LETTER

More on Incorrigible Sets of Binary Linear Codes*

Lingjun KONG[†a)], ***Member***, **Haiyang LIU**[††b)], ***Nonmember***, ***and*** **Lianrong MA**[†††c)], ***Member***

SUMMARY This letter is concerned with incorrigible sets of binary linear codes. For a given binary linear code C, we represent the numbers of incorrigible sets of size up to $\lceil \frac{3}{2}d - 1 \rceil$ using the weight enumerator of C, where d is the minimum distance of C. In addition, we determine the incorrigible set enumerators of binary Golay codes $\mathcal{G}_{23}$ and $\mathcal{G}_{24}$ through combinatorial methods.

key words: *incorrigible set, incorrigible set enumerator, weight enumerator, binary linear codes, binary Golay codes*

1. Introduction

The incorrigible set enumerator of a binary linear code, which enumerates the numbers of incorrigible sets according to their sizes, is an important property of the code [1], since it can be used to *exactly* characterize the optimal decoding performance over the binary erasure channel (BEC). From the theoretical point of view, it has been shown in [2] that the property is closely related to the matroid theory, which is an important part of combinatorial mathematics. In fact, the incorrigible set enumerator of a binary linear code is a specialization of the Tutte polynomial of the vector matroid induced by the parity-check matrix of the code [2]. From the computation point of view, however, it is a difficult problem to compute the incorrigible set enumerator for a code in general. In [3], the authors have established a relation between the incorrigible set enumerator and the generalized weight distributions of a code. But the relation is helpless in practice, since it is intractable to obtain the generalized weight distributions of a code. Only sporadic studies have considered the problem for some specific families of codes (e.g., codes related to graphs [2] or related to finite geometries [4]). Since the incorrigible set enumerator is of great importance, it is deserved to further investigate the problem.

In this letter, we present more results on incorrigible sets of binary linear codes. First, we provide a relation between the incorrigible set enumerator and the weight enumerator of a binary linear code. More concretely, for a binary linear code with minimum distance d, we represent the numbers of incorrigible sets of sizes up to $\lceil \frac{3}{2}d - 1 \rceil$ using the weight enumerator of the code, where $\lceil x \rceil$ is the smallest integer that is greater than or equal to x. Although the incorrigible set enumerator cannot be determined completely from the relation in general, we may get a better understanding on the code performance over the BEC using the obtained result, especially in the situation where the erasure probability is high. Second, we focus on the well-known binary Golay codes [5], [6], which are important codes discovered in the early days of error correction coding. The nice properties of the two codes have been studied in the literature, and both codes have been adopted in practical applications. Most interestingly, each code is the unique binary code with the corresponding code parameters under the code equivalence [6]. Using their properties, we determine the incorrigible set enumerators of the two codes through combinatorial methods, which is helpful in understanding the performance of the two codes over the BEC.

2. Preliminaries

In this section, we provide the concept of incorrigible sets. For more details, the reader can refer to [1]. We also review the constructions and properties of two binary Golay codes.

2.1 Incorrigible Sets

Assume C is an $[n, k, d]$ binary linear code, where n, k, and d are the code's length, dimension, and minimum distance, respectively. Assume $\boldsymbol{c} = (c_1, c_2, \cdots, c_n) \in C$. The set $\{l : c_l \neq 0\}$ is called the *support* of $\boldsymbol{c}$, denoted by $\mathrm{supp}(\boldsymbol{c})$. The size of $\mathrm{supp}(\boldsymbol{c})$, $|\mathrm{supp}(\boldsymbol{c})|$, is called the *weight* of $\mathbf{c}$, denoted by $\mathrm{wt}(\boldsymbol{c})$. Let $A_l (0 \leq l \leq n)$ be the number of codewords in C with weight l. The polynomial $A(x) = \sum_{l=0}^{n} A_l x^l$ is said to be the *weight enumerator* of C. It is evident that $A_0 = 1$ and $A_l = 0$ for $1 \leq l \leq d - 1$.

Let $\mathcal{D}$ be a subcode of C. The support of $\mathcal{D}$ is defined as $\mathrm{supp}(\mathcal{D}) = \bigcup_{\boldsymbol{c} \in \mathcal{D}} \mathrm{supp}(\boldsymbol{c})$. The size of $\mathrm{supp}(\mathcal{D})$ is called the *support weight* of $\mathcal{D}$. Let $A_i^{(r)}$ be the number of r-dimensional subcodes of C with support weight i for $1 \leq r \leq k$. The polynomial $A^{(r)}(x) = \sum_{l=0}^{n} A_l^{(r)} x^l$ is said to be the r-th *generalized weight enumerator* of C. By definition,

Manuscript received June 19, 2022.
Manuscript revised October 1, 2022.
Manuscript publicized October 31, 2022.

