Weak Flip Codes and its Optimality on the Binary Erasure Channel

Final Report of MOST Project

"Ultra-Short Blocklength Communication"

Date:	01 November 2014
Project-Number:	NSC 100–2221–E–009–068–MY3
Project Duration:	1 August 2011 – 31 July 2014
Funded by:	Ministry of Science and Technology

Author:	Po-Ning Chen
Co-Authors:	Stefan M. Moser, Hsuan-Yin Lin
Organization:	Information Theory Laboratory Department of Electrical and Computer Engineering National Chiao Tung University
Address:	Engineering Building IV, Office 727 1001 Daxue Rd. Hsinchu 30010, Taiwan
E-mail:	qponing@gmail.com stefan.moser@ieee.org lin.hsuanyin@ieee.org

Abstract

Based on a new way of designing codes using codebook columns, a family of *nonlinear* codes, called *weak flip codes*, is presented and shown to contain many beautiful properties. In particular the subfamily *fair weak flip codes*, which goes back to definitions by Berlekamp, Gallager, and Shannon and which was shown to achieve the error exponent with a fixed number of codewords M, can be seen as a generalization of linear codes. It is then noted that the fair weak flip codes are related to binary nonlinear Hadamard codes: both code families maximize the minimum Hamming distance and meet the Plotkin bound. However, while the binary nonlinear Hadamard codes have only been shown to possess good Hamming-distance properties, the fair weak flip codes are proven to be globally optimal (in the sense of minimizing the error probability) among all codes (including both linear and nonlinear ones) for the binary erasure channel (BEC) for many values of the blocklength n and for a number of codewords M satisfying $\mathsf{M} \leq 6$. For the performance analysis, an extension of pairwise Hamming distance, the *r-wise Hamming distance*, is proposed and found to be a key to the understanding of the codes' performance.

Keywords: Binary erasure channel (BEC), channel capacity, finite blocklength, weak flip codes, fair weak flip codes, maximum likelihood (ML) decoder, minimum average error probability, optimal codes.

Contents

1 Introduction

A goal in traditional coding theory is to find good codes that operate close to the ultimate limit of the *channel capacity* as introduced by Shannon [1]. Implicitly, by the definition of capacity, such codes are expected to have a large blocklength. Moreover, due to the potential simplifications and because such codes behave well for large blocklength, conventional coding theory often restricts itself to *linear codes*. It is also quite common to use the *minimum Hamming distance* and the *weight*

enumerating function (WEF) as a design and quality criterion [2]. This is motivated by the equivalence of Hamming weight and Hamming distance for linear codes, and by the union bound that converts the global error probability into pairwise error probabilities.

In this work we would like to break away from these traditional simplifications and instead focus on an optimal[1] design of codes for finite blocklength. Since for very short blocklength it is not realistic to transmit large quantities of information, we start by looking at codes with only a few codewords, so called *ultrasmall block-codes*. Such codes have many practical applications, e.g., in the situation of establishing an initial connection in a wireless link. There the amount of information that needs to be transmitted during the setup of the link is limited to usually only a couple of bits, however, these bits need to be transmitted in very short time (e.g., blocklength in the range of $n = 20$ to $n = 30$) with the highest possible reliability [3].

While conventional coding theory in the sense of Shannon theory often focuses on stating important fundamental insights and properties like, e.g., what rates are possible to achieve and what rates are not achievable, we specifically turn our attention to the concrete *code design*, i.e., we are interested in actually finding a globally optimum code for a certain given channel and a given fixed blocklength.

In this report, we introduce a new class of codes, called *fair weak flip codes*, that have many beautiful properties similar to those of binary linear codes. However, while binary linear codes are very much limited since they can only exist if the number of codewords M happens to be an integer-power of 2, our class of codes exists for arbitrary[2] M. We will investigate these "quasi-linear" codes and show that they satisfy the Plotkin bound.

Fair weak flip codes are related to a class of binary nonlinear codes that are constructed with the help of Hadamard matrices and Levenshtein's theorem [4, Ch. 2]. These *binary nonlinear Hadamard codes* also meet the Plotkin bound. As a matter of fact, if for the parameters (M, n) of a given fair weak flip code there exists a Hadamard code, then these two codes are equivalent.[3] In this sense we can consider the fair weak flip codes to be a subclass of Hadamard codes. However, note that there is no guarantee that for every choice of parameters (M, n) for which fair weak flip codes exist, there also exists a corresponding Hadamard code.

Moreover, also note that while Levenshtein's method is only concerned with an optimal Hamming distance structure, we will show that fair weak flip codes are globally optimal (i.e., they are the best with respect to error probability and not only pairwise Hamming distance, and they are best among *all* codes, linear or nonlinear!) for the *binary erasure channel (BEC)*. We prove this optimality in the case of the number of codewords $\mathsf{M} \leq 6$. Our analysis is based on a new generalized definition of the Hamming distance, the *r-wise Hamming distance*. This is a parameter vector that completely describes the exact average error probability of a code.

We also define a class of codes called *weak flip codes* that contains the fair weak flip codes as a special case. We prove that some particular weak flip codes are optimal for the BEC for $\mathsf{M} \leq 4$ and for *any* finite blocklength n, or for $\mathsf{M} = 5, 6$ and for blocklength n being a multiple of 10.

This work is an extension of our previous work [5], [6], where we study ultrasmall block-codes for the situation of general binary-input binary-output channels and where we derive the optimal code design for the two special cases of the *Z-channel*

[1] By *optimal* we always mean *minimum error probability*.
[2] Note that fair weak flip codes do not exist for all blocklength n.
[3] For a precise definition of *equivalence* see Remark 12.

(ZC) and the *binary symmetric channel (BSC)*. We will also briefly compare our findings here with these channels, especially with the symmetric BSC.

The foundations of our insights lie in a new powerful way of creating and analyzing both linear and nonlinear block-codes. As is customary, we use the *codebook matrix* containing the codewords in its rows to describe our codes. However, for our code construction and performance analysis, we look at this codebook matrix not row-wise, but *column-wise*. All our proofs and also our definitions of the new r-wise Hamming distance and the "quasi-linear" codes are fully based on this new approach. (This is another fundamental difference between our results and the binary nonlinear Hadamard codes that are constructed based on Hadamard matrices and Levenshtein's theorem [4].)

The remainder of this report is structured as follows. After some comments about our notation, we will introduce the channel model and review some common definitions in Section 2. In Section 3 we introduce the family of *weak flip codes* including its subfamily of *fair weak flip codes* and compare it to the well-known binary nonlinear Hadamard codes. Section 4 reviews some previous results. The main results are then summarized and discussed in Sections 5 and 6: Section 5 provides the definition of the r-wise Hamming distance and discusses the quasi-linear properties of weak flip codes, and in Section 6 the BEC and its optimal codes are presented. We conclude in Section 7. Many of the lengthy proofs are postponed to the appendix.

As a convention in coding theory, vectors (denoted by bold face Roman letters, e.g., $\mathbf{x}$) are row-vectors. However, for simplicity of notation and to avoid a large number of transpose-signs, we slightly misuse this notational convention for one special case: any vector $\mathbf{c}$ is a column-vector. It should be always clear from the context because these vectors are used to build codebook matrices and are therefore also conceptually quite different from the transmitted codeword $\mathbf{x}$ or the received sequence $\mathbf{y}$. Moreover, we use a bar $\bar{\mathbf{x}}$ to denote the flipped version of $\mathbf{x}$, i.e., $\bar{\mathbf{x}} \triangleq \mathbf{x} \oplus \mathbf{1}$ (where $\oplus$ denotes the componentwise XOR operation and where $\mathbf{1}$ is the all-one vector). We use capital letters for random quantities, e.g., X, and small letters for deterministic counterparts, e.g., x; constants are depicted by Greek letters, small Romans, or a special font, e.g., M; sets are denoted by calligraphic letters, e.g., $\mathcal{M}$; and $|\mathcal{M}|$ denotes the cardinality of the set $\mathcal{M}$.

2 Channel Model and Coding Schemes

2.1 Discrete Memoryless Channel

The probably most fundamental model describing communication over a noisy channel is the so-called *discrete memoryless channel (DMC)*. A DMC consists of a

- a finite input alphabet $\mathcal{X}$;
- a finite output alphabet $\mathcal{Y}$; and
- a conditional probability distribution $P_{Y|X}(\cdot|x)$ for all $x \in \mathcal{X}$ such that

$$P_{Y_k|X_1,X_2,\ldots,X_k,Y_1,Y_2,\ldots,Y_{k-1}}(y_k|x_1,x_2,\ldots,x_k,y_1,y_2,\ldots,y_{k-1}) = P_{Y|X}(y_k|x_k) \qquad \forall\, k. \quad (1)$$

Note that a DMC is called *memoryless* because the current output Y_k depends only on the current input x_k. Moreover also note that the channel is *time-invariant* in

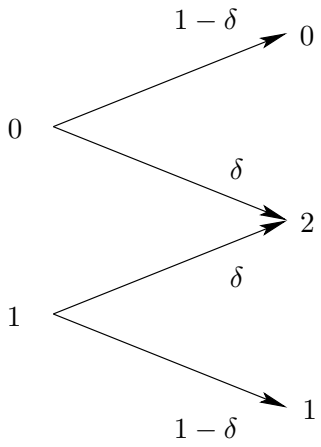

Figure 1: The binary erasure channel (BEC) with erasure probability δ. The channel output 2 corresponds to an erasure.

the sense that for a particular input x_k, the distribution of the output Y_k does not change over time.

Definition 1. We say a DMC is used *without feedback*, if

$$P(x_k|x_1,\ldots,x_{k-1},y_1,\ldots,y_{k-1}) = P(x_k|x_1,\ldots,x_{k-1}) \quad \forall\, k, \tag{2}$$

i.e., X_k depends only on past inputs (by choice of the encoder), but not on past outputs. Hence, there is no feedback link from the receiver back to the transmitter that would inform the transmitter about the last outputs.

Note that even though we assume the channel to be memoryless, we do *not* restrict the encoder to be memoryless! We now have the following theorem.

Theorem 2. *If a DMC is used without feedback, then*

$$P(y_1,\ldots,y_n|x_1,\ldots,x_n) = \prod_{k=1}^{n} P_{Y|X}(y_k|x_k) \quad \forall\, n \geq 1. \tag{3}$$

Proof: See, e.g., [7]. □

In this work, we consider the well-known *binary erasure channel (BEC)* given in Figure 1. The BEC is a discrete memoryless channel (DMC) with a binary input alphabet $\mathcal{X} = \{0,1\}$ and a ternary output alphabet $\mathcal{Y} = \{0,1,2\}$, and with a conditional channel law

$$P_{Y|X}(y|x) = \begin{cases} 1-\delta & \text{if } y = x,\ x \in \{0,1\}, \\ \delta & \text{if } y = 2,\ x \in \{0,1\}. \end{cases} \tag{4}$$

Here $0 \leq \delta < 1$ is called the *erasure probability*.

While we exclusively focus on the BEC, we will sometimes briefly compare our results with the situation of the *binary symmetric channel (BSC)*, in particular, in view of [6]. The BSC is a binary-input, binary-output DMC with conditional channel law

$$P_{Y|X}(y|x) = \begin{cases} 1-\epsilon & \text{if } y = x,\ x \in \{0,1\}, \\ \epsilon & \text{if } y = 1-x,\ x \in \{0,1\}, \end{cases} \tag{5}$$

where $0 \leq \epsilon < \frac{1}{2}$ is called *crossover probability*.

2.2 Coding for DMC

We next review some common definitions.

Definition 3. An (M, n) *coding scheme* for a DMC $(\mathcal{X}, \mathcal{Y}, P_{Y|X})$ consists of the message set $\mathcal{M} \triangleq \{1, 2, \ldots, \mathsf{M}\}$, a codebook $\mathscr{C}^{(\mathsf{M},n)}$ with M length-n codewords $\mathbf{x}_m = (x_{m,1}, x_{m,2}, \ldots, x_{m,n}) \in \mathcal{X}^n$, $m \in \mathcal{M}$, an encoder that maps every message m into its corresponding codeword $\mathbf{x}_m$, and a decoder that makes a decoding decision $g(\mathbf{y}) \in \mathcal{M}$ for every received n-vector $\mathbf{y} \in \mathcal{Y}^n$.

The set of codewords $\mathscr{C}^{(\mathsf{M},n)}$ is called (M, n) *codebook* or simply (M, n) *code*. Sometimes we follow the custom of traditional coding theory and use three parameters: (M, n, d) *code*, where the third parameter d denotes the *minimum Hamming distance* $d_{\min}\big(\mathscr{C}^{(\mathsf{M},n)}\big)$, i.e., the minimum number of components in which any two codewords differ.

Definition 4. A codebook is called *linear* if it can be seen as a subspace of the n-dimensional vector space over the channel input alphabet.[4]

Note that a linear code always contains the all-zero codeword. For more details see, e.g., [2], [4].

We assume that the M possible messages are equally likely and g is the *maximum likelihood (ML) decoder*[5]

$$g(\mathbf{y}) \triangleq \operatorname*{argmax}_{1 \le m \le \mathsf{M}} P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y}|\mathbf{x}_m), \tag{6}$$

and we define the decoding region for each codeword as follows.

Definition 5. For a given code $\mathscr{C}^{(\mathsf{M},n)}$ we define the *decoding region* $\mathcal{D}_m^{(\mathsf{M},n)}$ corresponding to the mth codeword $\mathbf{x}_m$ as

$$\mathcal{D}_m^{(\mathsf{M},n)} \triangleq \{\mathbf{y} \colon g(\mathbf{y}) = m\}. \tag{7}$$

Note that in Definition 5, all decoding regions must be disjoint, and their union be equal to $\mathcal{Y}^n$

$$\mathcal{D}_m^{(\mathsf{M},n)} \cap \mathcal{D}_{m'}^{(\mathsf{M},n)} = \emptyset, \quad 1 \le m < m' \le \mathsf{M}, \tag{8}$$

$$\bigcup_{m \in \mathcal{M}} \mathcal{D}_m^{(\mathsf{M},n)} = \mathcal{Y}^n. \tag{9}$$

Under the ML rule, unfortunately, there does not necessarily exist a unique m such that for a given $\mathbf{y}$,

$$P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y}|\mathbf{x}_m) = \max_{1 \le m' \le \mathsf{M}} P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y}|\mathbf{x}_{m'}), \tag{10}$$

i.e., $\mathbf{y}$ could be assigned to different decoding regions without changing the performance of the coding scheme. In the following we define *closed decoding regions* that break the condition (8).

[4] Being a subspace, linear codes usually are represented by a generator matrix, which is basically a basis of the subspace. As we are not interested in linear codes in particular, but in both linear and nonlinear codes, we will not use generator matrices in this work.

[5] Under the assumption of equally likely messages, the ML decoding rule is equivalent to the *maximum a posteriori (MAP)* decoding rule, i.e., for a given code and DMC, it minimizes the average error probability as defined in (14) among all possible decoders.

Definition 6. The *closed decoding region* $\overline{\mathcal{D}}_m^{(\mathsf{M},n)}$ corresponding to the mth codeword $\mathbf{x}_m$ is defined as

$$\overline{\mathcal{D}}_m^{(\mathsf{M},n)} \triangleq \Big\{\mathbf{y}\colon P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y}|\mathbf{x}_m) = \max_{1\le m'\le \mathsf{M}} P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y}|\mathbf{x}'_m)\Big\}, \quad m \in \mathcal{M}. \tag{11}$$

Note that $\mathcal{D}_m^{(\mathsf{M},n)} \subseteq \overline{\mathcal{D}}_m^{(\mathsf{M},n)}$.

