

Theorem 3: For the Hamming code $\mathcal{H}(m)$ and $i = 1,\ldots,2^m-1$,

$$I_i = \binom{2^m-1}{i} - N_{PG}(m-1,i-1)B_{PG}(i,i-1) \quad (22)$$

$$= \binom{2^m-1}{i} - \frac{1}{i!}\prod_{j=0}^{i-1}(2^m-2^j). \quad (23)$$

Proof: The number of i-sets of $PG(m-1,2)$ is $\binom{2^m-1}{i}$. Clearly, $PG(m-1,2)$ has $N_{PG}(m-1,i-1)$ $(i-1)$-flats and each of which has $B_{PG}(i,i-1)$ independent i-sets. Hence, the number of independent i-sets of $PG(m-1,2)$ is

$$N_{PG}(m-1,i-1)B_{PG}(i,i-1),$$

and (22) follows by Lemma 5. By Lemma 2, we have

$$I_i = \binom{2^m-1}{i} - \begin{bmatrix} m \\ i \end{bmatrix} \sum_{j=0}^{i-1}(-1)^j 2^{j(j-1)/2} \begin{bmatrix} i \\ j \end{bmatrix} \binom{2^{i-j}-1}{i}.$$

In order to show (23), we give an alternative expression of $B_{PG}(i,i-1)$. For $1 \le i \le m$ and a fixed $(i-1)$-flat F in $PG(m-1,2)$, $B_{PG}(i,i-1)$ is the number of independent i-sets in F by the definitions. The first point has $N_{PG}(i-1,0)$ choices, the second point has $N(i-1,0)-1$ choices, the third point has $N_{PG}(i-1,0)-N_{PG}(1,0)$ choices, the fourth point has $N_{PG}(i-1,0)-N_{PG}(2,0)$ choices, ..., the i-th point has $N_{PG}(i-1,0)-N_{PG}(i-2,0)$ choices, and there are exactly $i!$ repetitions in the above choices. Hence, by (7), it is easy to check that

$$B_{PG}(i,i-1) = \frac{1}{i!}\prod_{j=0}^{i-1}(2^i-2^j), \quad (24)$$

$$N_{PG}(m-1,i-1)B_{PG}(i,i-1) = \frac{1}{i!}\prod_{j=0}^{i-1}(2^m-2^j), \quad (25)$$

and (23) follows by (22). ∎

Remark 4: A simple proof for (23) could be obtained as follows. Let H be the $m \times (2^m-1)$ parity-check matrix of $\mathcal{H}(m)$ whose columns consist of all binary non-zero m-dimensional vectors. For any fixed i, $1 \le i \le 2^m-1$, it is easy to see that the number of i linearly independent columns of H, or the number of i independent m-dimensional vectors, is

$$\frac{(2^m-1)(2^m-2)(2^m-4)\cdots(2^m-2^{i-1})}{i!}.$$

By Proposition 1, the number of i linearly dependent columns of H, or the number of incorrigible sets of $\mathcal{H}(m)$, is

$$I_i = \binom{2^m-1}{i} - \frac{1}{i!}\prod_{j=0}^{i-1}(2^m-2^j).$$

Remark 5: By (23), it is easy to check that $I_1 = I_2 = 0$ and $I_3 = (2^m-1)(2^{m-1}-1)/3$. By (11) and (19), when $m+1 \le i \le 2^m-1$, $B_{PG}(i,i-1)=0$ and $I_i = \binom{2^m-1}{i}$. Hence,

$$I_i = \begin{cases} 0, & i=1,2, \\ (2^m-1)(2^{m-1}-1)/3, & i=3, \\ \binom{2^m-1}{i}, & m+1 \le i \le 2^m-1. \end{cases} \quad (26)$$

Note that for the Hamming code $\mathcal{H}(m)$, the length $n=2^m-1$, the minimum distance $d=3$, the dimension $k=2^m-1-m$, and $A_d = (2^m-1)(2^{m-1}-1)/3$ [20]. Thus, (26) coincides with (1).

Recall that $EG(m,2)$ has $n=2^m$ points. By using totally similar arguments, we could obtain the following results for $EG(m,2)$ and $\hat{\mathcal{H}}(m)$.

Lemma 6: For the extended Hamming code $\hat{\mathcal{H}}(m)$, a non-empty erasure set E is corrigible if and only if E is independent in $EG(m,2)$.