[†]The author is with the Faculty of Network and Telecommunication Engineering, Jinling Institute of Technology, Nanjing 211169, China.
[††]The author is with the Institute of Microelectronics of Chinese Academy of Sciences, Beijing 100029, China.
[†††]The author is with the Department of Mathematical Sciences, Tsinghua University, Beijing 100084, China.

*This work is supported in part by the NSFC under Grant 61871376 and in part by the JITSF under Grant jit-b-202110.

a) E-mail: kong@jit.edu.cn
b) E-mail: liuhaiyang@ime.ac.cn (Corresponding author)
c) E-mail: malian@tsinghua.edu.cn

DOI: 10.1587/transfun.2022EAL2054

we have $A^{(1)}(x) = A(x) - 1$.

Definition 1 ([1]): Let C be a binary linear code of length n. An *incorrigible set* $\mathcal{I}$ of C is a subset of $\{1, 2, \cdots, n\}$ such that $\mathcal{I}$ contains the support of a nonzero codeword in C. Let $I_l = |\{\mathcal{I} \text{ is an incorrigible set of } C : |\mathcal{I}| = l\}|$. The polynomial $I(x) = \sum_{l=0}^{n} I_l x^l$ is called the *incorrigible set enumerator* of C.

The following two lemmas are direct consequences of the definition.

Lemma 1 ([1]): Let C be a binary linear code specified by the parity-check matrix $\boldsymbol{H} = [\boldsymbol{h}_1, \boldsymbol{h}_2, \cdots, \boldsymbol{h}_n]$. Then a non-empty set $\mathcal{I} \subseteq \{1, 2, \cdots, n\}$ is incorrigible *if and only if* the set of column vectors $\{\boldsymbol{h}_l : l \in \mathcal{I}\}$ are linearly dependent.

Lemma 2 ([1]): With the above definition and notations, we have

$$I_l = \begin{cases} 0, & \text{if } 0 \le l \le d-1 \\ A_l, & \text{if } l = d \\ \binom{n}{l}, & \text{if } n-k+1 \le l \le n \end{cases} \tag{1}$$

for an $[n, k, d]$ binary linear code C, where $\binom{n}{l} = \frac{n!}{l!(n-l)!}$ is the binomial coefficient.

For $1 \le r \le k$, define

$$F_l^{(r)} = \sum_{j=0}^{n} \binom{n-j}{l-j} A_j^{(r)}. \tag{2}$$

It has been shown in [3] that

$$I_l = \sum_{r=1}^{k} (-1)^{r-1} 2^{\frac{r(r-1)}{2}} F_l^{(r)} \tag{3}$$

for a binary linear code C.

In practice, the incorrigible set enumerator can be used to *exactly* characterize the optimal decoding performance of a code over the BEC. Suppose the codewords in C is transmitted over a BEC with erasure probability ϵ. The probability of unsuccessful decoding for C under optimal decoding is given by [1]

$$p = \sum_{l=1}^{n} I_l \epsilon^l (1-\epsilon)^{n-l}. \tag{4}$$

2.2 Binary Golay Codes

Now we introduce the construction as well as several properties of binary $[24, 12, 8]$ Golay code $\mathcal{G}_{24}$ and $[23, 12, 7]$ Golay code $\mathcal{G}_{23}$. The code $\mathcal{G}_{24}$ is a self-dual code, whose parity-check matrix can be written as [5]

$$\boldsymbol{H} = [\boldsymbol{I}_{12} \mid \boldsymbol{P}], \tag{5}$$

where

$$\boldsymbol{P} = \begin{bmatrix} 0 & \mathbf{1} \\ \mathbf{1}^{\mathrm{T}} & \boldsymbol{A} \end{bmatrix}, \tag{6}$$

$\mathbf{1}$ is the all-one row vector of length 11. The matrix $\boldsymbol{A}$ is an 11×11 cyclic matrix whose first row is (1 1 0 1 1 1 0 0 0 1 0) and the i-th row is the cyclic shift of the $(i-1)$-th row for $2 \le i \le 11$.

The weight enumerator of $\mathcal{G}_{24}$ is $A(x) = 1 + 759x^8 + 2576x^{12} + 759x^{16} + x^{24}$. In addition, the minimum-weight codewords in $\mathcal{G}_{24}$ have the following nice property.

Lemma 3 ([6], [7]): There is a unique codeword of weight 8 in $\mathcal{G}_{24}$ that has ones in any five given coordinates.

Remark 1: Due to the above lemma, the number of codewords of weight 8 can be calculated as $\binom{24}{5}/\binom{8}{5} = 759$.