Definition 7. Given that message m has been sent, let λ_m be the *probability of decoding error* for an (M, n) code with blocklength n:

$$\lambda_m\big(\mathscr{C}^{(\mathsf{M},n)}\big) \triangleq \Pr[g(\mathbf{Y}) \neq m|\mathbf{X} = \mathbf{x}_m] \tag{12}$$

$$= \sum_{\mathbf{y}\notin\mathcal{D}_m^{(\mathsf{M},n)}} P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y}|\mathbf{x}_m). \tag{13}$$

The *average error probability* P_e of an (M, n) code is defined as

$$P_\mathrm{e}\big(\mathscr{C}^{(\mathsf{M},n)}\big) \triangleq \frac{1}{\mathsf{M}}\sum_{m=1}^{\mathsf{M}} \lambda_m\big(\mathscr{C}^{(\mathsf{M},n)}\big). \tag{14}$$

Sometimes it will be more convenient to focus on the probability of not making any error, denoted *success probability* ψ_m:

$$\psi_m\big(\mathscr{C}^{(\mathsf{M},n)}\big) \triangleq \Pr[g(\mathbf{Y}) = m|\mathbf{X} = \mathbf{x}_m] \tag{15}$$

$$= \sum_{\mathbf{y}\in\mathcal{D}_m^{(\mathsf{M},n)}} P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y}|\mathbf{x}_m) \tag{16}$$

$$\triangleq \Pr\big[\mathbf{Y} \in \mathcal{D}_m^{(\mathsf{M},n)}\big|\mathbf{X} = \mathbf{x}_m\big]. \tag{17}$$

The definition of the *average success probability*[6] P_c follows accordingly.

The most famous relation between code rate and error probability has been derived by Shannon in his landmark paper from 1948 [1].

Theorem 8 (The Channel Coding Theorem for a DMC). *Define*

$$\mathsf{C} \triangleq \max_{P_X(\cdot)} I(X;Y) \tag{18}$$

where X and Y have to be understood as input and output of a DMC and where the maximization is over all input distributions $P_X(\cdot)$.

Then for every $\mathsf{R} < \mathsf{C}$ there exists a sequence of $(2^{n\mathsf{R}}, n)$ coding schemes with maximum error probability $\lambda^{(n)} \to 0$ as the blocklength n gets very large.

Conversely, any sequence of $(2^{n\mathsf{R}}, n)$ coding schemes with maximum error probability $\lambda^{(n)} \to 0$ must have a rate $\mathsf{R} \le \mathsf{C}$.

So we see that C denotes the maximum rate at which reliable communication is possible. Therefore C is called ***channel capacity****.*

Note that this theorem considers only the situation of n tending to infinity and thereby the error probability going to zero. However, in a practical system, we cannot allow the blocklength n to be too large because of delay and complexity. On the other hand it is not necessary to have zero error probability either.

[6] The subscript "c" stands for "correct."

So the question arises what we can say about "capacity" for finite n, i.e., if we allow a certain maximal probability of error, what is the smallest necessary blocklength n to achieve it? Or, vice versa, fixing a certain short blocklength n, what is the best average error probability that can be achieved? And, what is the optimal code structure for a given channel?

Our goal is to find the structure of a code that minimizes the average error probability among all codes based on the ML decoding rule.

Definition 9. A code $\mathscr{C}^{(\mathsf{M},n)}$ is called *optimal* and denoted by $\mathscr{C}^{(\mathsf{M},n)*}$ if

$$P_{\mathrm{e}}\big(\mathscr{C}^{(\mathsf{M},n)*}\big) \leq P_{\mathrm{e}}\big(\mathscr{C}^{(\mathsf{M},n)}\big) \tag{19}$$

for any (linear or nonlinear) code $\mathscr{C}^{(\mathsf{M},n)}$.

3 Preliminaries

3.1 Capacity of the BEC

The capacity of a BEC is given by

$$\mathsf{C}_{\mathrm{BEC}} = 1 - \delta \tag{20}$$

bits. Then input distribution $P_X^*(\cdot)$ that achieve the capacity is the uniform distribution given by

$$P_X^*(0) = 1 - P_X^*(1) = \frac{1}{2}. \tag{21}$$

3.2 Average Error (and Success) Probability of the BEC

We start with the following definitions.

Definition 10. By $d_{\alpha,\beta}(\mathbf{x}_m, \mathbf{y})$ we denote the number of positions j where $x_{m,j} = \alpha$ and $y_j = \beta$. For $m \neq m'$, the *joint composition* $q_{\alpha,\beta}(m, m')$ of two codewords $\mathbf{x}_m$ and $\mathbf{x}_{m'}$ is defined as

$$q_{\alpha,\beta}(m, m') \triangleq \frac{d_{\alpha,\beta}(\mathbf{x}_m, \mathbf{x}_{m'})}{n}. \tag{22}$$

Note that $d_{\mathrm{H}}(\cdot,\cdot) \triangleq d_{0,1}(\cdot,\cdot) + d_{1,0}(\cdot,\cdot)$ and $w_{\mathrm{H}}(\mathbf{x}) \triangleq d_{\mathrm{H}}(\mathbf{x}, \mathbf{0})$ denote the commonly used Hamming distance and Hamming weight, respectively.

Definition 11. By $\mathsf{N}(\alpha|\mathbf{y})$ we denote the number of occurrences of a symbol α in a received vector $\mathbf{y}$, and $\mathcal{I}(\alpha|\mathbf{y})$ is defined as the set of indices j such that $y_j = \alpha$. I.e., $\mathsf{N}(\alpha|\mathbf{y}) = |\mathcal{I}(\alpha|\mathbf{y})|$. Moreover, we use $\mathbf{x}_{m,\mathcal{I}(\alpha|\mathbf{y})}$ to describe a vector of length $\mathsf{N}(\alpha|\mathbf{y})$ containing the components $x_{m,j}$ where $j \in \mathcal{I}(\alpha|\mathbf{y})$. We also write $\mathbf{x}_{m,\mathcal{I}(\alpha|\mathbf{y})} \cup \mathbf{x}_{m,\mathcal{I}(\mathcal{Y}\setminus\{\alpha\}|\mathbf{y})}$ for the complete vector $\mathbf{x}_m$, where the "union"-operation implicitly re-sorts the indices in the usual ascending order.

The error probability formula of transmitting code $\mathscr{C}^{(\mathsf{M},n)}$ over the BEC can be written as

$$P_{\mathrm{e}}\big(\mathscr{C}^{(\mathsf{M},n)}\big) = \frac{1}{\mathsf{M}} \sum_{m=1}^{\mathsf{M}} \sum_{\substack{\mathbf{y} \\ g(\mathbf{y}) \neq m}} (1-\delta)^{n-\mathsf{N}(2|\mathbf{y})}\, \delta^{\mathsf{N}(2|\mathbf{y})}\, \mathrm{I}\big\{d_{\mathrm{H}}\big(\mathbf{x}_{m,\mathcal{I}(b|\mathbf{y})}, \mathbf{y}_{\mathcal{I}(b|\mathbf{y})}\big) = 0\big\}, \tag{23}$$

where $b \in \{0,1\}$, and $\mathrm{I}\{\cdot\}$ denotes the indicator function whose value is 1 if the statement is correct and 0 otherwise.

The success probability accordingly is

$$P_{\mathrm{c}}\big(\mathscr{C}^{(\mathsf{M},n)}\big) = \frac{1}{\mathsf{M}} \sum_{m=1}^{\mathsf{M}} \sum_{\substack{\mathbf{y} \\ g(\mathbf{y})=m}} (1-\delta)^{n-\mathsf{N}(2|\mathbf{y})}\, \delta^{\mathsf{N}(2|\mathbf{y})}\, \mathrm{I}\big\{d_{\mathrm{H}}\big(\mathbf{x}_{m,\mathcal{I}(b|\mathbf{y})}, \mathbf{y}_{\mathcal{I}(b|\mathbf{y})}\big) = 0\big\}. \quad (24)$$

3.3 General Binary Codes Description

Usually, a general codebook $\mathscr{C}^{(\mathsf{M},n)}$ with M codewords and with a blocklength n is written as an $\mathsf{M} \times n$ *codebook matrix* where the M rows correspond to the M codewords:

$$\mathscr{C}^{(\mathsf{M},n)} = \begin{pmatrix} — \ \mathbf{x}_1 \ — \\ \vdots \\ — \ \mathbf{x}_{\mathsf{M}} \ — \end{pmatrix} = \begin{pmatrix} | & | & & | \\ \mathbf{c}_1 & \mathbf{c}_2 & \cdots & \mathbf{c}_n \\ | & | & & | \end{pmatrix}. \quad (25)$$

In our approach, we prefer to consider the codebook *column-wise* rather than row-wise [6]. We denote the (length-M) column-vectors of the codebook by $\mathbf{c}_j$, $j \in \{1,\ldots,n\}$.

Remark 12. Since we assume equally likely messages, any permutation of rows only changes the assignment of codewords to messages and has therefore no impact on the performance. We thus consider two codes with permuted rows as being *equal* (this agrees with the concept of a code being a *set* of codewords, where the ordering of the codewords is irrelevant). Furthermore, since we only consider memoryless channels, any permutation of the columns of $\mathscr{C}^{(\mathsf{M},n)}$ will lead to another code with identical error probability. We say that such two codes are *equivalent*. We would like to emphasize that two codes being equivalent is not the same as two codes being equal. However, as we are mainly interested in the performance of a code, we usually treat two equivalent codes as being the same.

Due to the symmetry of the BEC[7] we have an additional equivalence in the codebook design (compare also with the BSC [6]).

Lemma 13. *Consider an arbitrary code $\mathscr{C}^{(\mathsf{M},n)}$ to be used on the BEC and consider an arbitrary M-vector $\mathbf{c}$. Construct a new length-$(n+1)$ code $\mathscr{C}^{(\mathsf{M},n+1)}$ by appending $\mathbf{c}$ to the codebook matrix of $\mathscr{C}^{(\mathsf{M},n)}$ and another new length-$(n+1)$ code $\bar{\mathscr{C}}^{(\mathsf{M},n+1)}$ by appending the flipped vector $\bar{\mathbf{c}} = \mathbf{c} \oplus \mathbf{1}$ to the codebook matrix of $\mathscr{C}^{(\mathsf{M},n)}$. Then the performance of these two new codes are identical:*

$$P_{\mathrm{e}}^{(n+1)}\big(\mathscr{C}^{(\mathsf{M},n+1)}\big) = P_{\mathrm{e}}^{(n+1)}\big(\bar{\mathscr{C}}^{(\mathsf{M},n+1)}\big). \quad (26)$$

Note that Lemma 13 cannot be generalized further, i.e., for some $\mathscr{C}^{(\mathsf{M},n)}$, appending a vector $\tilde{\mathbf{c}}$ other than $\bar{\mathbf{c}}$ may result in a length-$(n+1)$ code $\tilde{\mathscr{C}}^{(\mathsf{M},n+1)}$ that is not equivalent to $\mathscr{C}^{(\mathsf{M},n+1)}$.

Next we define a convenient numbering system for the possible columns of the codebook matrix of binary codes.

[7] The symmetry property here is identical to the symmetry definitions in [8, p. 94]. Hence, it is not surprising that Lemma 13 also holds for general binary-input symmetric channels.

Definition 14. For fixed M and $b_m \in \{0,1\}$, $m \in \mathcal{M}$, we describe the column vector $(b_1\ b_2\ \cdots\ b_{\mathsf{M}})^{\mathsf{T}}$ by its reverse binary representation of nonnegative integers

$$j = \sum_{m=1}^{\mathsf{M}} b_m\, 2^{\mathsf{M}-m}, \tag{27}$$

and write $\mathbf{c}_j^{(\mathsf{M})} \triangleq (b_1\ b_2\ \cdots\ b_{\mathsf{M}})^{\mathsf{T}}$.

Due to Lemma 13, we discard any column starting with a one, i.e., we require $b_1 = 0$. Moreover, as it will never help to improve the performance, we exclude the all-zero column. Hence, the set of all possible *candidate columns* of general binary codes can be restricted to

$$\mathcal{C}^{(\mathsf{M})} \triangleq \left\{\mathbf{c}_1^{(\mathsf{M})}, \mathbf{c}_2^{(\mathsf{M})}, \ldots, \mathbf{c}_{2^{\mathsf{M}-1}-1}^{(\mathsf{M})}\right\}. \tag{28}$$

For a given codebook and for any $j \in \mathcal{J} \triangleq \{1, \ldots, 2^{\mathsf{M}-1}-1\}$, let t_j denote the number of the corresponding candidate columns $\mathbf{c}_j^{(\mathsf{M})}$ appearing in the codebook matrix of $\mathscr{C}^{(\mathsf{M},n)}$. Because of Remark 12, the ordering of the candidate columns is irrelevant, and any binary code with blocklength

$$n = \sum_{j=1}^{2^{\mathsf{M}-1}-1} t_j \tag{29}$$

can therefore be described completely by the parameter vector

$$\mathbf{t} \triangleq \left[t_1, t_2, \ldots, t_{2^{\mathsf{M}-1}-1}\right]. \tag{30}$$

We say that such a code has *type* $\mathbf{t}$ and write[8] $\mathscr{C}^{(\mathsf{M},n)}_{t_1,\ldots,t_{2^{\mathsf{M}-1}-1}}$ or simply $\mathscr{C}^{(\mathsf{M},n)}_{\mathbf{t}}$.

Example 15. For $\mathsf{M} = 3, 4$, the candidate columns sets are

$$\mathcal{C}^{(3)} = \left\{\mathbf{c}_1^{(3)} = \begin{pmatrix}0\\0\\1\end{pmatrix},\ \mathbf{c}_2^{(3)} \triangleq \begin{pmatrix}0\\1\\0\end{pmatrix},\ \mathbf{c}_3^{(3)} \triangleq \begin{pmatrix}0\\1\\1\end{pmatrix}\right\}, \tag{31}$$

$$\mathcal{C}^{(4)} = \left\{\mathbf{c}_1^{(4)} = \begin{pmatrix}0\\0\\0\\1\end{pmatrix},\ \mathbf{c}_2^{(4)} \triangleq \begin{pmatrix}0\\0\\1\\0\end{pmatrix},\ \mathbf{c}_3^{(4)} \triangleq \begin{pmatrix}0\\0\\1\\1\end{pmatrix},\right.$$
$$\left.\mathbf{c}_4^{(4)} = \begin{pmatrix}0\\1\\0\\0\end{pmatrix},\ \mathbf{c}_5^{(4)} \triangleq \begin{pmatrix}0\\1\\0\\1\end{pmatrix},\ \mathbf{c}_6^{(4)} \triangleq \begin{pmatrix}0\\1\\1\\0\end{pmatrix},\ \mathbf{c}_7^{(4)} \triangleq \begin{pmatrix}0\\1\\1\\1\end{pmatrix}\right\}. \tag{32}$$

A codebook $\mathscr{C}^{(4,7)}_{\mathbf{t}}$ of type $\mathbf{t} = [2,0,2,0,2,1,0]$ is equivalent to all the columns permutations of the following codebook:

$$\begin{pmatrix}0&0&0&0&0&0&0\\0&0&0&0&1&1&1\\0&0&1&1&0&0&1\\1&1&1&1&1&1&0\end{pmatrix}. \tag{33}$$

$\Diamond$

[8] Note that sometimes, for the sake of convenience, we will omit the superscripts (M, n) or (M).

3.4 Weak Flip Codes and Hadamard Codes

We next introduce some special families of binary codes.

Definition 16. Given an integer $\mathsf{M} \geq 2$, a length-M candidate column is called a *weak flip column* and denoted $\mathbf{c}_{\text{weak}}^{(\mathsf{M})}$ if its first component is 0 and its Hamming weight equals to $\lfloor \frac{\mathsf{M}}{2} \rfloor$ or $\lceil \frac{\mathsf{M}}{2} \rceil$. The collection of all possible weak flip columns is called *weak flip candidate columns set* and is denoted by $\mathcal{C}_{\text{weak}}^{(\mathsf{M})}$, and the remaining, nonweak flip candidate columns are collected in $\mathcal{C}_{\text{nonweak}}^{(\mathsf{M})}$.