Theorem 4: For the extended Hamming code $\hat{\mathcal{H}}(m)$ and $i=1,\ldots,2^m$,

$$I_i = \binom{2^m}{i} - N_{EG}(m,i-1)B_{EG}(i,i-1) \quad (27)$$

$$= \binom{2^m}{i} - \frac{2^m}{i!}\prod_{j=0}^{i-2}(2^m-2^j). \quad (28)$$

Remark 6: A simple proof for (28) could be obtained as follows. Let $\hat{H}$ be the $(m+1)\times 2^m$ parity-check matrix of $\hat{\mathcal{H}}(m)$ whose columns consist of all binary non-zero $(m+1)$-dimensional vectors with odd weights. For any fixed i, $1 \le i \le 2^m$, it is easy to see that the number of i linearly independent columns of $\hat{H}$ is

$$\frac{2^m(2^m-1)(2^m-2)\cdots(2^m-2^{i-2})}{i!}.$$

By Proposition 1, the number of i linearly dependent columns of $\hat{H}$, or the number of incorrigible sets of $\hat{\mathcal{H}}(m)$, is

$$I_i = \binom{2^m}{i} - \frac{2^m}{i!}\prod_{j=0}^{i-2}(2^m-2^j).$$

Remark 7: It is easy to check by Theorem 4 that

$$I_i = \begin{cases} 0, & i=1,2,3, \\ 2^{m-2}(2^m-1)(2^{m-1}-1)/3, & i=4, \\ \binom{2^m}{i}, & m+2 \le i \le 2^m. \end{cases} \quad (29)$$

which coincides with (1).

Example 2: By Theorem 3, we can easily calculate the ISD for $\mathcal{H}(m)$. Here are some examples. For $\mathcal{H}(3)$,

$$I(x) = 7x^3 + x^4 + 21x^5 + 7x^6 + x^7.$$

For $\mathcal{H}(4)$,

$$I(x) = 35x^3 + 525x^4 + 3003x^5 + 5005x^6 + 6435x^7 + 6435x^8 + 5005x^9 + 3003x^{10} + 1365x^{11} + 455x^{12} + 105x^{13} + 15x^{14} + x^{15}.$$

IV. The probability of unsuccessful decoding

For a binary linear code C over the BEC with erasing probability ϵ, it is desirable that the probability $P_{ud}(C,\epsilon)$ of unsuccessful decoding for an optimal decoder is non-decreasing on ϵ in the interval $[0,1]$, i.e., $P'_{ud}(C,\epsilon) \geq 0$. In this section, we will show that this property does hold for all binary linear codes.

Firstly, we gives a property of incorrigible set distribution for a binary linear code.

Lemma 7: For any binary linear $[n,k]$ code C,

$$(i+1)I_{i+1} \geq (n-i)I_i, \quad i = 1, 2, \ldots, n-1.$$

Proof: Let $H = (\mathbf{h}_1, \ldots, \mathbf{h}_n)$ be an $m \times n$ parity-check matrix of C. For any fixed $1 \leq i \leq n-1$, let E be an incorrigible set with size i. By Proposition 1, the columns $\{\mathbf{h_j}, j \in E\}$ are linearly dependent. For any $j' \notin E$, let $E' = \{j\} \cup E$. Clearly, the columns $\{\mathbf{h_j}, j \in E'\}$ are linearly dependent, which implies that E' is also an incorrigible set. It is easy to see that for any fixed incorrigible set E with size i, the number of choices of E' is $(n-i)$. On the other hand, for any fixed incorrigible set E' with size $i+1$, it could be obtained from an incorrigible set with size i in at most $\binom{i+1}{i} = i+1$ ways since some subsets of E' with size i may not be incorrigible sets. In other words, all the $(n-i)I_i$ incorrigible sets with size $i+1$ that obtained from incorrigible sets with size i must repeat at most $i+1$ times, which implies that $(i+1)I_{i+1} \geq (n-i)I_i$. ∎

Then, the main result of this section is obtained by Lemma 7.

Theorem 5: For any binary linear $[n,k]$ code C, the probability $P_{ud}(C,\epsilon)$ of unsuccessful decoding for an optimal decoder is non-decreasing when ϵ is increasing in the interval $[0,1]$, i.e., $P'_{ud}(C,\epsilon) \geq 0$.

Proof: By (2) and Lemma 7, we have

$$\begin{aligned}
& P'_{ud}(C,\epsilon) \\
= & \sum_{i=1}^{n} iI_i\epsilon^{i-1}(1-\epsilon)^{n-i} - \sum_{i=1}^{n}(n-i)I_i\epsilon^i(1-\epsilon)^{n-i-1} \\
= & I_1(1-\epsilon)^{n-1} + \sum_{i=1}^{n-1}(i+1)I_{i+1}\epsilon^i(1-\epsilon)^{n-i-1} \\
& - \sum_{i=1}^{n-1}(n-i)I_i\epsilon^i(1-\epsilon)^{n-i-1} \\
= & I_1(1-\epsilon)^{n-1} + \sum_{i=1}^{n-1}\left[(i+1)I_{i+1} - (n-i)I_i\right] \\
& \cdot \epsilon^i(1-\epsilon)^{n-i-1} \ \geq \ 0.
\end{aligned}$$

∎

V. Conclusions

In this paper, the incorrigible set distributions (ISD) of the simplex codes, the Hamming codes, the first order Reed-Muller codes and the extended Hamming codes are determined by using finite geometry theory. Then, we show that for all binary linear codes, the probabilities of unsuccessful decoding under optimal decoding are monotonously non-decreasing on ϵ in the interval $[0,1]$, where ϵ is the erasing probability of the BEC.