The code $\mathcal{G}_{23}$ is a perfect triple-error-correction code [5], [6], whose weight enumerator is $A(x) = 1 + 253x^7 + 506x^8 + 1288x^{11} + 1288x^{12} + 506x^{15} + 253x^{16} + x^{23}$. It is interesting to note that $\mathcal{G}_{23}$ can be obtained from $\mathcal{G}_{24}$ by puncturing the last coordinate from each codeword [6]. Furthermore, each codeword of weight 7 in $\mathcal{G}_{23}$ can be obtained from a codeword of weight 8 in $\mathcal{G}_{24}$ by puncturing the last coordinate with value 1 [6].

3. Main Results

In this section, we will present the main results of this letter. First, we provide a formula to represent the numbers of incorrigible sets of certain sizes using the weight enumerator of the code.

Theorem 1: Let $A(x) = \sum_{l=0}^{n} A_l x^l$ and $I(x) = \sum_{l=0}^{n} I_l x^l$ be the weight enumerator and the incorrigible set enumerator of an $[n, k, d]$ binary linear code C, respectively. Then

$$I_l = \sum_{i=d}^{l} A_i \binom{n-i}{l-i} \tag{7}$$

holds for $d \le l \le \lceil \frac{3}{2}d - 1 \rceil$.

Proof: By inspection, the theorem is true if $l = d$. Now consider $l > d$. Suppose $\boldsymbol{c}$ is a codeword in C of weight i and $\mathcal{S} = \mathrm{supp}(\boldsymbol{c})$, where $d \le i \le l \le \lceil \frac{3}{2}d - 1 \rceil$. Let $\mathcal{N} = \{1, 2, \cdots, n\}$ and $\bar{\mathcal{S}} = \mathcal{N} \backslash \mathcal{S}$. Suppose $\mathcal{I}$ is the set formed by the union of $\mathcal{S}$ and a subset of $\bar{\mathcal{S}}$ with size $l-i$. By definition, $\mathcal{I}$ is an incorrigible set of size l. Moreover, $\boldsymbol{c}$ is the unique codeword in C such that $\mathrm{supp}(\boldsymbol{c}) \subseteq \mathcal{I}$. (Otherwise, assume $\boldsymbol{c}'$ is another codeword in C satisfying $\mathrm{supp}(\boldsymbol{c}') \subseteq \mathcal{I}$. Then we have $l \ge \mathrm{wt}(\boldsymbol{c}) + \mathrm{wt}(\boldsymbol{c}') - |\mathrm{supp}(\boldsymbol{c}) \cap \mathrm{supp}(\boldsymbol{c}')|$, i.e., $|\mathrm{supp}(\boldsymbol{c}) \cap \mathrm{supp}(\boldsymbol{c}')| \ge \mathrm{wt}(\boldsymbol{c}) + \mathrm{wt}(\boldsymbol{c}') - l$. Since C is linear, $\boldsymbol{c} + \boldsymbol{c}'$ is also a codeword in C. Moreover,

$$\begin{aligned} \mathrm{wt}(\boldsymbol{c} + \boldsymbol{c}') &= \mathrm{wt}(\boldsymbol{c}) + \mathrm{wt}(\boldsymbol{c}') - 2|\mathrm{supp}(\boldsymbol{c}) \cap \mathrm{supp}(\boldsymbol{c}')| \\ &\le \mathrm{wt}(\boldsymbol{c}) + \mathrm{wt}(\boldsymbol{c}') - 2(\mathrm{wt}(\boldsymbol{c}) + \mathrm{wt}(\boldsymbol{c}') - l) \\ &= 2l - \mathrm{wt}(\boldsymbol{c}) - \mathrm{wt}(\boldsymbol{c}'). \end{aligned}$$

Since $l \le \lceil \frac{3}{2}d - 1 \rceil$, we have $2l < 3d$. This, together with $\mathrm{wt}(\boldsymbol{c}) \ge d$ and $\mathrm{wt}(\boldsymbol{c}') \ge d$, indicates that $\mathrm{wt}(\boldsymbol{c} + \boldsymbol{c}') < d$, a contradiction.) This, together with the facts that C has A_i codewords of weight i and $\bar{\mathcal{S}}$ has a total of $\binom{n-i}{l-i}$ subsets with size $l - i$, proves the theorem. □

Remark 2: For an $[n, k, d]$ binary linear code C such that $n - k \le \lceil \frac{3}{2}d - 1 \rceil$, we can obtain the incorrigible set enumerator of C using Theorem 1 and Lemma 2. It should be noted that such binary linear code is non-trivial.