We see that a weak flip column contains an almost equal number of zeros and ones. For the remainder of this report, we introduce the following shorthands:

$$\mathsf{J} \triangleq 2^{\mathsf{M}-1} - 1, \quad \bar{\ell} \triangleq \left\lceil \frac{\mathsf{M}}{2} \right\rceil, \quad \underline{\ell} \triangleq \left\lfloor \frac{\mathsf{M}}{2} \right\rfloor, \quad \mathsf{L} \triangleq \binom{2\bar{\ell}-1}{\bar{\ell}}. \tag{34}$$

Lemma 17. *The cardinality of a weak flip candidate columns set is*

$$\left|\mathcal{C}_{\text{weak}}^{(\mathsf{M})}\right| = \mathsf{L} \tag{35}$$

and the cardinality of the nonweak flip candidate columns set is

$$\left|\mathcal{C}_{\text{nonweak}}^{(\mathsf{M})}\right| = \mathsf{J} - \mathsf{L}. \tag{36}$$

Proof: If $\mathsf{M} = 2\bar{\ell}$, then we have $\binom{2\bar{\ell}-1}{\bar{\ell}}$ possible choices of weak flip columns, while if $\mathsf{M} = 2\bar{\ell} - 1$, we have $\binom{2\bar{\ell}-2}{\bar{\ell}-1} + \binom{2\bar{\ell}-2}{\bar{\ell}} = \binom{2\bar{\ell}-1}{\bar{\ell}}$ choices.

Since in total we have J candidate columns, (36) follows directly from (35). It can also be computed as

$$\left|\mathcal{C}_{\text{nonweak}}^{(\mathsf{M})}\right| = \sum_{h=1}^{\underline{\ell}-1} \binom{\mathsf{M}-1}{h} + \sum_{h=\bar{\ell}+1}^{\mathsf{M}-1} \binom{\mathsf{M}-1}{h} = \mathsf{J} - \mathsf{L}. \tag{37}$$

□

Remark 18. The above lemma assures that the cardinalities of weak flip candidate column sets respectively for $\mathsf{M} = 2\bar{\ell} - 1$ and $\mathsf{M} = 2\bar{\ell}$ are the same for any positive integer $\bar{\ell}$, and both are given by $\binom{2\bar{\ell}-1}{\bar{\ell}}$. An important observation is that appending a one to all weak flip columns of weight $\underline{\ell} = \bar{\ell} - 1$ in $\mathcal{C}_{\text{weak}}^{(2\bar{\ell}-1)}$ and appending a zero to all weak flip columns of weight $\bar{\ell}$ in $\mathcal{C}_{\text{weak}}^{(2\bar{\ell}-1)}$ will result in $\mathcal{C}_{\text{weak}}^{(2\bar{\ell})}$. Hence, $\mathcal{C}_{\text{weak}}^{(2\bar{\ell}-1)}$ is obtained from $\mathcal{C}_{\text{weak}}^{(2\bar{\ell})}$ by removing the last bit from all column vectors. See for example (40) and (41) below.

Definition 19. A *weak flip code* is constructed only by weak flip columns. Since in its type (see (30)) all positions corresponding to nonweak flip columns are zero, we use a reduced type vector for weak flip codes:

$$\mathbf{t}_{\text{weak}} \triangleq \left[t_{j_1}, t_{j_2}, \ldots, t_{j_{\mathsf{L}}}\right], \tag{38}$$

where

$$\sum_{w=1}^{\mathsf{L}} t_{j_w} = n \tag{39}$$

with j_w, $w = 1, \ldots, \mathsf{L}$, representing the numbers of the candidate columns that are weak flip columns.

For $\mathsf{M} = 2$ or $\mathsf{M} = 3$, all candidate columns are also weak flip columns (note that $2^{\mathsf{M}-1} - 1 = \binom{\mathsf{M}-1}{\bar{\ell}}$). For $\mathsf{M} = 4$, $\mathbf{t}_{\text{weak}} = [t_3, t_5, t_6]$. A similar definition can be given also for larger M, however, one needs to be aware that the number of weak flip candidate columns is increasing fast. For $\mathsf{M} = 5$ or $\mathsf{M} = 6$, we have ten weak flip candidate columns:

$$\mathcal{C}_{\text{weak}}^{(5)} = \left\{ \mathbf{c}_3^{(5)} \triangleq \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}, \mathbf{c}_5^{(5)} \triangleq \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}, \mathbf{c}_6^{(5)} \triangleq \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}, \mathbf{c}_7^{(5)} \triangleq \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix}, \mathbf{c}_9^{(5)} \triangleq \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \right.$$
$$\left. \mathbf{c}_{10}^{(5)} \triangleq \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \mathbf{c}_{11}^{(5)} \triangleq \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 1 \end{pmatrix}, \mathbf{c}_{12}^{(5)} \triangleq \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \mathbf{c}_{13}^{(5)} \triangleq \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 1 \end{pmatrix}, \mathbf{c}_{14}^{(5)} \triangleq \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 0 \end{pmatrix} \right\} \quad (40)$$

and

$$\mathcal{C}_{\text{weak}}^{(6)} = \left\{ \mathbf{c}_7^{(6)} \triangleq \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix}, \mathbf{c}_{11}^{(6)} \triangleq \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \end{pmatrix}, \mathbf{c}_{13}^{(6)} \triangleq \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \end{pmatrix}, \mathbf{c}_{14}^{(6)} \triangleq \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \end{pmatrix}, \mathbf{c}_{19}^{(6)} \triangleq \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}, \right.$$
$$\left. \mathbf{c}_{21}^{(6)} \triangleq \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}, \mathbf{c}_{22}^{(6)} \triangleq \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}, \mathbf{c}_{25}^{(6)} \triangleq \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \mathbf{c}_{26}^{(6)} \triangleq \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \mathbf{c}_{28}^{(6)} \triangleq \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} \right\}, \quad (41)$$

respectively.

We will next introduce a special subclass of weak flip codes that, as we will see in Section 5.2, possesses particularly beautiful properties.

Definition 20. A weak flip code is called *fair* if it is constructed by an equal number of all possible weak flip candidate columns in $\mathcal{C}_{\text{weak}}^{(\mathsf{M})}$. Note that by definition the blocklength of a fair weak flip code is always a multiple of L.

Fair weak flip codes have been used by Shannon *et al.* [9] for the derivation of error exponents, although the codes were not named at that time. Note that in their derivation, the error exponents are defined when blocklength n goes to infinity, but in this work we consider finite n.

Related to the weak flip codes and the fair weak flip codes are the families of *Hadamard codes* [4, Ch. 2].

Definition 21. For an even integer m, a (*normalized*) *Hadamard matrix* H_m of order m is an $m \times m$ matrix with entries $+1$ and -1 and with the first row and column being all $+1$, such that

$$\mathsf{H}_m \mathsf{H}_m^{\mathsf{T}} = m \mathsf{I}_m, \quad (42)$$

if such a matrix exists. Here I_m is the identity matrix of size m. If the entries $+1$ are replaced by 0 and the entries -1 by 1, H_m is changed into the *binary Hadamard matrix* A_m.

Note that a necessary (but not sufficient) condition for the existence of H_m (and the corresponding A_m) is that m is 1, 2, or a multiple of 4 [4, Ch. 2].

Definition 22. The binary Hadamard matrix A_m gives rise to three families of Hadamard codes:

1. The $\left(m, m-1, \frac{m}{2}\right)$ *Hadamard code* $\mathscr{H}_{1,m}$ consists of the rows of A_m with the first column deleted. (Here we follow the custom of traditional coding theory and specify the code with three parameters (M, n, d) where d denotes the minimum Hamming distance.) Moreover, the codewords in $\mathscr{H}_{1,m}$ that begin with 0 form the $\left(\frac{m}{2}, m-2, \frac{m}{2}\right)$ *Hadamard code* $\mathscr{H}'_{1,m}$ if the initial zero is deleted.

2. The $\left(2m, m-1, \frac{m}{2}-1\right)$ *Hadamard code* $\mathscr{H}_{2,m}$ consists of $\mathscr{H}_{1,m}$ together with the complements of all its codewords.

3. The $\left(2m, m, \frac{m}{2}\right)$ *Hadamard code* $\mathscr{H}_{3,m}$ consists of the rows of A_m and their complements.

Further Hadamard codes can be created by an arbitrary combination of the codebook matrices of different Hadamard codes.

Example 23. Consider the $(8, 7, 4)$ $\mathscr{H}_{1,8}$ code

$$\begin{pmatrix} 0&0&0&0&0&0&0\\ 0&0&1&0&1&1&1\\ 0&1&0&1&0&1&1\\ 0&1&1&1&1&0&0\\ 1&0&0&1&1&0&1\\ 1&0&1&1&0&1&0\\ 1&1&0&0&1&1&0\\ 1&1&1&0&0&0&1 \end{pmatrix}. \tag{43}$$

From this code, an $(8, 35, 20)$ Hadamard code can be constructed by simply concatenating $\mathscr{H}_{1,8}$ five times. ◊

Note that since the rows of A_m are orthogonal, any two rows of A_m agree in $\frac{1}{2}m$ places and differ in $\frac{1}{2}m$ places, i.e., they have a Hamming distance $\frac{m}{2}$. Moreover, by definition the first row of a binary Hadamard matrix is the all-zero row. Hence, we see that all Hadamard codes are weak flip codes, i.e., the family of weak flip codes is a superset of Hadamard codes.

On the other hand, fair weak flip codes can be seen as a "subset" of Hadamard codes because for all parameters (M, n) for which fair weak flip codes and also Hadamard codes exist, a Hadamard code can be constructed that is also a fair weak flip code. The problem with this statement lies in the fact that the Hadamard codes rely on the existence of Hadamard matrices, which in general is not guaranteed, i.e., it is difficult to predict whether for a given pair (M, n), a Hadamard code exists or not. This is in stark contrast to weak flip codes (which exist for all M and n) and fair weak flip codes (which exist for all M and all n being a multiple of L).

We also remark that a Hadamard code of parameters (M, n) for which fair weak flip codes exist is not necessarily equivalent to a fair weak flip code.

Example 24. We continue with Example 23 and note that the $(8, 35, 20)$ Hadamard code that is constructed by five repetitions of the matrix given in (43) is actually not a fair weak flip code since we have not used all possible weak flip candidate columns. However, it is possible to find five $(8, 7, 4)$ Hadamard codes that combine to a $(8, 35, 20)$ fair weak flip code. A $(8, 35, 20)$ fair weak flip code is composed by all $\binom{7}{4} = 35$ possible different weak flip columns. $\lozenge$

Note that two Hadamard matrices can be equivalent if one can be obtained from the other by permuting rows and columns and multiplying rows and columns by -1. In other words, Hadamard codes can actually be constructed from weak flip candidate columns. This also follows directly from the already mentioned fact that Hadamard codes are weak flip codes.

We quickly recall an important bound that holds for any $\big(\mathsf{M}, n, d\big)$ code.

Lemma 25 (Plotkin Bound [4]). *The minimum distance of an* (M, n) *binary code* $\mathscr{C}^{(\mathsf{M},n)}$ *always satisfies*

$$d_{\min}\big(\mathscr{C}^{(\mathsf{M},n)}\big) \leq \begin{cases} \frac{n\cdot\frac{\mathsf{M}}{2}}{\mathsf{M}-1} & \mathsf{M} \text{ even}, \\ \frac{n\cdot\frac{\mathsf{M}+1}{2}}{\mathsf{M}} & \mathsf{M} \text{ odd}. \end{cases} \tag{44}$$

Proof: We show a quick proof. We sum the Hamming distance over all possible pairs of two codewords apart from the codeword with itself:

$$\begin{aligned} &\mathsf{M}(\mathsf{M}-1)\cdot d_{\min}(\mathscr{C}^{(\mathsf{M},n)}) \\ &\quad\leq \sum_{\mathbf{u}\in\mathscr{C}^{(\mathsf{M},n)}} \sum_{\substack{\mathbf{v}\in\mathscr{C}^{(\mathsf{M},n)} \\ \mathbf{v}\neq\mathbf{u}}} d_{\mathrm{H}}(\mathbf{u},\mathbf{v}) && (45) \\ &\quad= \sum_{j=1}^{n} 2h_j\cdot(\mathsf{M}-h_j) && (46) \\ &\quad\leq \begin{cases} n\cdot\frac{\mathsf{M}^2}{2} & \text{if } \mathsf{M} \text{ even (achieved if } h_j=\frac{\mathsf{M}}{2}), \\ n\cdot\frac{\mathsf{M}^2-1}{2} & \text{if } \mathsf{M} \text{ odd (achieved if } h_j=\frac{\mathsf{M}\pm1}{2}), \end{cases} && (47) \end{aligned}$$

where in (46) we rearrange the order of summation: instead of summing over all codewords (rows), we approach the problem column-wise and assume that the jth column of $\mathscr{C}^{(\mathsf{M},n)}$ contains h_j zeros and $\mathsf{M}-h_j$ ones: then this column contributes $2h_j(\mathsf{M}-h_j)$ to the sum. $\square$

Note that from the proof of Lemma 25 we can see that a necessary condition for a codebook to meet the Plotkin-bound is that the codebook is composed by weak flip candidate columns. Furthermore, Levenshtein [4, Ch. 2] proved that the Plotkin bound can be achieved provided that Hadamard matrices exist.

4 Previous Results

4.1 SGB Bounds on the Average Error Probability

In [9], Shannon, Gallager, and Berlekamp derive upper and lower bounds on the average error probability of a given code used on a DMC. We next quickly review their results.

Definition 26. For $0 < s < 1$ we define

$$\mu_{\alpha,\beta}(s) \triangleq \log\left(\sum_y P_{Y|X}(y|\alpha)^{1-s} P_{Y|X}(y|\beta)^s\right). \tag{48}$$

Then the *discrepancy* $\mathsf{D}^{(\mathrm{DMC})}(m,m')$ between $\mathbf{x}_m$ and $\mathbf{x}_{m'}$ is defined as

$$\mathsf{D}^{(\mathrm{DMC})}(m,m') \triangleq -\min_{0\le s\le 1} \sum_\alpha \sum_\beta q_{\alpha,\beta}(m,m')\mu_{\alpha,\beta}(s) \tag{49}$$

with $q_{\alpha,\beta}(m,m')$ given in Definition 10.

Note that the discrepancy is a generalization of the Hamming distance. However, it depends strongly on the conditional channel law. We use a superscript "(DMC)" to indicate the channel to which the discrepancy refers.

Definition 27. The *minimum discrepancy* $\mathsf{D}_{\min}^{(\mathrm{DMC})}(\mathscr{C}^{(\mathsf{M},n)})$ for a codebook is the minimum value of $\mathsf{D}^{(\mathrm{DMC})}(m,m')$ over all pairs of codewords. The *maximum minimum discrepancy* is the maximum value of $\mathsf{D}_{\min}^{(\mathrm{DMC})}(\mathscr{C}^{(\mathsf{M},n)})$ over all possible codebooks $\mathscr{C}^{(\mathsf{M},n)}$: $\max_{\mathscr{C}^{(\mathsf{M},n)}} \mathsf{D}_{\min}^{(\mathrm{DMC})}(\mathscr{C}^{(\mathsf{M},n)})$.

Theorem 28 (SGB Bounds on Average Error Probability [9]). *For an arbitrary DMC, the average error probability $P_{\mathrm{e}}\big(\mathscr{C}^{(\mathsf{M},n)}\big)$ of a given code $\mathscr{C}^{(\mathsf{M},n)}$ with M codewords and blocklength n is upper- and lower-bounded as follows:*

$$\begin{aligned}\frac{1}{4\mathsf{M}} e^{-n\left(\mathsf{D}_{\min}^{(\mathrm{DMC})}(\mathscr{C}^{(\mathsf{M},n)})+\sqrt{\frac{2}{n}}\log\frac{1}{P_{\min}}\right)} \\ \le P_{\mathrm{e}}\big(\mathscr{C}^{(\mathsf{M},n)}\big) \le (\mathsf{M}-1)e^{-n\mathsf{D}_{\min}^{(\mathrm{DMC})}(\mathscr{C}^{(\mathsf{M},n)})}\end{aligned} \tag{50}$$

where $P_{\min}$ denotes the smallest nonzero transition probability of the channel.