Acknowledgment

The authors wish to express their appreciation to the three anonymous reviewers for their valuable suggestions and comments that helped to greatly improve the paper. In particular, one reviewer provides some simple proofs for some results in this paper.

This research is supported in part by the 973 Program of China (2012CB315803, 2013CB834204), the National Natural Science Foundation of China (Nos. 60972011, 61171082, 60872025, 10990011), the Research Fund for the Doctoral Program of Higher Education of China (20100002110033), and the open research fund of National Mobile Communications Research Laboratory of Southeast University (2011D11). The author Shu-Tao Xia is also with the National Mobile Communications Research Laboratory of Southeast University of China.

References

[1] J. H. Weber and K. A. S. Abdel-Ghaffar, "Results on parity-check matrices with optimal stopping and/or dead-end set enumerators," *IEEE Trans. Inf. Theory*, vol. 54, no. 3, pp. 1368–1374, 2008.

[2] C. Di, D. Proietti, I. E. Telatar, *et al.* "Finite-length analysis of low-density parity-check codes on the binary erasure channel," *IEEE Trans. Inf. Theory*, vol. 48, no. 6, pp. 1570–1579, 2002.

[3] M. Schwartz and A. Vardy, "On the stopping distance and the stopping redundancy of codes," *IEEE Trans. Inf. Theory*, vol. 52, no. 3, pp. 922–932, 2006.

[4] T. Etzion, "On the stopping redundancy of Reed-Muller codes," *IEEE Trans. Inf. Theory*, vol. 52, no. 11, pp. 4867–4879, 2006.

[5] A. Orlitsky, K. Viswanathan, and J. Zhang, "Stopping set distribution of LDPC code ensembles," *IEEE Trans. Inform. Theory*, vol. 51, no. 3, pp. 929-953, Mar. 2005.

[6] V. Rathi, "On the asymptotic weight and stopping set distribution of regular LDPC ensembles," *IEEE Trans. Inform. Theory*, vol. 52, no. 9, pp. 4212-4218, Sep. 2006.

[7] H. Hollmann and L. Tolhuizen, "Erasure correcting sets: bounds and constructions," *Journal of Combinatorial Theory, Series A*, vol. 113, pp. 1746–1759, 2006.

[8] H. Hollmann and L. Tolhuizen, "On parity-check collections for iterative erasure decoding that correct all correctable erasure patterns of a given size," *IEEE Trans. Inf. Theory*, vol. 53, no. 2, pp. 823–828, 2007.

[9] K. A. S. Abdel-Ghaffar and J. H. Weber, "Complete enumeration of stopping sets of full-rank parity-check matrices of Hamming codes," *IEEE Trans. Inf. Theory*, vol. 53, no. 9, pp. 3196–3201, 2007.

[10] J. Han and P. H. Siegel, "Improved upper bounds on stopping redundancy," *IEEE Trans. Inform. Theory*, vol. 53, no. 1, pp. 901-104, Jan. 2007.

[11] J. Han, P. H. Siegel, and A. Vardy, "Improved probabilistic bounds on stopping redundancy," *IEEE Trans. Inform. Theory*, vol. 54, no. 4, pp. 1749-1753, Apr. 2008.

[12] K. M. Krishnan and P. Shankar, "Computing the stopping distance of a Tanner graph is NP-hard," *IEEE Trans. Inform. Theory*, vol. 53, no. 6, pp. 2278-2280, Jun. 2007.

[13] A. McGregor and O. Milenkovic, "On the hardness of approximating stopping and trapping sets," *IEEE Trans. Inform. Theory*, vol. 56, no. 4, pp. 1640-1650, Apr. 2010.

[14] M. Esmaeili and M. J. Amoshahy, "On the stopping distance of array code parity-check matrices," *IEEE Trans. Inform. Theory*, vol. 55, no. 8, pp. 3488-3493, Aug. 2009.

[15] M. Esmaeili, H. M. Tadayon, and T. A. Gulliver, "More on the stopping and minimum distances of array codes," *IEEE Trans. Communications*, vol. 59, no. 3, pp. 750-757, Mar. 2011.

[16] S.-T. Xia and F.-W. Fu, "On the stopping distance of finite geometry LDPC Codes," *IEEE Communications Letters*, vol. 10, no.5, pp. 381-383, May 2006.

[17] Y. Jiang, S.-T. Xia and F.-W. Fu, "Stopping set distributions of some Reed-Muller codes," *IEEE Trans. Inf. Theory*, vol. 57, no. 9, pp. 6078–6088, 2011.

[18] H. Tang, J. Xu, S. Lin, and K. A. S. Abdel-Ghaffar, "Codes on finite geometries," *IEEE Trans. Inf. Theory*, vol. 51, no. 2, pp. 572–596, 2005.

[19] T. Kløve, Codes for error detection, World Scientific, 2007.

[20] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1981.