Remark 3: A codeword $\boldsymbol{c}$ in a binary linear code C is

said to be *minimal* if there does not exist a codeword $\boldsymbol{c}'$ in C such that $\mathrm{supp}(\boldsymbol{c}') \subset \mathrm{supp}(\boldsymbol{c})$ (see e.g., [8]). In other words, $\boldsymbol{c}$ is the only codeword whose support is a subset of $\mathrm{supp}(\boldsymbol{c})$. It is known from [8, Lemma 2.1] that every codeword $\boldsymbol{c}$ in C such that $\mathrm{wt}(\boldsymbol{c}) \leq \left\lceil \frac{3}{2}d - 1 \right\rceil$ is minimal. On the other hand, we know from the proof of Theorem 1 that if an incorrigible set $\mathcal{I}$ of C satisfying $|\mathcal{I}| \leq \left\lceil \frac{3}{2}d - 1 \right\rceil$ contains the support of a codeword $\boldsymbol{c}$, then $\boldsymbol{c}$ is the only codeword in C whose support is a subset of $\mathcal{I}$.

We note that the numbers of incorrigible sets with sizes from d to $\left\lceil \frac{3}{2}d - 1 \right\rceil$ can also be calculated from Eqs. (2) and (3). Consider $r = 1$ in (2). Using the property that $A_j^{(1)} = 0$ for $1 \leq j < d$, we conclude that $F_l^{(1)} = \sum_{j=d}^{l} A_j^{(1)} \binom{n-j}{l-j}$. (By convention, $\binom{n}{m} = 0$ if $m > n$ or $m < 0$.) Now let us consider $2 \leq r \leq k$. We let

$$d_r = \min\{j : A_j^{(r)} > 0\}, \tag{8}$$

which is the *r-th generalized Hamming weight* of C [9]. We have $d_1 = d$. It is known that $d_i < d_j$ if $i < j$ [9]. As a consequence, we have $F_l^{(r)} = \sum_{j=d}^{l} A_j^{(r)} \binom{n-j}{l-j}$. Moreover, d_r satisfies the generalized Griesmer bound [9], i.e., $d_r \geq \sum_{i=0}^{r-1} \left\lceil \frac{d}{2^i} \right\rceil$. From (8), we conclude that $A_j^{(r)} = 0$ for $d \leq j \leq l \leq \left\lceil \frac{3}{2}d - 1 \right\rceil$. Hence, it holds that $F_l^{(r)} = 0$ for $2 \leq r \leq k$. Then we have $I_l = \sum_{j=d}^{l} A_j^{(1)} \binom{n-j}{l-j}$ according to (3). For $d \leq j \leq l$, we have $A_j^{(1)} = A_j$. In other words, Eqs. (2) and (3) can be brought into (7) for $d \leq l \leq \left\lceil \frac{3}{2}d - 1 \right\rceil$. Compared to (2) and (3), our formula (7) is formally simpler. It is known from (7) that we need at most $l - d + 1$ binomial coefficient computations, $l-d+1$ integer multiplications and $l-d$ integer additions to calculate I_l for a given $l (d \leq l \leq \left\lceil \frac{3}{2}d - 1 \right\rceil)$. If a code has few weights in the range between d and $\left\lceil \frac{3}{2}d - 1 \right\rceil$, the calculations can be further reduced.

Example 1: Consider the triple-error-correcting BCH code C, which is a $[15, 5, 7]$ cyclic code with generator polynomial $g(x) = 1 + x + x^2 + x^4 + x^5 + x^8 + x^{10}$ [5]. After listing the codewords in C, we obtain the weight enumerator of C is $A(x) = 1 + 15x^7 + 15x^8 + x^{15}$. By Theorem 1, we have $I_7 = A_7 = 15$, $I_8 = A_7\binom{8}{1} + A_8 = 135$, $I_9 = A_7\binom{8}{2} + A_8\binom{7}{1} = 525$, and $I_{10} = A_7\binom{8}{3} + A_8\binom{7}{2} = 1155$. Combing these results with Lemma 2, we have $I(x) = 15x^7 + 135x^8 + 525x^9 + 1155x^{10} + 1365x^{11} + 455x^{12} + 105x^{13} + 15x^{14} + x^{15}$.

Example 2: Suppose $C^{\perp}$ is the dual of the code provided in Example 1. It can be verified that $C^{\perp}$ is a code with parameters $[15, 10, 4]$, which contains all the codewords in the $[15, 11, 3]$ Hamming code with even weights. The weight enumerator of Hamming codes is provided in [5, Eq. (4.1)]. As a consequence, we conclude that the weight enumerator of $C^{\perp}$ is $A(x) = 1 + 105x^4 + 280x^6 + 435x^8 + 168x^{10} + 35x^{12}$. By Theorem 1, we have $I_4 = A_4 = 105$, $I_5 = A_4\binom{11}{1} = 1155$. Combing these results with Lemma 2, we have $I(x) = 105x^4 + 1155x^5 + 5005x^6 + 6435x^7 + 6435x^8 + 5005x^9 + 3003x^{10} + 1365x^{11} + 455x^{12} + 105x^{13} + 15x^{14} + x^{15}$.