Note that these bounds are specific to a given code design (via $\mathsf{D}_{\min}^{(\mathrm{DMC})}$). Therefore, the upper bound is a generally valid upper bound on the optimal performance, while the lower bound only holds in general if we apply it to the optimal code or to a suboptimal code that achieves the optimal $\mathsf{D}_{\min}^{(\mathrm{DMC})}$.

The bounds (50) are tight enough to derive the *error exponent* of the DMC (for a fixed number M of codewords).

Theorem 29 ([9]). *The error exponent of a DMC for a fixed number M of codewords*

$$\mathsf{E}_{\mathsf{M}} \triangleq \varlimsup_{n\to\infty} \max_{\mathscr{C}^{(\mathsf{M},n)}} \left\{-\frac{1}{n}\log P_{\mathrm{e}}\big(\mathscr{C}^{(\mathsf{M},n)}\big)\right\} \tag{51}$$

is given as

$$\mathsf{E}_{\mathsf{M}} = \lim_{n\to\infty} \max_{\mathscr{C}^{(\mathsf{M},n)}} \mathsf{D}_{\min}^{(\mathrm{DMC})}\big(\mathscr{C}^{(\mathsf{M},n)}\big). \tag{52}$$

Unfortunately, in general the evaluation of the error exponent is very difficult. For the class of so-called *pairwise reversible channels*, the calculation of the error exponent turns out to be uncomplicated.

Definition 30. A *pairwise reversible channel* is a DMC that has $\frac{\mathrm{d}}{\mathrm{d}s}\mu_{\alpha,\beta}(s)\big|_{s=\frac{1}{2}} = 0$ for any inputs α, β.

Clearly, the BEC is a pairwise reversible channel.

Note that it is easy to compute the pairwise discrepancy of a linear code on a pairwise reversible channel, so linear codes are quite suitable for computing (50).

Theorem 31 ([9]). *For pairwise reversible channels with* $\mathsf{M} > 2$*,*

$$\mathsf{E}_{\mathsf{M}} = \frac{1}{\mathsf{M}(\mathsf{M}-1)} \max_{\substack{\{\mathsf{M}_x\} \text{ s.t.} \\ \sum_x \mathsf{M}_x = \mathsf{M}}} \left\{ -\sum_{x\in\mathcal{X}} \sum_{x'\in\mathcal{X}} \mathsf{M}_x \mathsf{M}_{x'} \log \left(\sum_{y\in\mathcal{Y}} \sqrt{P_{Y|X}(y|x) P_{Y|X}(y|x')} \right) \right\} \tag{53}$$

where each M_x *denotes a nonnegative integer satisfying* $\sum_{x\in\mathcal{X}} \mathsf{M}_x = \mathsf{M}$*. Moreover,* E_{M} *is achieved by fair weak flip codes.*

We would like to emphasize that while Shannon *et al.* proved that fair weak flip codes achieve the error exponent, they did not investigate the error performance of fair weak flip codes for finite n. As we will see later, fair weak flip codes might be strictly suboptimal for finite n for the BSC (see also [6], [10]).

4.2 PPV Bounds for the BEC

In [11], Polyanskiy, Poor, and Verdú present upper and lower bounds on the optimal average error probability for finite blocklength for general DMC. For some special cases like BSC or BEC, these bounds can be expressed explicitly by closed-form formulas. The upper bound is based on *random coding*.

Theorem 32 (PPV Upper Bound [11, Th. 36]). *For the BEC with erasure probability* δ*, if the codebook* $\mathscr{C}^{(\mathsf{M},n)}$ *is created at random based on a uniform distribution, the expected average error probability (averaged over all codewords and all codebooks) satisfies*

$$\begin{aligned} &\mathsf{E}\left[P_{\mathrm{e}}\left(\mathscr{C}^{(\mathsf{M},n)}\right)\right] \\ &\quad = 1 - \sum_{j=0}^{n} \binom{n}{j} (1-\delta)^j \delta^{n-j} \sum_{m=0}^{\mathsf{M}-1} \frac{1}{m+1} \binom{\mathsf{M}-1}{m} (2^{-j})^m (1-2^{-j})^{\mathsf{M}-1-m}. \end{aligned} \tag{54}$$

Note that there must exist a codebook whose average error probability achieves (54), so Theorem 32 provides a general achievable upper bound on the error probability, although we do not know the concrete code structure.

Polyanskiy, Poor, and Verdú also provide a new general converse for the average error probability, based on which a close-form formula can be derived for the BEC.

Theorem 33 (PPV Lower Bound [11, Th. 38]). *For the BEC with erasure probability* δ*, any codebook* $\mathscr{C}^{(\mathsf{M},n)}$ *satisfies*

$$P_{\mathrm{e}}\left(\mathscr{C}^{(\mathsf{M},n)}\right) \geq \sum_{e=\lfloor n-\log_2 \mathsf{M} \rfloor+1}^{n} \binom{n}{e} \delta^e (1-\delta)^{n-e} \left(1 - \frac{2^{n-e}}{\mathsf{M}}\right). \tag{55}$$

Note that (55) was first derived based on an "*ad hoc*" (i.e., BEC specific) argument in [11]. It is then shown in [12] that the same result can also be obtained using the so-called *meta-converse* methodology.

5 Column-Wise Analysis of Codes

5.1 r-wise Hamming Distance

The minimum Hamming distance is a well-known and widely used quality criterion of a code. Unfortunately, a design based on the minimum Hamming distance can be strictly suboptimal even for a very symmetric channel like the BSC and even for linear codes [6], [10].[9] We therefore define a slightly more general and more concise description of a code: the *pairwise Hamming distance vector*.

Definition 34. Given a code $\mathscr{C}^{(\mathsf{M},n)}$ with codewords $\mathbf{x}_m$, $m \in \mathcal{M}$, we define the *pairwise Hamming distance vector* $\mathbf{d}^{(\mathsf{M},n)}$ of length $\frac{1}{2}(\mathsf{M}-1)\mathsf{M}$ as

$$\begin{aligned}\mathbf{d}^{(\mathsf{M},n)} \triangleq \big(&d_{12}^{(n)},\ d_{13}^{(n)}, d_{23}^{(n)},\ d_{14}^{(n)}, d_{24}^{(n)}, d_{34}^{(n)}, \ldots,\\ &d_{1\mathsf{M}}^{(n)}, d_{2\mathsf{M}}^{(n)}, \ldots, d_{(\mathsf{M}-1)\mathsf{M}}^{(n)}\big)\end{aligned} \tag{56}$$

with $d_{mm'}^{(n)} \triangleq d_{\mathrm{H}}(\mathbf{x}_m, \mathbf{x}_{m'})$, $1 \le m < m' \le \mathsf{M}$. The *minimum Hamming distance* $d_{\min}$ is the minimum component of the pairwise Hamming distance vector $\mathbf{d}^{(\mathsf{M},n)}$.

Lemma 35. *The pairwise Hamming distance vector of a general code of type* $\mathbf{t}$ *for* $\mathsf{M}=3$ *or* $\mathsf{M}=4$ *is given as follows:*

$$\begin{aligned}\mathbf{d}^{(3,n)} &= \big(d_{12}^{(n)}, d_{13}^{(n)}, d_{23}^{(n)}\big) && (57)\\ &= (t_2+t_3, t_1+t_3, t_1+t_2) && (58)\\ &= (n-t_1, n-t_2, n-t_3); && (59)\\ \mathbf{d}^{(4,n)} &= \big(d_{12}^{(n)}, d_{13}^{(n)}, d_{14}^{(n)}, d_{23}^{(n)}, d_{24}^{(n)}, d_{34}^{(n)}\big) && (60)\\ &= (t_4+t_5+t_6+t_7, t_2+t_3+t_6+t_7, t_2+t_3+t_4+t_5,\\ &\quad t_1+t_3+t_5+t_7, t_1+t_3+t_4+t_6, t_1+t_2+t_5+t_6) && (61)\\ &= \big(n-(t_1+t_2+t_3), n-(t_1+t_4+t_5), n-(t_1+t_6+t_7),\\ &\quad n-(t_2+t_4+t_6), n-(t_2+t_5+t_7), n-(t_3+t_4+t_7)\big). && (62)\end{aligned}$$

We remind the reader of our convention to number the codewords according to rows in the codebook matrix, see (25).

The following generalization of the pairwise Hamming distance turns out to be convenient for the performance analysis of the BEC.

Definition 36 (r-wise Hamming Distance)**.** For a given general codebook $\mathscr{C}_{\mathbf{t}}^{(\mathsf{M},n)}$ and an arbitrary integer $2 \le r \le \mathsf{M}$, choose some $1 \le i_1 < i_2 < \cdots < i_r \le \mathsf{M}$. Then the r-wise Hamming distance $d_{i_1\, i_2 \cdots\, i_r}\big(\mathscr{C}_{\mathbf{t}}^{(\mathsf{M},n)}\big)$ is defined as

$$d_{i_1\, i_2 \cdots\, i_r}\Big(\mathscr{C}_{\mathbf{t}}^{(\mathsf{M},n)}\Big) \triangleq n - \sum_{\substack{j\in\mathcal{J} \text{ s.t.}\\ c_{j,i_1}=c_{j,i_2}=\cdots=c_{j,i_r}}} t_j. \tag{63}$$

Here t_j denotes the jth component of the code parameter vector $\mathbf{t}$ of length $\mathsf{J} = 2^{\mathsf{M}-1}-1$, and c_{j,i_ℓ} is the i_ℓth component of the jth candidate column $\mathbf{c}_j^{(\mathsf{M})}$ as given in Definition 14, and $\mathcal{J} \triangleq \{1, \ldots, 2^{\mathsf{M}-1}-1\} = \{1, \ldots, \mathsf{J}\}$.

It can be verified from Definition 36 that the 2-wise Hamming distances are identical to the pairwise Hamming distances. When the considered $\mathbf{t}$-type code

[9] This is in spite of the fact that the error probability performance of a BSC is completely specified by the Hamming distances between codewords and received vectors!

is unambiguous from the context, we will omit the specification of the code and abbreviate the r-wise Hamming distance (63) as $d^{(\mathsf{M},n)}_{i_1\, i_2 \cdots i_r}$ or, even shorter, $d^{(\mathsf{M},n)}_{\mathcal{I}}$ (for some given $\mathcal{I} = \{i_1, i_2, \ldots, i_r\}$).

Example 37. There are $\binom{\mathsf{M}}{r}$ r-wise Hamming distances. For example, for $\mathsf{M} = 4$ and $r = 3$, the $\binom{\mathsf{M}}{r} = \binom{4}{3} = 4$ 3-wise Hamming distances can be derived as follows:

$$d^{(4,n)}_{123} = n - t_1, \quad d^{(4,n)}_{124} = n - t_2, \quad d^{(4,n)}_{134} = n - t_4, \quad d^{(4,n)}_{234} = n - t_7, \tag{64}$$

and there is only one 4-wise Hamming distance $d^{(4,n)}_{1234} = n$. ◊

Next we give some properties concerning the relation between the r-wise Hamming distance and general code parameters.

Theorem 38. *For any integer $2 \le r \le \mathsf{M}$ and any choice $1 \le i_1 < i_2 < \cdots < i_r \le \mathsf{M}$, the cardinality of the index set*

$$\left\{ j \in \mathcal{J} \colon c_{j,i_1} = c_{j,i_2} = \cdots = c_{j,i_r} \right\} \tag{65}$$

is equal to $2^{\mathsf{M}-r} - 1$, where c_{j,i_ℓ} denotes the i_ℓth component of the jth candidate column $\mathbf{c}^{(\mathsf{M})}_j$.

Proof: First, consider the case when $i_1 = 1$. Since the first position of each candidate column is always equal to zero, we only need to consider those $j \in \mathcal{J}$ such that $c_{j,i_1} = c_{j,i_2} = \cdots = c_{j,i_r} = 0$. There are in total $2^{\mathsf{M}-r}$ such columns, but we need to subtract 1 because we exclude the all-zero column.

Second, consider the case when $i_1 > 1$. Since the first position is fixed to zero, we ignore it. There are $2^{\mathsf{M}-1-r}$ columns with $c_{j,i_1} = c_{j,i_2} = \cdots = c_{j,i_r} = 0$ and the same amount with $c_{j,i_1} = c_{j,i_2} = \cdots = c_{j,i_r} = 1$. Once again excluding the all-zero column, we have in total $2 \cdot 2^{\mathsf{M}-1-r} - 1$ possible columns. □

Corollary 39. *The Hamming weight of the second codeword of a $\mathbf{t}$-type code $\mathscr{C}^{(\mathsf{M},n)}_{\mathbf{t}}$ is given by*

$$w_{\mathrm{H}}(\mathbf{x}_2) = d_{\mathrm{H}}(\mathbf{x}_1, \mathbf{x}_2) = \sum_{j=2^{\mathsf{M}-2}}^{\mathsf{J}} t_j, \tag{66}$$

where the second codeword corresponds to the second row in the code matrix of $\mathscr{C}^{(\mathsf{M},n)}_{\mathbf{t}}$. If every candidate column in $\mathcal{C}^{(\mathsf{M})}$ is used exactly once in $\mathscr{C}^{(\mathsf{M},n)}_{\mathbf{t}}$, i.e., $t_j = 1$ for $1 \le j \le \mathsf{J}$, then all codewords have the same Hamming weight and for $1 \le i_1 < i_2 \le \mathsf{M}$,

$$d^{(\mathsf{M},n)}_{i_1\, i_2} = 2^{\mathsf{M}-2} = w_{\mathrm{H}}(\mathbf{x}_2) = w_{\mathrm{H}}(\mathbf{x}_3) = \cdots = w_{\mathrm{H}}(\mathbf{x}_{\mathsf{M}}). \tag{67}$$

Proof: By Definition 36 and Theorem 38, we have

$$d^{(\mathsf{M},n)}_{12} = n - \sum_{\substack{j \in \mathcal{J} \text{ s.t.} \\ c_{j,1} = c_{j,2} = 0}} t_j = n - \sum_{j=1}^{2^{\mathsf{M}-2}-1} t_j = \sum_{j=2^{\mathsf{M}-2}}^{\mathsf{J}} t_j. \tag{68}$$

If $t_1 = t_2 = \cdots = t_{\mathsf{J}} = 1$ (see (28)), we obtain again by Theorem 38 for $1 \le i_1 < i_2 \le \mathsf{M}$, $d^{(\mathsf{M},n)}_{i_1\, i_2} = (2^{\mathsf{M}-1} - 1) - (2^{\mathsf{M}-2} - 1) = 2^{\mathsf{M}-2}$, which implies $w_{\mathrm{H}}(\mathbf{x}_{i_2}) = d^{(\mathsf{M},n)}_{1\, i_2} = 2^{\mathsf{M}-2}$ for $2 \le i_2 \le \mathsf{M}$. □

5.2 Characteristics of Weak Flip Codes

In this section, we concentrate on the analysis of the family of weak flip codes.

Note that in traditional coding theory most results are restricted to linear codes, which possess very powerful algebraic properties. For more details and the proofs of the following properties see, e.g., [2], [4].

One of the most important property of a linear code is as follows.

Proposition 40. *Let $\mathscr{C}_{\text{lin}}$ be linear and let $\mathbf{x}_m \in \mathscr{C}_{\text{lin}}$ be given. Then the code obtained by adding $\mathbf{x}_m$ to each codeword of $\mathscr{C}_{\text{lin}}$ is equal to $\mathscr{C}_{\text{lin}}$.*

Another property concerns the column weights.

Proposition 41. *If an (M, n) binary code is linear, then each column of its codebook matrix has Hamming weight $\frac{\mathsf{M}}{2}$, i.e., the code is a weak flip code.*

Hence, linear codes are weak flip codes. Note, however, that linear codes only exist if $\mathsf{M} = 2^r$, where $r \in \mathbb{N} \triangleq \{1, 2, \ldots\}$, while weak flip codes are defined for any M. Also note that the converse of Proposition 41 does not hold, i.e., even if $\mathsf{M} = 2^r$ for some $r \in \mathbb{N}$, a weak flip code $\mathscr{C}^{(\mathsf{M},n)}$ is not necessarily linear. It is not even the case that a fair weak flip code for $\mathsf{M} = 2^r$ is necessarily linear.

Now the question arises as to which of the many powerful algebraic properties of linear codes are retained in weak flip codes.

Theorem 42. *Consider a weak flip code $\mathscr{C}_{\text{weak}}^{(\mathsf{M},n)}$ and fix some codeword $\mathbf{x}_m \in \mathscr{C}_{\text{weak}}^{(\mathsf{M},n)}$. If we add this codeword to all codewords in $\mathscr{C}_{\text{weak}}^{(\mathsf{M},n)}$, then the resulting code $\tilde{\mathscr{C}}^{(\mathsf{M},n)} \triangleq \left\{\mathbf{x}_m \oplus \mathbf{x} \,\middle|\, \forall\, \mathbf{x} \in \mathscr{C}_{\text{weak}}^{(\mathsf{M},n)}\right\}$ is still a weak flip code; however, it is not necessarily the same one.*

Proof: Let $\mathscr{C}_{\text{weak}}^{(\mathsf{M},n)}$ be a weak flip code according to Definition 19. We have to prove that

$$\begin{pmatrix} \mathbf{x}_1 \\ \mathbf{x}_2 \\ \vdots \\ \mathbf{x}_{\mathsf{M}} \end{pmatrix} \oplus \begin{pmatrix} \mathbf{x}_m \\ \mathbf{x}_m \\ \vdots \\ \mathbf{x}_m \end{pmatrix} = \begin{pmatrix} \mathbf{x}_1 \oplus \mathbf{x}_m \\ \vdots \\ \mathbf{x}_m \oplus \mathbf{x}_m = \mathbf{0} \\ \vdots \\ \mathbf{x}_{\mathsf{M}} \oplus \mathbf{x}_m \end{pmatrix} \triangleq \tilde{\mathscr{C}}^{(\mathsf{M},n)} \tag{69}$$

is a weak flip code. Let $\mathbf{c}_i$, $1 \le i \le n$, denote the ith column vector of the code matrix of $\mathscr{C}_{\text{weak}}^{(\mathsf{M},n)}$. Then $\tilde{\mathscr{C}}^{(\mathsf{M},n)}$ has the column vectors

$$\tilde{\mathbf{c}}_i = \begin{cases} \mathbf{c}_i & \text{if } x_{m,i} = 0, \\ \bar{\mathbf{c}}_i & \text{if } x_{m,i} = 1. \end{cases} \tag{70}$$

Since $\mathbf{c}_i$ is a weak flip column, either $w_{\text{H}}(\mathbf{c}_i) = \lfloor \frac{\mathsf{M}}{2} \rfloor$ or $w_{\text{H}}(\mathbf{c}_i) = \lceil \frac{\mathsf{M}}{2} \rceil$, implying either $w_{\text{H}}(\bar{\mathbf{c}}_i) = \lceil \frac{\mathsf{M}}{2} \rceil$ or $w_{\text{H}}(\bar{\mathbf{c}}_i) = \lfloor \frac{\mathsf{M}}{2} \rfloor$. What remains is to interchange the first codeword of $\tilde{\mathscr{C}}^{(\mathsf{M},n)}$ and the all-zero codeword in the mth row in $\tilde{\mathscr{C}}^{(\mathsf{M},n)}$ (which is always possible, see Remark 12). As a result, $\tilde{\mathscr{C}}^{(\mathsf{M},n)}$ is also a weak flip code. □

Theorem 42 is a beautiful property of weak flip codes; however, it still represents a considerable weakening of the powerful property of linear codes given in Proposition 40. This can be fixed by considering the subfamily of fair weak flip codes.

Theorem 43 (Quasi-Linear Codes). *Let $\mathscr{C}_{\text{fair}}^{(\mathsf{M},n)}$ be a fair weak flip code and let $\mathbf{x}_m \in \mathscr{C}_{\text{fair}}^{(\mathsf{M},n)}$ be given. Then the code $\tilde{\mathscr{C}}^{(\mathsf{M},n)} = \left\{\mathbf{x}_m \oplus \mathbf{x} \,\middle|\, \forall\, \mathbf{x} \in \mathscr{C}_{\text{fair}}^{(\mathsf{M},n)}\right\}$ is equivalent to $\mathscr{C}_{\text{fair}}^{(\mathsf{M},n)}$.*

Proof: Divide the weak flip candidate columns in $\mathcal{C}_{\text{weak}}^{(\mathsf{M})}$ into two subfamilies: one subfamily consists of the columns with the mth component being zero, and the columns in the other subfamily have their mth component equal to one. Next add the mth codeword to the codewords in $\mathscr{C}_{\text{fair}}^{(\mathsf{M},n)}$ and then interchange the first and mth components of each column in the code matrix of $\mathscr{C}_{\text{fair}}^{(\mathsf{M},n)}$ to form a new code $\tilde{\mathscr{C}}^{(\mathsf{M},n)}$.

It is apparent that the columns in the first subfamily are unchanged by such code-addition manipulation. However, when M is odd, the weights of columns in the second subfamily change either from $\underline{\ell}$ to $\bar{\ell}$, or from $\bar{\ell}$ to $\underline{\ell}$, while these weights stay the same when M is even. As a result, after such code-addition manipulation, the columns belonging to the second subfamily remain distinct weak flip columns and are still contained in the second subfamily (since their mth components are still equal to one). Thus, all the weak flip columns remain to be used equally in $\tilde{\mathscr{C}}^{(\mathsf{M},n)}$, and the proof is completed. □

If we recall Proposition 41 and the discussion after it, we realize that the definition of the quasi-linear fair weak flip code is a considerable enlargement of the set of codes having the property given in Theorem 43.

The following corollary is a direct consequence of Corollary 39.

Corollary 44. *The Hamming weights of each codeword of a fair weak flip code are all identical except the all-zero codeword $\mathbf{x}_1$, and are given by*

$$w_{\mathrm{H}}(\mathbf{x}_2) = w_{\mathrm{H}}(\mathbf{x}_3) = \cdots = w_{\mathrm{H}}(\mathbf{x}_{\mathsf{M}}) = \frac{n \cdot \bar{\ell}}{2\bar{\ell} - 1}. \tag{71}$$

Proof: For a fair weak flip code, the Hamming weight of its mth codeword is a fixed integer multiple (i.e., n/L) of the number of weak flip columns with mth component equal to 1. When M is odd, such number of weak flip columns with weight $\underline{\ell}$ equals $\binom{\mathsf{M}-2}{\underline{\ell}-1}$, and that of weak flip columns with weight $\bar{\ell}$ is $\binom{\mathsf{M}-2}{\bar{\ell}-1}$. In total, we have

$$w_{\mathrm{H}}(\mathbf{x}_m) = \frac{n}{\mathsf{L}}\left[\binom{\mathsf{M}-2}{\underline{\ell}-1} + \binom{\mathsf{M}-2}{\bar{\ell}-1}\right] = \frac{n}{\mathsf{L}}\binom{2\bar{\ell}-2}{\bar{\ell}-1}, \tag{72}$$

where we take $\mathsf{M} = 2\bar{\ell} - 1$ in the last equality. Similarly, given $\mathsf{M} = 2\bar{\ell}$ is even, we derive using the same argument that

$$w_{\mathrm{H}}(\mathbf{x}_m) = \frac{n}{\mathsf{L}}\binom{\mathsf{M}-2}{\bar{\ell}-1} = \frac{n}{\mathsf{L}}\binom{2\bar{\ell}-2}{\bar{\ell}-1}. \tag{73}$$

The proof is completed by replacing L with $\binom{2\bar{\ell}-1}{\bar{\ell}}$. □

We next investigate the minimum Hamming distance of the quasi-linear fair weak flip codes.

Theorem 45. *Fix some M and a blocklength n with $n \bmod \mathsf{L} = 0$. Then a fair weak flip code $\mathscr{C}_{\text{fair}}^{(\mathsf{M},n)}$ achieves the largest minimum Hamming distance among all codes of given blocklength and satisfies*

$$d_{\min}\left(\mathscr{C}_{\text{fair}}^{(\mathsf{M},n)}\right) = \frac{n \cdot \bar{\ell}}{2\bar{\ell} - 1}. \tag{74}$$

Proof: For $\mathsf{M} = 2\bar{\ell}$, we know that by definition the Hamming weight of each column of the codebook matrix is equal to $\bar{\ell}$. Hence, when changing the sum from column-wise to row-wise, where we can ignore the first row of zero weight (corresponding to the all-zero codeword $\mathbf{x}_1$), we get

$$n \cdot \bar{\ell} = \sum_{i=1}^{n} w_{\mathrm{H}}(\mathbf{c}_i) = \sum_{m=2}^{2\bar{\ell}} w_{\mathrm{H}}(\mathbf{x}_m) \tag{75}$$

$$= \sum_{m=2}^{2\bar{\ell}} d_{\min}\big(\mathscr{C}_{\mathrm{fair}}^{(\mathsf{M},n)}\big) \tag{76}$$

$$= (2\bar{\ell} - 1) \cdot d_{\min}\big(\mathscr{C}_{\mathrm{fair}}^{(\mathsf{M},n)}\big), \tag{77}$$

where (76) follows from Theorem 43 and Corollary 44. The proof is completed by confirming that $d_{\min}\big(\mathscr{C}_{\mathrm{fair}}^{(\mathsf{M},n)}\big) = \frac{n\cdot\bar{\ell}}{2\bar{\ell}-1}$ meets the Plotkin bound in Lemma 25 and hence achieves the largest minimum Hamming distance among all codes of given blocklength.

In the case of $\mathsf{M} = 2\bar{\ell} - 1$, Remark 18 indicates that all codewords in $\mathscr{C}_{\mathrm{fair}}^{(2\bar{\ell}-1,n)}$ are contained in $\mathscr{C}_{\mathrm{fair}}^{(2\bar{\ell},n)}$; hence, $d_{\min}\big(\mathscr{C}_{\mathrm{fair}}^{(2\bar{\ell}-1,n)}\big) \geq d_{\min}\big(\mathscr{C}_{\mathrm{fair}}^{(2\bar{\ell},n)}\big) = \frac{n\cdot\bar{\ell}}{2\bar{\ell}-1}$, which again achieves (and hence equates) the Plotkin bound in Lemma 25. □

Corollary 46. *The pairwise Hamming distance vector of a weak flip code of type* $\mathbf{t}_{\mathrm{weak}}$ *for* $\mathsf{M} = 4$ *can be simplified from* (62) *as follows:*

$$\mathbf{d}^{(4,n)} = (t_5 + t_6, t_3 + t_6, t_3 + t_5, t_3 + t_5, t_3 + t_6, t_5 + t_6) \tag{78}$$

$$= (n - t_3, n - t_5, n - t_6, n - t_6, n - t_5, n - t_3). \tag{79}$$

Note that for weak flip code of type $\mathbf{t}_{\mathrm{weak}}$, $\mathbf{d}^{(3,n)}$ *remains the same as shown in* (59).

6 Analysis of the BEC

In Section 3.3 we have shown that any codebook can be described by the code parameter vector $\mathbf{t}$. Therefore the minimization of the average error probability among all possible codebooks turns into an optimization problem on the discrete variables $\mathbf{t}$, subject to the condition that $\sum_{j=1}^{\mathsf{J}} t_j = n$. Consequently, the r-wise Hamming distance and the code parameter properties play an important role in our analysis.

6.1 Exact Average Error Probability of a Code with an Arbitrary Number of Codewords M

We firstly derive a useful result that gives the exact average error probability as a function of the code parameter vector $\mathbf{t}$.

Lemma 47 (Inclusion–Exclusion Principle in Probability Theory [13]). *Let* $\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_{\mathsf{M}}$ *be* M *(not necessarily independent) events in a probability space. The inclusion–exclusion principle states that*

$$\Pr\left(\bigcup_{m=1}^{\mathsf{M}} \mathcal{A}_m\right) = \sum_{r=1}^{\mathsf{M}} (-1)^{r-1} \sum_{\substack{\mathcal{I}\subseteq\{1,2,\ldots,\mathsf{M}\} \\ |\mathcal{I}|=r}} \Pr\left(\bigcap_{i\in\mathcal{I}} \mathcal{A}_i\right). \tag{80}$$

We will next apply the idea of the inclusion–exclusion principle to the closed decoding regions defined in Definition 6. To simplify our notation, we define the following shorthands:

$$\Pr\Big(\overline{\mathcal{D}}_m^{(\mathsf{M},n)}\Big|\mathbf{x}_m\Big) \triangleq \sum_{\mathbf{y}\in\overline{\mathcal{D}}_m^{(\mathsf{M},n)}} P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y}|\mathbf{x}_m), \tag{81}$$

$$\Pr\left(\bigcap_{i\in\mathcal{I}}\overline{\mathcal{D}}_i^{(\mathsf{M},n)}\middle|\mathbf{x}_\ell\right) \triangleq \sum_{\mathbf{y}\in\bigcap_{i\in\mathcal{I}}\overline{\mathcal{D}}_i^{(\mathsf{M},n)}} P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y}|\mathbf{x}_\ell), \quad \forall \ell\in\mathcal{I}, \quad \mathcal{I}\subseteq\mathcal{M}, \tag{82}$$

where the exact choice of ℓ is irrelevant because according to Definition 6, for given $\mathcal{I}=\{i_1,i_2,\ldots,i_r\}$, we have

$$\max_{1\le m'\le\mathsf{M}} P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y}|\mathbf{x}_{m'}) = P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y}|\mathbf{x}_{i_1}) = P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y}|\mathbf{x}_{i_2}) = \cdots = P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y}|\mathbf{x}_{i_r}), \quad \forall\,\mathbf{y}\in\bigcap_{i\in\mathcal{I}}\overline{\mathcal{D}}_i^{(\mathsf{M},n)}. \tag{83}$$

Theorem 48. *Consider an (M,n) coding scheme with ML decoding, its corresponding decoding regions $\mathcal{D}_m$, and the closed decoding regions $\overline{\mathcal{D}}_m$ as defined in Definition 6, where we drop the superscript "(M,n)" for notational convenience. Then*

$$\Pr(\mathcal{D}_m|\mathbf{x}_m) = \Pr\big(\overline{\mathcal{D}}_m\big|\mathbf{x}_m\big) - \sum_{r=1}^{m-1}(-1)^{r-1}\sum_{\substack{\mathcal{I}\subseteq\{1,\ldots,m-1\}\\|\mathcal{I}|=r}}\Pr\left(\bigcap_{i\in\mathcal{I}}\big(\overline{\mathcal{D}}_i\cap\overline{\mathcal{D}}_m\big)\middle|\mathbf{x}_m\right) \tag{84}$$

and the exact average success probability can be expressed as

$$P_{\mathrm{c}}\big(\mathscr{C}^{(\mathsf{M},n)}\big) = \frac{1}{\mathsf{M}}\sum_{r=1}^{\mathsf{M}}(-1)^{r-1}\sum_{\substack{\mathcal{I}\subseteq\{1,\ldots,\mathsf{M}\}\\|\mathcal{I}|=r}}\Pr\left(\bigcap_{i\in\mathcal{I}}\overline{\mathcal{D}}_i\middle|\mathbf{x}_{\ell,\ell\in\mathcal{I}}\right). \tag{85}$$

Proof: By Definition 6, a possible choice of ML decoding regions are given as follows:

$$\begin{aligned}
\mathcal{D}_1 &\triangleq \overline{\mathcal{D}}_1, && (86)\\
\mathcal{D}_2 &\triangleq \overline{\mathcal{D}}_2\setminus\overline{\mathcal{D}}_1 && (87)\\
&= \overline{\mathcal{D}}_2\setminus\big(\overline{\mathcal{D}}_2\cap\overline{\mathcal{D}}_1\big), && (88)\\
\mathcal{D}_3 &\triangleq \overline{\mathcal{D}}_3\setminus\big(\overline{\mathcal{D}}_1\cup\overline{\mathcal{D}}_2\big) && (89)\\
&= \overline{\mathcal{D}}_3\setminus\big(\overline{\mathcal{D}}_3\cap\big(\overline{\mathcal{D}}_1\cup\overline{\mathcal{D}}_2\big)\big), && (90)\\
&\ \ \vdots
\end{aligned}$$

i.e.,

$$\begin{aligned}
\mathcal{D}_m &= \overline{\mathcal{D}}_m\setminus\left(\overline{\mathcal{D}}_m\cap\left(\bigcup_{i\in\{1,\ldots,m-1\}}\overline{\mathcal{D}}_i\right)\right) && (91)\\
&= \overline{\mathcal{D}}_m\setminus\left(\bigcup_{i\in\{1,\ldots,m-1\}}\big(\overline{\mathcal{D}}_m\cap\overline{\mathcal{D}}_i\big)\right). && (92)
\end{aligned}$$

Hence, by Lemma 47,

$$\Pr(\mathcal{D}_m|\mathbf{x}_m) = \Pr\left(\overline{\mathcal{D}}_m \setminus \left(\bigcup_{i\in\{1,\dots,m-1\}} (\overline{\mathcal{D}}_m \cap \overline{\mathcal{D}}_i)\right)\middle|\mathbf{x}_m\right) \tag{93}$$

$$= \Pr\big(\overline{\mathcal{D}}_m\big|\mathbf{x}_m\big) - \Pr\left(\bigcup_{i\in\{1,\dots,m-1\}} (\overline{\mathcal{D}}_m \cap \overline{\mathcal{D}}_i)\middle|\mathbf{x}_m\right) \tag{94}$$

$$= \Pr\big(\overline{\mathcal{D}}_m\big|\mathbf{x}_m\big) - \sum_{r=1}^{m-1}(-1)^{r-1} \sum_{\substack{\mathcal{I}\subseteq\{1,\dots,m-1\}\\|\mathcal{I}|=r}} \Pr\left(\bigcap_{i\in\mathcal{I}}(\overline{\mathcal{D}}_m \cap \overline{\mathcal{D}}_i)\middle|\mathbf{x}_m\right), \tag{95}$$

which proves (84).