In general, we cannot get the complete formula of $I(x)$ from Theorem 1. However, it is worth mentioning that the results in Theorem 1 allow us to make a better understanding on the code performance over the BEC.

Now we analyze several methods for approximating p, the probability of unsuccessful decoding for a code over a BEC with erasure probability ϵ, provided in (4). It is known that the probability p can be well approximated by

$$p^{(1)} = I_d \epsilon^d = A_d \epsilon^d \tag{9}$$

if ϵ is small [1]. However, the approximation $p^{(1)}$ is degraded as ϵ increases. In particular, if $\left(\frac{1}{A_d}\right)^{\frac{1}{d}} < \epsilon < 1$, we have $p^{(1)} > 1$, which becomes meaningless.

Using the results in Lemma 2, p can be approximated by

$$p^{(2)} = I_d \epsilon^d (1-\epsilon)^{n-d} + \sum_{l=n-k+1}^{n} I_l \epsilon^l (1-\epsilon)^{n-l}. \tag{10}$$

Our Theorem 1, together with the results in Lemma 2, suggests that p can be approximated by

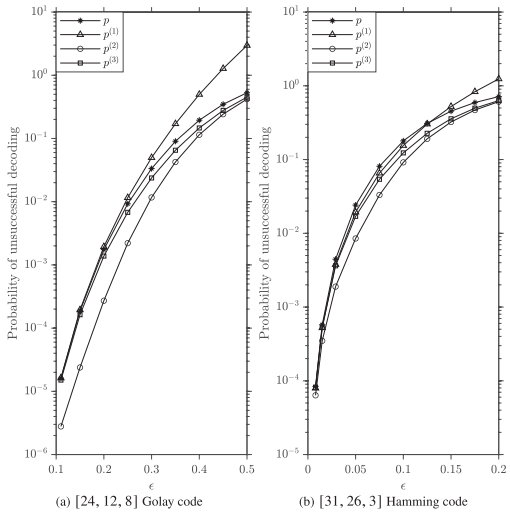
$$p^{(3)} = \sum_{l=d}^{\left\lceil \frac{3}{2}d-1 \right\rceil} I_l \epsilon^l (1-\epsilon)^{n-l} + \sum_{l=n-k+1}^{n} I_l \epsilon^l (1-\epsilon)^{n-l}. \tag{11}$$

Define $e^{(2)} = p - p^{(2)}$ and $e^{(3)} = p - p^{(3)}$. By calculation, we obtain $e^{(2)} \geq e^{(3)} \geq 0$. This indicates that the gap between p and $p^{(3)}$ is no larger than that between p and $p^{(2)}$ for a given ϵ. In order to compare the performance evaluations, we provide examples for two codes whose incorrigible set enumerators are known.

Example 3: Consider binary Golay code $\mathcal{G}_{24}$. By Theorem 1, we can get I_i for $8 \leq i \leq 11$. In [3, Table II], the values of I_i have been provided, from which $I(x)$ can be determined for $\mathcal{G}_{24}$. Figure 1(a) illustrates the performances of $\mathcal{G}_{24}$ under various methods. We can see from the figure that $p^{(1)}$ and $p^{(3)}$ are desirable if ϵ is small. As ϵ increases, $p^{(1)}$ becomes unsatisfactory. In particular, when ϵ is close to 0.5, $p^{(1)}$ is larger than 1, which is meaningless. In contrast, $p^{(2)}$ and $p^{(3)}$ can be used as approximations in this situation, in which $p^{(3)}$ is better than $p^{(2)}$. This indicates that the determination of I_i for $d < i \leq \left\lceil \frac{3}{2}d - 1 \right\rceil$ can help us better understand the code performance as a whole.

Example 4: Consider the $[31, 26, 3]$ Hamming code. By Theorem 1, we can get I_i for $i = 3$ and 4. For the code, the values of I_i can be calculated by [4, Eq. (23)], from which $I(x)$ can be determined for the code. We also evaluate the code performances using various approaches, as shown in Fig. 1(b). We can also conclude from the figure that our Theorem 1 can help us better understand the code performance as a whole.

Now we determine the incorrigible set enumerator of binary Golay codes $\mathcal{G}_{24}$ and $\mathcal{G}_{23}$ as an application of Theorem 1. In fact, the incorrigible set enumerator of $\mathcal{G}_{24}$ can be obtained using the results in [3, Table II]. However, our proof only uses the weight enumerator of $\mathcal{G}_{24}$ as well as some combinatorial methods. For the sake of completeness, the



(a) [24, 12, 8] Golay code (b) [31, 26, 3] Hamming code

Fig. 1 Performance comparisons of different approaches.

proof is also provided. Also, we note that the incorrigible set distributions of the dual of $\mathcal{G}_{23}$ are provided in [3, Table I].

Lemma 4: For $\mathcal{G}_{24}$, we have $I_{12} = 1313116$.

Proof: Assume $\mathcal{I}$ is an incorrigible set of $\mathcal{G}_{24}$ with size 12. Then $\mathcal{I}$ contains the support of a codeword $\boldsymbol{c}$ of weight 8 or 12 in $\mathcal{G}_{24}$ but not both. (Otherwise, $\mathcal{G}_{24}$ has a codeword of weight 4, a contradiction.) We consider the following two cases.

Case 1: $\mathrm{wt}(\boldsymbol{c}) = 12$. In this case, $\mathcal{I}$ is the support of a codeword of weight 12 in $\mathcal{G}_{24}$ and vice versa. We know from the weight enumerator of $\mathcal{G}_{24}$ that there are 2576 such incorrigible sets.

Case 2: $\mathrm{wt}(\boldsymbol{c}) = 8$. Let $\mathcal{N} = \{1, 2, \cdots, 24\}$. Suppose $\boldsymbol{c}$ is a codeword in $\mathcal{G}_{24}$ of weight 8 and $\mathcal{S} = \mathrm{supp}(\boldsymbol{c})$. Then, $\mathcal{I}$, the union of $\mathcal{S}$ and a subset of $\bar{\mathcal{S}}$ with size 4, is an incorrigible set of size 12, where $\bar{\mathcal{S}} = \mathcal{N}\backslash\mathcal{S}$. For each of the 759 minimum-weight codewords, we have $\binom{16}{4}$ ways to choose a subset of $\bar{\mathcal{S}}$ with size 4 and form such an incorrigible set of $\mathcal{G}_{24}$. On the other hand, it should be noted that some incorrigible sets of size 12 contain the supports of more than one codeword of weight 8 in $\mathcal{G}_{24}$.

Assume $\boldsymbol{c}$ and $\boldsymbol{c}'$ are different codewords of weight 8 in $\mathcal{G}_{24}$ whose supports are the subsets of an incorrigible set $\mathcal{I}$ of size 12. Let $\boldsymbol{c}'' = \boldsymbol{c} + \boldsymbol{c}'$. Then $\boldsymbol{c}'' = \boldsymbol{c} + \boldsymbol{c}'$ is also a codeword in $\mathcal{G}_{24}$, whose support is also a subset of $\mathcal{I}$. Since $|\mathrm{supp}(\boldsymbol{c}'')| = |\mathrm{supp}(\boldsymbol{c})| + |\mathrm{supp}(\boldsymbol{c}')| - 2|\mathrm{supp}(\boldsymbol{c}) \cap \mathrm{supp}(\boldsymbol{c}')|$, $\mathrm{supp}(\boldsymbol{c}) \subset \mathcal{I}$, and $\mathrm{supp}(\boldsymbol{c}') \subset \mathcal{I}$, it holds that $|\mathrm{supp}(\boldsymbol{c}) \cap \mathrm{supp}(\boldsymbol{c}')| \geq 4$, which implies $\mathrm{wt}(\boldsymbol{c}'') = |\mathrm{supp}(\boldsymbol{c}'')| \leq 8$. Because the minimum codeword weight of $\mathcal{G}_{24}$ is 8, we have $\mathrm{wt}(\boldsymbol{c}'') = 8$ and $|\mathrm{supp}(\boldsymbol{c}) \cap \mathrm{supp}(\boldsymbol{c}')| = 4$. In other words, $\mathcal{I}$ contains the supports of three minimum-weight codewords $\boldsymbol{c}$, $\boldsymbol{c}'$, and $\boldsymbol{c}''$. Moreover, $\boldsymbol{c}$, $\boldsymbol{c}'$, and $\boldsymbol{c}''$ are the only three minimum-weight codewords in $\mathcal{G}_{24}$ whose supports are the subsets of $\mathcal{I}$. (Otherwise, $\mathcal{G}_{24}$ contains a codeword of weight less than 8, a contradiction.)