The average success probability can now be expressed as follows:

$$\mathsf{M}\cdot P_{\mathrm{c}}\big(\mathscr{C}^{(\mathsf{M},n)}\big)$$

$$= \sum_{m=1}^{\mathsf{M}} \Pr(\mathcal{D}_m|\mathbf{x}_m) \tag{96}$$

$$= \sum_{m=1}^{\mathsf{M}} \left(\Pr\big(\overline{\mathcal{D}}_m\big|\mathbf{x}_m\big) - \sum_{r=1}^{m-1}(-1)^{r-1} \sum_{\substack{\mathcal{I}\subseteq\{1,\dots,m-1\}\\|\mathcal{I}|=r}} \Pr\left(\bigcap_{i\in\mathcal{I}}(\overline{\mathcal{D}}_m \cap \overline{\mathcal{D}}_i)\middle|\mathbf{x}_m\right)\right) \tag{97}$$

$$= \sum_{m=1}^{\mathsf{M}} \left(\Pr\big(\overline{\mathcal{D}}_m\big|\mathbf{x}_m\big) + \sum_{r=1}^{m-1}(-1)^{r} \sum_{\substack{\mathcal{I}\subseteq\{1,\dots,m-1\}\\|\mathcal{I}|=r}} \Pr\left(\bigcap_{i\in\mathcal{I}}(\overline{\mathcal{D}}_m \cap \overline{\mathcal{D}}_i)\middle|\mathbf{x}_{\ell,\ell\in\mathcal{I}\cup\{m\}}\right)\right) \tag{98}$$

$$= \sum_{m=1}^{\mathsf{M}} \left(\sum_{r=0}^{m-1}(-1)^{r} \sum_{\substack{\mathcal{I}\subseteq\{1,\dots,m-1\}\\|\mathcal{I}|=r}} \Pr\left(\bigcap_{i\in\mathcal{I}}(\overline{\mathcal{D}}_m \cap \overline{\mathcal{D}}_i)\middle|\mathbf{x}_{\ell,\ell\in\mathcal{I}\cup\{m\}}\right)\right) \tag{99}$$

$$= \sum_{r=0}^{\mathsf{M}-1}(-1)^{r} \sum_{m=r+1}^{\mathsf{M}} \left(\sum_{\substack{\mathcal{I}\subseteq\{1,\dots,m-1\}\\|\mathcal{I}|=r}} \Pr\left(\bigcap_{i\in\mathcal{I}}(\overline{\mathcal{D}}_m \cap \overline{\mathcal{D}}_i)\middle|\mathbf{x}_{\ell,\ell\in\mathcal{I}\cup\{m\}}\right)\right) \tag{100}$$

$$= \sum_{r=0}^{\mathsf{M}-1}(-1)^{r} \sum_{\substack{\mathcal{I}\subseteq\{1,\dots,\mathsf{M}\}\\|\mathcal{I}|=r+1}} \Pr\left(\bigcap_{i\in\mathcal{I}}\overline{\mathcal{D}}_i\middle|\mathbf{x}_{\ell,\ell\in\mathcal{I}}\right) \tag{101}$$

$$= \sum_{r=1}^{\mathsf{M}}(-1)^{r-1} \sum_{\substack{\mathcal{I}\subseteq\{1,\dots,\mathsf{M}\}\\|\mathcal{I}|=r}} \Pr\left(\bigcap_{i\in\mathcal{I}}\overline{\mathcal{D}}_i\middle|\mathbf{x}_{\ell,\ell\in\mathcal{I}}\right). \tag{102}$$

Here, (97) follows from (95); in (98) we allow different choices of the conditioning argument, which does not change the expression because of (83); in (99) we included the empty set into the sum to take care of the first term; and in (100) and (101) we exchange the two outer sums and then combine the resulting two inner sums. This completes the proof. □

By the r-wise Hamming distance and Theorem 48, we are now able to give a closed-form expression for the exact average error probability of an arbitrary code $\mathscr{C}_{\mathbf{t}}^{(\mathsf{M},n)}$ used on a BEC.

Theorem 49 (Average Error Probability on the BEC). *Consider a BEC with arbitrary erasure probability $0 \leq \delta < 1$ and an arbitrary code $\mathscr{C}_{\mathbf{t}}^{(\mathsf{M},n)}$. The average ML error probability can be expressed using the code parameters $\mathbf{t}$ as follows:*

$$P_{\mathrm{e}}\Big(\mathscr{C}_{\mathbf{t}}^{(\mathsf{M},n)}\Big) = \frac{1}{\mathsf{M}} \sum_{r=2}^{\mathsf{M}} (-1)^r \sum_{\substack{\mathcal{I} \subseteq \{1,\ldots,\mathsf{M}\} \\ |\mathcal{I}|=r}} \delta^{d_{\mathcal{I}}^{(\mathsf{M},n)}}, \tag{103}$$

where $d_{\mathcal{I}}^{(\mathsf{M},n)}$ denotes the r-wise Hamming distance as given in Definition 36.

Proof: Comparing (85) and (103), we see that the theorem can be proved by showing

$$\Pr\big(\overline{\mathcal{D}}_m \big| \mathbf{x}_m\big) = 1, \quad \forall\, m \in \mathcal{M}, \tag{104}$$

$$\Pr\left(\bigcap_{i\in\mathcal{I}} \overline{\mathcal{D}}_i \middle| \mathbf{x}_\ell\right) = \delta^{d_{\mathcal{I}}^{(\mathsf{M},n)}}, \quad \forall \ell \in \mathcal{I}, \quad \forall\, \mathcal{I} \subseteq \mathcal{M} \text{ with } |\mathcal{I}| \geq 2. \tag{105}$$

By its definition,

$$\overline{\mathcal{D}}_m = \big\{\mathbf{y} \colon d_{\mathrm{H}}\big(\mathbf{x}_{m,\mathcal{I}(0|\mathbf{y})}, \mathbf{y}_{\mathcal{I}(0|\mathbf{y})}\big) = d_{\mathrm{H}}\big(\mathbf{x}_{m,\mathcal{I}(1|\mathbf{y})}, \mathbf{y}_{\mathcal{I}(1|\mathbf{y})}\big) = 0\big\} \tag{106}$$

$$= \bigcup_{\mathsf{N}=0}^{n} \bigcup_{\substack{\mathcal{N} \subseteq \{1,\ldots,n\} \\ |\mathcal{N}|=\mathsf{N}}} \big\{\mathbf{y} \colon d_{\mathrm{H}}(\mathbf{2}_{\mathcal{N}}, \mathbf{y}_{\mathcal{N}}) = d_{\mathrm{H}}\big(\mathbf{x}_{m,\{1,\ldots,n\}\setminus\mathcal{N}}, \mathbf{y}_{\{1,\ldots,n\}\setminus\mathcal{N}}\big) = 0\big\} \tag{107}$$

where $\mathbf{2}$ denotes the all-two vector. Therefore, the conditional success probability of the closed decoding region $\overline{\mathcal{D}}_m$ is

$$\Pr\big(\overline{\mathcal{D}}_m \big| \mathbf{x}_m\big) = \sum_{\mathbf{y}\in\overline{\mathcal{D}}_m} P_{\mathbf{Y}|\mathbf{X}}\big(\mathbf{y}\big|\mathbf{x}_m\big) = \sum_{\mathsf{N}=0}^{n} \binom{n}{\mathsf{N}} \delta^{\mathsf{N}} (1-\delta)^{n-\mathsf{N}} = 1. \tag{108}$$

Similarly,

$$\bigcap_{i\in\mathcal{I}} \overline{\mathcal{D}}_i = \big\{\mathbf{y} \colon d_{\mathrm{H}}\big(\mathbf{x}_{i,\mathcal{I}(0|\mathbf{y})}, \mathbf{y}_{\mathcal{I}(0|\mathbf{y})}\big) = d_{\mathrm{H}}\big(\mathbf{x}_{i,\mathcal{I}(1|\mathbf{y})}, \mathbf{y}_{\mathcal{I}(1|\mathbf{y})}\big) = 0 \quad \forall\, i \in \mathcal{I}\big\} \tag{109}$$

$$= \bigcup_{\mathsf{N}=d_{\mathcal{I}}^{(\mathsf{M},n)}}^{n} \bigcup_{\substack{\mathbb{N}_n\setminus\mathcal{N} \subseteq \mathbb{N}_{\mathcal{I}} \\ |\mathcal{N}|=\mathsf{N}}} \big\{\mathbf{y} \colon d_{\mathrm{H}}(\mathbf{2}_{\mathcal{N}}, \mathbf{y}_{\mathcal{N}}) = d_{\mathrm{H}}\big(\mathbf{x}_{i_1,\mathbb{N}_n\setminus\mathcal{N}}, \mathbf{y}_{\mathbb{N}_n\setminus\mathcal{N}}\big) = 0\big\} \tag{110}$$

where for convenience, we abbreviate $\mathbb{N}_n \triangleq \{1,\ldots,n\}$ and $\mathbb{N}_{\mathcal{I}} = \mathbb{N}_{\{i_1,\ldots,i_r\}} \triangleq \{j \in \mathbb{N}_n \colon x_{i_1,j} = x_{i_2,j} = \cdots = x_{i_r,j}\}$. This implies

$$\Pr\left(\bigcap_{i\in\mathcal{I}} \overline{\mathcal{D}}_i \middle| \mathbf{x}_\ell\right) = \sum_{\mathbf{y}\in\bigcap_{i\in\mathcal{I}}\overline{\mathcal{D}}_i} P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y}|\mathbf{x}_{i_1}) \tag{111}$$

$$= \sum_{\mathsf{N}=d_{\mathcal{I}}^{(\mathsf{M},n)}}^{n} \binom{n-d_{\mathcal{I}}^{(\mathsf{M},n)}}{\mathsf{N}-d_{\mathcal{I}}^{(\mathsf{M},n)}} \delta^{\mathsf{N}} (1-\delta)^{n-\mathsf{N}} \tag{112}$$

$$= \delta^{d_{\mathcal{I}}^{(\mathsf{M},n)}}. \tag{113}$$

□

6.2 Optimal Codes with Two Codewords ($\mathsf{M} = 2$)

Theorem 50. *For a BEC and for any $n \geq 1$, an optimal codebook with two codewords $\mathsf{M} = 2$ is the (unique) weak flip code with parameter $t_1 = n$. It has an error probability*

$$P_{\mathrm{e}}\big(\mathscr{C}_n^{(2,n)}\big) = \frac{1}{2}\delta^n. \tag{114}$$

Proof: By Lemma 13 and since we have only one column in the candidate columns set, any codebook consisting of an arbitrary codeword and its flipped version is equivalent to $\mathscr{C}^{(2,n)}$ and hence is optimal. □

6.3 Optimal Codes with Three or Four Codewords ($\mathsf{M} = 3, 4$)

Even though we know the exact average error probability for a code with an arbitrary number of codewords M on a BEC, the optimal code structure is not obvious. We are now trying to shed more light on this ultimate problem.

We firstly start with the following lemma.

Lemma 51 ([6, Lem. 32]). *Fix the number of codewords M and a DMC. The success probability $P_{\mathrm{c}}(\mathscr{C}^{(\mathsf{M},n)})$ for a sequence of codes $\{\mathscr{C}^{(\mathsf{M},n)}\}_{n\geq 1}$, where each code is generated by appending a column to the code of smaller blocklength, is nondecreasing with respect to the blocklength n.*

Proof: See [6, Sec. VIII-B]. □

Lemma 51 suggests a recursive code construction that guarantees largest *total probability increase*,[10] i.e., we can find some locally optimal code parameters.

Theorem 52. *For a BEC with arbitrary erasure probability $0 \leq \delta < 1$, an optimal code with three codewords $\mathsf{M} = 3$ or four codewords $\mathsf{M} = 4$ and with a blocklength $n = 2$ is*

$$\mathscr{C}_{\mathrm{BEC}}^{(\mathsf{M},2)\diamond} = \begin{cases} \begin{pmatrix} \mathbf{c}_1^{(\mathsf{M})} & \mathbf{c}_2^{(\mathsf{M})} \end{pmatrix} & \text{if } \mathsf{M} = 3, \\ \begin{pmatrix} \mathbf{c}_3^{(\mathsf{M})} & \mathbf{c}_5^{(\mathsf{M})} \end{pmatrix} & \text{if } \mathsf{M} = 4. \end{cases} \tag{115}$$

If we recursively construct a locally optimal codebook with three codewords $\mathsf{M} = 3$ or four codewords $\mathsf{M} = 4$ and with a blocklength $n \geq 3$ by appending a new column to $\mathscr{C}_{\mathrm{BEC}}^{(\mathsf{M},n-1)\diamond}$, the increase in average success probability is maximized by the following choice of appended columns:

$$\begin{cases} \mathbf{c}_3^{(\mathsf{M})} & \text{if } n \bmod 3 = 0, \\ \mathbf{c}_1^{(\mathsf{M})} & \text{if } n \bmod 3 = 1, \\ \mathbf{c}_2^{(\mathsf{M})} & \text{if } n \bmod 3 = 2, \end{cases} \quad \text{when } \mathsf{M} = 3 \tag{116}$$

and

$$\begin{cases} \mathbf{c}_6^{(\mathsf{M})} & \text{if } n \bmod 3 = 0, \\ \mathbf{c}_3^{(\mathsf{M})} & \text{if } n \bmod 3 = 1, \\ \mathbf{c}_5^{(\mathsf{M})} & \text{if } n \bmod 3 = 2, \end{cases} \quad \text{when } \mathsf{M} = 4. \tag{117}$$

[10] See [6, Def. 33].

Proof: See Appendix A. □

This theorem suggests that for a given fixed code size M, a sequence of good codes can be generated by appending the correct columns to a code of smaller blocklength. For a given DMC and code of blocklength n, we ask the question what is the optimal improvement (i.e., the maximum reduction of error probability) when increasing the blocklength from n to $n+\gamma$ (with $\gamma = 1$) when $\mathsf{M} = 3$ or 4 (note that γ may be larger than 1 when $\mathsf{M} \geq 5$). The answer to this question then leads to the recursive construction of (116) and (117).

While Theorem 52 only guarantees local optimality for the given recursive construction, further investigation shows that the given construction is actually globally optimum.

Theorem 53. *For a BEC and for any $n \geq 2$, an optimal codebook with $\mathsf{M} = 3$ or $\mathsf{M} = 4$ codewords is the weak flip code of type $\mathbf{t}^*_{\text{weak}}$, where for $\mathsf{M} = 3$*

$$t_1^* = \left\lfloor \frac{n+2}{3} \right\rfloor, \quad t_2^* = \left\lfloor \frac{n+1}{3} \right\rfloor, \quad t_3^* = \left\lfloor \frac{n}{3} \right\rfloor \tag{118}$$

and for $\mathsf{M} = 4$

$$t_3^* = \left\lfloor \frac{n+2}{3} \right\rfloor, \quad t_5^* = \left\lfloor \frac{n+1}{3} \right\rfloor, \quad t_6^* = \left\lfloor \frac{n}{3} \right\rfloor. \tag{119}$$

Note that the recursively constructed code of Theorem 52 is equivalent to the optimal code given here:

$$\mathscr{C}_{\text{BEC}}^{(\mathsf{M},n)\diamond} \equiv \mathscr{C}_{\mathbf{t}^*_{\text{weak}}}^{(\mathsf{M},n)}. \tag{120}$$

Proof: See Appendix B. □

Using the shorthand

$$k \triangleq \left\lfloor \frac{n}{3} \right\rfloor, \tag{121}$$

the code parameters of these optimal codes can be summarized as

$$\mathbf{t}^*_{\text{weak}} = \begin{cases} [t_1^*, t_2^*, t_3^*] & \text{for } \mathsf{M} = 3, \\ [t_3^*, t_5^*, t_6^*] & \text{for } \mathsf{M} = 4 \end{cases} \tag{122}$$

$$= \begin{cases} [k, k, k] & \text{if } n \bmod 3 = 0, \\ [k+1, k, k] & \text{if } n \bmod 3 = 1, \\ [k+1, k+1, k] & \text{if } n \bmod 3 = 2. \end{cases} \tag{123}$$

From (116) and (117), or from (118) and (119), or from (122), we confirm again what has been addressed in Remark 18, and that $\mathscr{C}_{\mathbf{t}^*_{\text{weak}}}^{(3,n)}$ can be obtained by simply removing the last codeword of $\mathscr{C}_{\mathbf{t}^*_{\text{weak}}}^{(4,n)}$.

The corresponding optimal average error probabilities are given as

$$P_{\text{e}}\Big(\mathscr{C}_{\mathbf{t}^*_{\text{weak}}}^{(\mathsf{M},n)}\Big) = \begin{cases} \frac{1}{3}\big(\delta^{n-t_1^*} + \delta^{n-t_2^*} + \delta^{n-t_3^*} - \delta^n\big) & \text{if } \mathsf{M} = 3, \\ \frac{1}{4}\big(2\delta^{n-t_3^*} + 2\delta^{n-t_5^*} + 2\delta^{n-t_6^*} - 3\delta^n\big) & \text{if } \mathsf{M} = 4. \end{cases} \tag{124}$$

6.4 Quick Comparison between BSC and BEC

In [6], it has been shown that the optimal codes for $\mathsf{M} = 3$ or $\mathsf{M} = 4$ for the BSC are weak flip codes with code parameters

$$\mathbf{t}^*_{\text{weak}} = \begin{cases} [k+1, k, k-1] & \text{if } n \bmod 3 = 0, \\ [k+1, k, k] & \text{if } n \bmod 3 = 1, \\ [k+1, k+1, k] & \text{if } n \bmod 3 = 2. \end{cases} \tag{125}$$

The corresponding pairwise Hamming distance vectors (see Corollary 46) are

$$\mathbf{d}^{(3,n)*} = \begin{cases} (2k-1, 2k, 2k+1) & \text{if } n \bmod 3 = 0, \\ (2k, 2k+1, 2k+1) & \text{if } n \bmod 3 = 1, \\ (2k+1, 2k+1, 2k+2) & \text{if } n \bmod 3 = 2, \end{cases} \tag{126}$$

and

$$\mathbf{d}^{(4,n)*} = \begin{cases} (2k-1, 2k, 2k+1, 2k+1, 2k, 2k-1) & \text{if } n \bmod 3 = 0, \\ (2k, 2k+1, 2k+1, 2k+1, 2k+1, 2k) & \text{if } n \bmod 3 = 1, \\ (2k+1, 2k+1, 2k+2, 2k+2, 2k+1, 2k+1) & \text{if } n \bmod 3 = 2, \end{cases} \tag{127}$$

respectively. Comparing these to the corresponding pairwise Hamming distance vectors for the BEC (see Theorem 53),

$$\mathbf{d}^{(3,n)*} = \begin{cases} (2k, 2k, 2k) & \text{if } n \bmod 3 = 0, \\ (2k, 2k+1, 2k+1) & \text{if } n \bmod 3 = 1, \\ (2k+1, 2k+1, 2k+2) & \text{if } n \bmod 3 = 2 \end{cases} \tag{128}$$

and

$$\mathbf{d}^{(4,n)*} = \begin{cases} (2k, 2k, 2k, 2k, 2k, 2k) & \text{if } n \bmod 3 = 0, \\ (2k, 2k+1, 2k+1, 2k+1, 2k+1, 2k) & \text{if } n \bmod 3 = 1, \\ (2k+1, 2k+1, 2k+2, 2k+2, 2k+1, 2k+1) & \text{if } n \bmod 3 = 2, \end{cases} \tag{129}$$

we can draw the following conclusion.[11]

Corollary 54. *Apart from* $n \bmod 3 = 0$*, the optimal codes for the BSC are identical to the optimal codes for the BEC for* $\mathsf{M} = 3$ *or* $\mathsf{M} = 4$ *codewords.*

It is interesting to note that when $n \bmod 3 = 0$, the optimal codes for the BEC are fair and therefore maximize the minimum Hamming distance (while this is not the case for the very symmetric BSC). However, the converse is *not* true: if a code maximizes the minimum Hamming distance, then it is not necessarily an optimal code for the BEC! Thus, in particular, it is not clear whether binary nonlinear Hadamard codes are optimal. As we will see in the cases of $\mathsf{M} = 5, 6$, the pairwise Hamming distance vector (2-wise Hamming distance) is not enough to determine the global optimality among all possible codes; therefore the r-wise Hamming distances with $r > 2$ have to be taken into account.

[11] For a BEC and for weak flip codes with $\mathsf{M} = 3$ or $\mathsf{M} = 4$ codewords, we only need to compare the pairwise Hamming distances because the 3-wise and 4-wise Hamming distances are all identical.

6.5 Application to Known Bounds on the Error Probability for a Finite Blocklength ($\mathsf{M} = 3, 4$)

Since we now know the optimal code structure, we can compare its performance to the known bounds in Section 4.

Note that the optimal error exponents for $\mathsf{M} = 3, 4$ codewords are

$$\mathsf{E}_3 = \mathsf{E}_4 = -\frac{2}{3}\log\delta. \tag{130}$$

Moreover, for $\mathsf{M} = 3, 4$,

$$\mathsf{D}_{\min}^{(\mathrm{BEC})}\left(\mathscr{C}_{\mathbf{t}^*_{\mathrm{weak}}}^{(\mathsf{M},n)}\right) = \begin{cases} -\frac{2}{3}\log\delta & \text{if } n \bmod 3 = 0, \\ -\frac{\lfloor \frac{n}{3} \rfloor + \lfloor \frac{n+1}{3} \rfloor}{n}\log\delta & \text{if } n \bmod 3 = 1, \\ -\frac{\lfloor \frac{n}{3} \rfloor + \lfloor \frac{n+1}{3} \rfloor}{n}\log\delta & \text{if } n \bmod 3 = 2. \end{cases} \tag{131}$$

Figures 2 and 3 compare the exact optimal performances for $\mathsf{M} = 3$ and $\mathsf{M} = 4$, respectively, with some bounds: the SGB upper and lower bounds based on the optimal code as used by Shannon *et al.* for every $n \bmod 3 = 0$ (thereby confirming that this lower bound is valid generally), the Gallager upper bound, and also the PPV upper and lower bounds.

We can see that the SGB upper bound is closer to the exact optimal performance (and hence tighter) than the PPV upper bound and the Gallager upper bound. Note that the PPV upper bound is not exactly the same as the Gallager upper bound, even though for $\mathsf{M} = 3$ their curves look almost identical. Also note that the SGB upper bound does exhibit the correct error exponent. It is shown in [11] that when n goes to infinity under fixed M, the PPV upper bound only tends to the suboptimal Gallager exponent [8]; this fact is confirmed again by the two figures.

Concerning the lower bounds, we see that the PPV lower bound is much better for finite n than the SGB lower bound. However, the exponential growth rate of the PPV lower bound only approaches that of the sphere-packing bound [12], and does not equal the optimal exponent E_{M} either [9].

Once more we would like to emphasize that even though for $\mathsf{M} = 3, 4$, the fair weak flip codes are optimal for the BEC and achieves the optimal error exponent for both the BEC and the BSC, they are strictly suboptimal for every $n \bmod 3 = 0$ for the BSC.

6.6 Optimal Codes with Five or Six Codewords ($\mathsf{M} = 5, 6$)

The idea of recursively designing a locally optimal code turned out to be a powerful approach to obtain globally optimal codes for $\mathsf{M} = 3, 4$. Unfortunately, for larger values of M, we might need a recursion from n to $n + \gamma$ with a step-size $\gamma > 1$, and—according to our numerical examination— this step-size γ might be a function of the blocklength n. Since the exact average error probability expression becomes involved as M grows, we only succeeded in investigating globally optimal code construction subject to the recursive design approach when block length n is a multiple of L. Based on our definition of fair weak flip codes and on Theorem 55 below, we conjecture that the necessary step-size for global optimality satisfies $\gamma \leq \mathsf{L}$.

For n being a multiple of L, we succeeded to find globally optimal codes.

Theorem 55. *For a BEC and for any n being a multiple of $\mathsf{L} = 10$, an optimal codebook with $\mathsf{M} = 5$ or $\mathsf{M} = 6$ codewords is the corresponding fair weak flip code.*

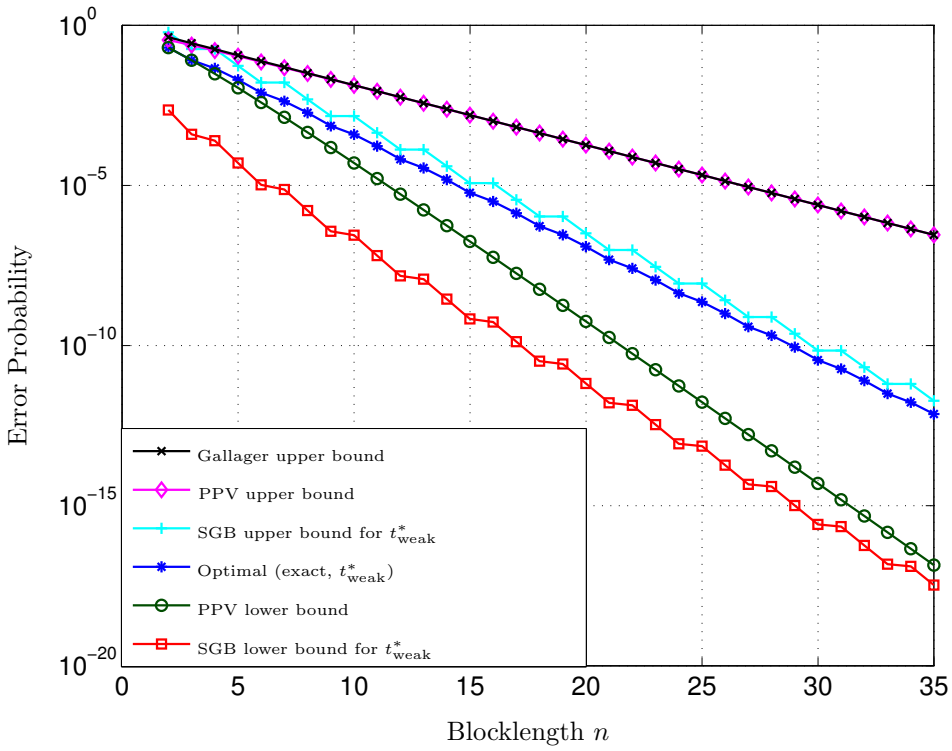

Figure 2: Exact value of, and bounds on, the performance of an optimal code with $\mathrm{M} = 3$ codewords on the BEC with $\delta = 0.3$ as a function of blocklength n.

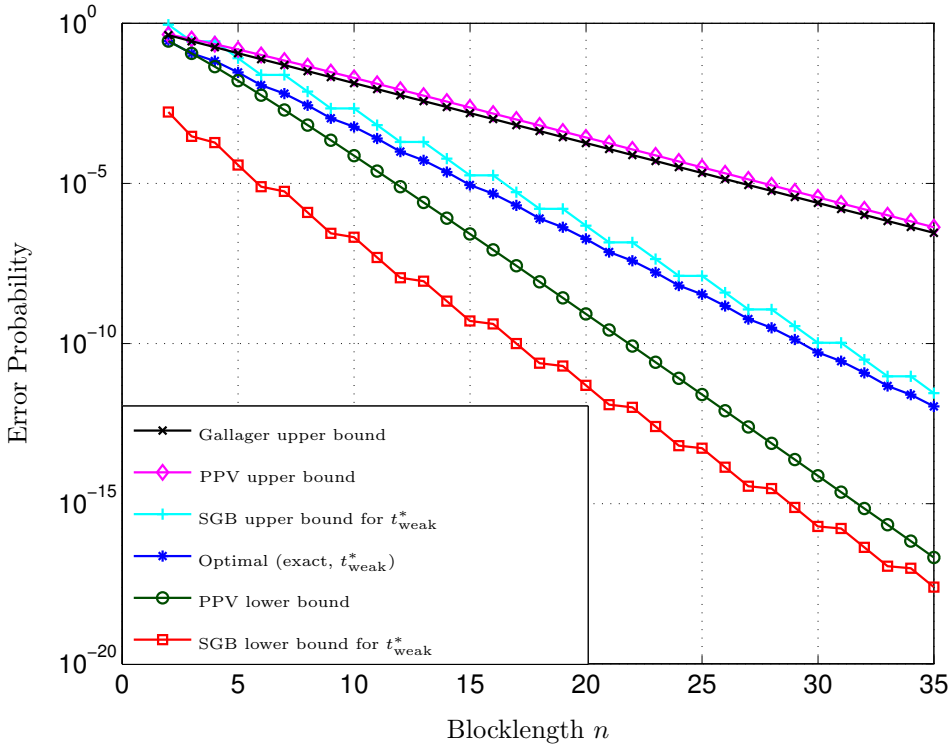

Figure 3: Exact value of, and bounds on, the performance of an optimal code with $\mathrm{M} = 4$ codewords on the BEC with $\delta = 0.3$ as a function of blocklength n.

Proof: See Appendix C. □

Note that the restriction on n comes from the restriction that fair weak flip codes are only defined for n with $n \bmod \mathsf{L} = 0$, for which case the optimal code uses each of the weak flip columns κ times, where $\kappa = n/\mathsf{L}$ is an integer. We can show that if we relax the error minimization problem by allowing noninteger values for the code parameters $\mathbf{t}$, the optimal code parameters will be equally distributed among all possible weak flip columns also when $n \bmod \mathsf{L} \neq 0$. Unfortunately, a block-code always must use integer numbers of candidate columns and the globally optimal choice of integers in the neighborhood of the optimal noninteger values is rather involved. Based on this observation and on our extensive numerical examinations, we give the following conjecture.