Denote by T the number of triples $(\boldsymbol{c}, \boldsymbol{c}', \boldsymbol{c}'')$, where $\boldsymbol{c}$, $\boldsymbol{c}'$, and $\boldsymbol{c}''$ are the codewords of weight 8 in $\mathcal{G}_{24}$ satisfying $\boldsymbol{c}'' = \boldsymbol{c} + \boldsymbol{c}'$. From the above discussions, we conclude that the number of incorrigible sets of size 12 is given by $759\binom{16}{4} - 2T$ in this case. Now let us calculate the number T. Recall that $|\mathrm{supp}(\boldsymbol{c}) \cap \mathrm{supp}(\boldsymbol{c}')| = 4$ for the above triple. Assume $\mathcal{R}$ is a subset of $\mathcal{S} = \mathrm{supp}(\boldsymbol{c})$ with size 4. We know from Lemma 3 that for each $i \in \bar{\mathcal{S}}$ there is a unique codeword of weight 8 in $\mathcal{G}_{24}$ whose support contains i as well as the coordinates in the set $\mathcal{R}$. Since $|\bar{\mathcal{S}}| = 16$, we can obtain a list of 16 codewords, each of which occurs in the list four times. As a result, for any four given coordinates in $\mathrm{supp}(\boldsymbol{c})$, there are $16/4 = 4$ ways of choosing $\boldsymbol{c}'$ such that $\mathrm{supp}(\boldsymbol{c}')$ also contains these four coordinates. Since $\mathcal{G}_{24}$ has a total of 759 minimum-weight codewords, there are $4{\times}759\binom{8}{4}$ ways of choosing the codeword pairs $\boldsymbol{c}$ and $\boldsymbol{c}'$ in the above triple, and each pair is counted twice in this manner. Finally, because each triple contributes three such codeword pairs, T is $\frac{1}{2\times3} \times 4 \times 759\binom{8}{4} = 35420$. Hence, the number of incorrigible sets in this case is $759\binom{16}{4} - 2 \times 35420 = 1310540$.

Combining the above two cases, we have $I_{12} = 1310540 + 2576 = 1313116$. □

Theorem 2: The incorrigible set enumerator of $\mathcal{G}_{24}$ is $I(x) = 759x^8 + 12144x^9 + 91080x^{10} + 425040x^{11} + 1313116x^{12} + 2496144x^{13} + 1961256x^{14} + 1307504x^{15} + 735471x^{16} + 346104x^{17} + 134596x^{18} + 42504x^{19} + 10626x^{20} + 2024x^{21} + 276x^{22} + 24x^{23} + x^{24}$.

Proof: The theorem follows from Lemmas 2 and 4 as well as Theorem 1. □

Now let us consider $\mathcal{G}_{23}$. From Lemma 2 and Theorem 1, we only need to calculate I_{11} for the code.

Lemma 5: For $\mathcal{G}_{23}$, we have $I_{11} = 655270$.

Proof: Let $\mathcal{N} = \{1, 2, \cdots, 23\}$. Assume $\mathcal{I}$ is an incorrigible set of $\mathcal{G}_{23}$ with size 11. Then $\mathcal{I}$ contains the support of a codeword of weight 7 or 8 in $\mathcal{G}_{23}$. Suppose $\boldsymbol{c}$ (resp., $\boldsymbol{c}'$) is a codeword in $\mathcal{G}_{23}$ of weight 7 (resp., 8). Assume $\mathcal{S} = \mathrm{supp}(\boldsymbol{c})$, $\mathcal{S}' = \mathrm{supp}(\boldsymbol{c}')$, $\bar{\mathcal{S}} = \mathcal{N}\backslash\mathcal{S}$, and $\bar{\mathcal{S}}' = \mathcal{N}\backslash\mathcal{S}'$. Then, $\mathcal{I}$, the union of $\mathcal{S}$ (resp., $\mathcal{S}'$) and a subset of $\bar{\mathcal{S}}$ (resp., $\bar{\mathcal{S}}'$) with size 4 (resp., 3), is an incorrigible set of size 11. For each of the 253 codewords of weight 7, we have $\binom{16}{4}$ ways to choose a subset of $\bar{\mathcal{S}}$ with size 4 and form such an incorrigible set of $\mathcal{G}_{23}$. Similarly, for each of the 506 codewords of weight 8, we have $\binom{15}{3}$ ways to choose a subset of $\bar{\mathcal{S}}'$ with size 3 and form such an incorrigible set of $\mathcal{G}_{23}$. On the other hand, it should be noted that some incorrigible sets of size 11 contain the supports of more than one codeword of weight 7 or 8 in $\mathcal{G}_{23}$.

Using the similar method as in Case 2 of Lemma 4, we conclude that if an incorrigible set $\mathcal{I}$ of size 11 contains the supports of more than one codeword in $\mathcal{G}_{23}$, then it exactly contains the supports of three codewords $\boldsymbol{c}$, $\boldsymbol{c}'$, and $\boldsymbol{c}''$ in $\mathcal{G}_{23}$, two of which are of weight 7 and the remaining of which is of weight 8.

Denote by T the number of minimum-weight codeword pair $(\boldsymbol{c}, \boldsymbol{c}'')$ in $\mathcal{G}_{23}$ such that $\boldsymbol{c} + \boldsymbol{c}''$ is a codeword of weight 8. Then I_{11} is given by $253\binom{16}{4} + 506\binom{15}{3} - 2T$. Now let us calculate the number T. Recall the property that $\mathcal{G}_{23}$ can be obtained from $\mathcal{G}_{24}$ by puncturing the last coordinate from

each codeword. Denote by $\tilde{\boldsymbol{c}}$ and $\tilde{\boldsymbol{c}}''$ the codewords in $\mathcal{G}_{24}$ that correspond to $\boldsymbol{c}$ and $\boldsymbol{c}''$, respectively. Then the last coordinates of $\tilde{\boldsymbol{c}}$ and $\tilde{\boldsymbol{c}}''$ are both 1. Again, using the similar method as in Case 2 of Lemma 4, we conclude that for the last coordinate as well as any other three coordinates in $\mathrm{supp}(\tilde{\boldsymbol{c}})$, there are 4 ways of choosing $\tilde{\boldsymbol{c}}''$ such that $\mathrm{supp}(\tilde{\boldsymbol{c}}'')$ also contains these four coordinates. Because $\mathcal{G}_{24}$ has a total of 253 codewords of weight 8 whose last coordinate is 1, there are $4 \times 253\binom{7}{3}$ ways of choosing the codeword pair $(\tilde{\boldsymbol{c}}, \tilde{\boldsymbol{c}}'')$, and each pair is counted twice in this manner. Since there is a one-to-one correspondence between $(\boldsymbol{c}, \boldsymbol{c}'')$ and $(\tilde{\boldsymbol{c}}, \tilde{\boldsymbol{c}}'')$, the number T is $\frac{1}{2} \times 4 \times 253\binom{7}{3} = 17710$.

Hence, $I_{11} = 253\binom{16}{4}+506\binom{15}{3}-2\times17710 = 655270$. □

Theorem 3: The incorrigible set enumerator of $\mathcal{G}_{23}$ is $I(x) = 253x^7+4554x^8+37950x^9+194810x^{10}+655270x^{11}+1352078x^{12}+1144066x^{13}+817190x^{14}+490314x^{15}+245157x^{16}+100947x^{17}+33649x^{18}+8855x^{19}+1771x^{20}+253x^{21}+23x^{22}+x^{23}$.

Proof: The theorem is a direct consequence of Lemmas 2 and 5 as well as Theorem 1. □

4. Concluding Remarks

In this letter, we have provided a formula to represent the numbers of incorrigible sets of sizes between d and $\lceil \frac{3}{2}d - 1 \rceil$ for a binary linear code with minimum distance d, which is helpful in understanding the code performance over the BEC. We have also determined the incorrigible set enumerators of binary Golay codes $\mathcal{G}_{23}$ and $\mathcal{G}_{24}$.

Acknowledgments

The authors wish to thank the anonymous reviewer for the valuable suggestions.

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, March 2008.
[2] H. Hou, H. Liu, and L. Ma, "Some results on incorrigible sets of binary linear codes," IEICE Trans. Fundamentals, vol.E104-A, no.2, pp.582–586, Feb. 2021.
[3] L.-Z. Shen and F.-W. Fu, "The decoding error probability of linear codes over the erasure channel," IEEE Trans. Inf. Theory, vol.65, no.10, pp.6194–6203, Oct. 2019.
[4] Y. Jiang, S.-T. Xia, X.-J. Liu, and F.-W. Fu, "Incorrigible set distributions and unsuccessful decoding probability of linear codes," IEEE Int. Symp. Inf. Theory, Istanbul, Turkey, pp.1042–1046, July 2013.
[5] S. Lin and D.J. Costello, Jr., Error Correcting Coding: Fundamentals and Applications, 2nd ed., Prentice-Hall, Upper Saddle River, NJ, 2004.
[6] F.J. MacWilliams and N.J.A. Sloane, The Theory of Error-Correcting Codes, North-Holland, Amsterdam, The Netherlands, 1981.
[7] E.R. Berlekamp, "Decoding the Golay code," JPL Technical Report, vol.32-1526, pp.81–85, Oct. 1972.
[8] A. Ashikhmin and A. Barg, "Minimal vectors in linear codes," IEEE Trans. Inf. Theory, vol.44, no.5, pp.2010–2017, Sept. 1998.
[9] V.K. Wei, "Generalized Hamming weights for linear codes," IEEE Trans. Inf. Theory, vol.37, no.5, pp.1412–1418, Sept. 1991.