Conjecture 56. *Consider the BEC and a blocklength $n \geq 3$, and define the shorthand*

$$\kappa \triangleq \left\lfloor \frac{n}{10} \right\rfloor. \tag{132}$$

An optimal code that minimizes the average error probability among all code designs with $\mathsf{M} = 5$ codewords is a weak flip code with code parameters given by:

$$\mathbf{t}_{\text{weak}} = \left[t_3, t_5, t_6, t_7, t_9, t_{10}, t_{11}, t_{12}, t_{13}, t_{14}\right]$$
$$= \begin{cases} \left[\kappa+1, \kappa, \kappa, \kappa, \kappa, \kappa, \kappa, \kappa, \kappa, \kappa\right] & \text{if } n \bmod 10 = 1, \\ \left[\kappa+1, \kappa+1, \kappa+1, \kappa-1, \kappa, \kappa, \kappa, \kappa, \kappa, \kappa\right] & \text{if } n \bmod 10 = 2, \\ \left[\kappa+1, \kappa+1, \kappa, \kappa, \kappa+1, \kappa, \kappa, \kappa, \kappa, \kappa\right] & \text{if } n \bmod 10 = 3, \\ \left[\kappa+1, \kappa+1, \kappa, \kappa, \kappa+1, \kappa, \kappa, \kappa, \kappa, \kappa+1\right] & \text{if } n \bmod 10 = 4, \\ \left[\kappa+1, \kappa+1, \kappa+1, \kappa, \kappa+1, \kappa+1, \kappa, \kappa, \kappa, \kappa\right] & \text{if } n \bmod 10 = 5, \\ \left[\kappa+1, \kappa+1, \kappa+1, \kappa, \kappa+1, \kappa+1, \kappa, \kappa+1, \kappa, \kappa\right] & \text{if } n \bmod 10 = 6, \\ \left[\kappa+1, \kappa+1, \kappa+1, \kappa, \kappa+1, \kappa+1, \kappa, \kappa, \kappa+1, \kappa+1\right] & \text{if } n \bmod 10 = 7, \\ \left[\kappa+2, \kappa+1, \kappa+1, \kappa, \kappa+1, \kappa+1, \kappa, \kappa, \kappa+1, \kappa+1\right] & \text{if } n \bmod 10 = 8. \\ \left[\kappa+1, \kappa+1, \kappa+1, \kappa+1, \kappa+1, \kappa+1, \kappa+1, \kappa+1, \kappa+1, \kappa\right] & \\ & \text{if } n \bmod 10 = 9. \end{cases} \tag{133}$$

Except for $n \bmod 10 = 7$, an optimal code that minimizes the average error probability among all code designs with $\mathsf{M} = 6$ codewords is a weak flip code with code parameters given by:

$$\mathbf{t}_{\text{weak}} = \left[t_7, t_{11}, t_{13}, t_{14}, t_{19}, t_{21}, t_{22}, t_{25}, t_{26}, t_{28}\right]$$
$$= \begin{cases} \left[\kappa+1, \kappa, \kappa, \kappa, \kappa, \kappa, \kappa, \kappa, \kappa, \kappa\right] & \text{if } n \bmod 10 = 1, \\ \left[\kappa+1, \kappa+1, \kappa, \kappa, \kappa, \kappa, \kappa, \kappa, \kappa, \kappa\right] & \text{if } n \bmod 10 = 2, \\ \left[\kappa+1, \kappa+1, \kappa, \kappa, \kappa, \kappa+1, \kappa, \kappa, \kappa, \kappa\right] & \text{if } n \bmod 10 = 3, \\ \left[\kappa+1, \kappa+1, \kappa, \kappa, \kappa, \kappa+1, \kappa, \kappa+1, \kappa, \kappa\right] & \text{if } n \bmod 10 = 4, \\ \left[\kappa+1, \kappa+1, \kappa, \kappa, \kappa+1, \kappa+1, \kappa, \kappa+1, \kappa, \kappa\right] & \text{if } n \bmod 10 = 5, \\ \left[\kappa+1, \kappa+1, \kappa+1, \kappa, \kappa+1, \kappa+1, \kappa, \kappa+1, \kappa, \kappa\right] & \text{if } n \bmod 10 = 6, \\ \left[\kappa+1, \kappa+1, \kappa+1, \kappa+1, \kappa+1, \kappa+1, \kappa+1, \kappa+1, \kappa, \kappa\right] & \\ & \text{if } n \bmod 10 = 8, \\ \left[\kappa+1, \kappa+1, \kappa+1, \kappa+1, \kappa+1, \kappa+1, \kappa+1, \kappa+1, \kappa+1, \kappa\right] & \\ & \text{if } n \bmod 10 = 9. \end{cases} \tag{134}$$

For $n \bmod 10 = 7$ and $\mathsf{M} = 6$, an optimal code that minimizes the average error probability among all code designs is actually not a weak flip code but a nonweak flip code with code parameters given by

$$\begin{cases} t_{14} = t_{22} = t_{26} = t_{28} = \kappa, \\ t_7 = t_{11} = t_{13} = t_{19} = t_{21} = t_{25} = \kappa + 1, \\ t_{30} = 1, \\ t_j = 0 \text{ for the remaining indices.} \end{cases} \tag{135}$$

Note that t_{30} is the only nonweak flip column in this code.

Surprisingly, the optimal code for $n \bmod 10 = 7$ and $\mathsf{M} = 6$ is not a weak flip code. We point out again that the exact average error probability expression for the BEC with $\mathsf{M} = 6$ is a function of the discrete multivariate nonnegative integers $t_1, t_2, \ldots, t_{31}$ under the constraint that their sum equals n. If we allow noninteger solutions, the minimizers are $t_j = n/\mathsf{L}$ for all t_j enumerating weak flip columns. Yet, (135) shows that the nearest *integer* minimizer might be a only nearly weak flip code instead of a weak flip code.

Note that according to Conjecture 56, it is possible to recursively construct optimal codes with $\mathsf{M} = 5, 6$ codewords using a step size $\gamma < 10$.

Further theoretical substantiation of these observations should be useful when considering optimal codes for larger M.

7 Conclusion

Based on a column-wise analysis of codebooks, we have provided an extension to the pairwise Hamming distance, called *r-wise Hamming distance*, and shown that it actually is a key factor to determine the exact error probability for an optimal code of arbitrary blocklength n on a BEC.

We have introduced the *weak flip codes*, a new class of codes containing both the class of binary nonlinear Hadamard codes and the class of linear codes as special cases. We have shown that weak flip codes have many desirable properties; in particular, we have been able to prove that besides retaining many of the good Hamming distance properties of Hadamard codes, they are actually optimal with respect to the minimum error probability over a binary erasure channel (BEC) for certain numbers of codewords M and many finite blocklengths n.

We have also introduced the subclass of *fair weak flip codes* that can be seen as a generalization of linear codes to arbitrary numbers of codewords M. We have shown that fair weak flip codes are optimal with respect to the error probability for the BEC for $\mathsf{M} \leq 6$ and a blocklength that depends on M. Furthermore, we have also shown that the optimal code performance is really close to the upper bound of Shannon–Gallager–Berlekamp on the BEC for $\mathsf{M} \leq 4$, while for the BSC this is not the case.

Note that it has been known for quite some time that binary nonlinear Hadamard codes have good Hamming distance properties [4]; however, their behavior with respect to error probability for finite blocklength remained uninvestigated. In particular, while fair weak flip codes have been used before (although without being named) in the derivation of results related to error probability [9] and have been shown to be error-exponent achieving, their global (among all possible linear or nonlinear codes) optimality with respect to the error probability was not known so far.

In conclusion, this report tries to build a bridge between coding theory, which usually is concerned with the design of codes with good Hamming distance properties (like, e.g., the binary nonlinear Hadamard codes), and information theory, which deals with error probability and with the existence of codes that have good or optimal error probability behavior (often in the asymptotic sense for very large blocklength).

References

[1] Claude E. Shannon, "A mathematical theory of communication," *Bell System Technical Journal*, vol. 27, pp. 379–423 and 623–656, July and October 1948.

[2] Shu Lin and Daniel J. Costello, Jr., *Error Control Coding*, 2nd ed. Upper Saddle River, NJ, USA: Prentice-Hall, 2004.

[3] Chia-Lung Wu, Po-Ning Chen, Yunghsiang S. Han, and Yan-Xiu Zheng, "On the coding scheme for joint channel estimation and error correction over block fading channels," in *Proceedings IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, Tokyo, Japan, September 13–16, 2009, pp. 1272–1276.

[4] F. Jessy MacWilliams and Neil J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1977.

[5] Po-Ning Chen, Hsuan-Yin Lin, and Stefan M. Moser, "Weak flip codes and applications to optimal code design on the binary erasure channel," in *Proceedings Fiftieth Allerton Conference on Communication, Control and Computing*, Allerton House, Monticello, IL, USA, October 1–5, 2012, pp. 160–167.

[6] ——, "Optimal ultrasmall block-codes for binary discrete memoryless channels," *IEEE Transactions on Information Theory*, vol. 59, no. 11, pp. 7346–7378, November 2013.

[7] Stefan M. Moser, *Information Theory (Lecture Notes)*, version 1, fall semester 2011/2012, Information Theory Lab, Department of Electrical Engineering, National Chiao Tung University (NCTU), September 2011. [Online]. Available: http://moser-isi.ethz.ch/scripts.html

[8] Robert G. Gallager, *Information Theory and Reliable Communication*. New York, NY, USA: John Wiley & Sons, 1968.

[9] Claude E. Shannon, Robert G. Gallager, and Elwyn R. Berlekamp, "Lower bounds to error probability for coding on discrete memoryless channels," *Information and Control*, pp. 522–552, May 1967, part II.

[10] Po-Ning Chen, Hsuan-Yin Lin, and Stefan M. Moser, "Equidistant codes meeting the Plotkin bound are not optimal on the binary symmetric channel," in *Proceedings IEEE International Symposium on Information Theory (ISIT)*, Istanbul, Turkey, July 7–13, 2013, pp. 3015–3019.

[11] Yury Polyanskiy, H. Vincent Poor, and Sergio Verdú, "Channel coding rate in the finite blocklength regime," *IEEE Transactions on Information Theory*, vol. 56, no. 5, pp. 2307–2359, May 2010.

[12] Yury Polyanskiy, "Saddle point in the minimax converse for channel coding," *IEEE Transactions on Information Theory*, vol. 59, no. 5, pp. 2576–2595, May 2013.

[13] Richard A. Brualdi, *Introductory Combinatorics*, 5th ed. Upper Saddle River, NJ, USA: Prentice-Hall, 2010.

A Appendix: Proof of Theorem 52

We refer to [6, Def. 33] and define

$$P_{\mathrm{c}}\big(\mathscr{C}^{(\mathsf{M},n+\gamma)}\big) = P_{\mathrm{c}}\big(\mathscr{C}^{(\mathsf{M},n)}\big) + \frac{1}{\mathsf{M}}\sum_{m=1}^{\mathsf{M}} \sum_{\substack{\mathbf{y}^{(n+\gamma)} \\ \text{s.t. } \mathbf{y}^{(n)}\in\mathcal{D}_m^{(\mathsf{M},n)} \\ \text{but } \mathbf{y}^{(n+\gamma)}\in\mathcal{D}_{m'}^{(\mathsf{M},n+\gamma)} \\ \text{for some } m'\neq m}} \Big(P_{\mathbf{Y}|\mathbf{X}}\Big(\mathbf{y}^{(n+\gamma)}\Big|\mathbf{x}_{m'}^{(n+\gamma)}\Big) - P_{\mathbf{Y}|\mathbf{X}}\big(\mathbf{y}^{(n+\gamma)}\big|\mathbf{x}_{m}^{(n+\gamma)}\big)\Big) \tag{136}$$

$$\triangleq P_{\mathrm{c}}\big(\mathscr{C}^{(\mathsf{M},n)}\big) + \Delta\Psi\big(\mathscr{C}^{(\mathsf{M},n+\gamma)}\big). \tag{137}$$

In the proof of Theorem 52, our goal is to maximize the total probability increase $\Delta\Psi\big(\mathscr{C}^{(\mathsf{M},n+\gamma)}\big)$ among all possible $\mathscr{C}^{(\mathsf{M},\gamma)}$ with $\gamma = 1$ for $\mathsf{M} = 3, 4$. Note that codebook $\mathscr{C}^{(\mathsf{M},n+\gamma)}$ is formed by concatenating $\mathscr{C}^{(\mathsf{M},n)}$ with $\mathscr{C}^{(\mathsf{M},\gamma)}$. This induction proof for a BEC follows along the lines of the proof for the BSC shown in [6, App. C.A] with some modifications that take into account the details of the decoding rule for the BEC. Similarly to [6, App. C.A], we need a case distinction depending on n mod 3. For space reason, we only outline the case from $n-1 = 3k-1$ to $n = 3k$. Moreover, we only consider the more complicated case of $\mathsf{M} = 4$. Similar arguments can be applied to $\mathsf{M} = 3$.

We have reduced the number of candidate columns to $\mathcal{C}^{(4)}$. We start with the code $\mathscr{C}^{(4,n)}_{\mathbf{t}^{\diamond}_{\mathrm{weak}}}$, whose code parameters are as follows:

$$\mathbf{t}^{\diamond}_{\mathrm{weak}} = [t_3^{\diamond}, t_5^{\diamond}, t_6^{\diamond}] = [k, k, k-1]. \tag{138}$$

We require to show that appending $\mathbf{c}_6^{(4)}$ yields the largest total probability increase among all possible candidate columns in $\mathcal{C}^{(4)}$. Later in the proof, we establish extended decoding regions to compute the total probability increase.

Consider the three possible extended decoding regions of blocklength n, i.e., $\big[\mathcal{D}_m^{(4,n-1)}\ 0\big]$, $\big[\mathcal{D}_m^{(4,n-1)}\ 1\big]$, and $\big[\mathcal{D}_m^{(4,n-1)}\ 2\big]$, for $m = 1, \ldots, 4$. Owing to $P_{Y|X}(0|1) = P_{Y|X}(1|0) = 0$, we know for the mth new codeword of blocklength n with $x_{m,n} = b$, where $b \in \{0, 1\}$, its extended decoding region $\mathcal{D}_m^{(4,n)}$ should include both $\big[\mathcal{D}_m^{(4,n-1)}\ b\big]$ and $\big[\mathcal{D}_m^{(4,n-1)}\ 2\big]$, and all the received vectors in $\big[\mathcal{D}_m^{(4,n-1)}\ \bar{b}\big]$ will be decoded to one of the other three codewords. Since

$$\psi_m\big(\mathscr{C}^{(4,n-1)}\big) = \psi_m\big(\mathscr{C}^{(4,n-1)}\big)\cdot(1-\delta+\delta) \tag{139}$$

$$= \Pr\Big(\mathcal{D}_m^{(4,n-1)}\Big|\mathbf{x}_m^{(n-1)}\Big)\big(P_{Y|X}(b|b) + P_{Y|X}(2|b)\big) \tag{140}$$

$$= \Pr\Big(\big[\mathcal{D}_m^{(4,n-1)}\ b\big]\Big|\big[\mathbf{x}_m^{(n-1)}\ b\big]\Big) + \Pr\Big(\big[\mathcal{D}_m^{(4,n-1)}\ 2\big]\Big|\big[\mathbf{x}_m^{(n-1)}\ b\big]\Big), \tag{141}$$

we obtain that $\psi_m(\mathscr{C}^{(4,n)})$ is no less than $\psi_m(\mathscr{C}^{(4,n-1)})$. As a result, the total probability increase for each codeword will be determined by how the received vectors

in $\big[\mathcal{D}_m^{(4,n-1)}\ \overline{b}\big]$ are decoded to the other three codewords. Now we consider the appended columns in a case by case fashion.

Appending $\mathbf{c}_1^{(4)}$: We build a new length-n code $\mathscr{C}_{\mathbf{t}}^{(4,n)}$ from the given code $\mathscr{C}_{\mathbf{t}_{\text{weak}}^{\diamond}}^{(4,n-1)}$ by appending $\mathbf{c}_1^{(4)} = (0\ 0\ 0\ 1)^{\mathsf{T}}$. The code parameters become

$$\mathbf{t}_1 = [1, 0, k, 0, k, k-1, 0]. \tag{142}$$

We now compute the total probability increase in this case. Because $x_{4,n} = 1$ and $x_{m,n} = 0$ for $m = 1, 2, 3$, there are some received vectors in the extended decoding regions $\big[\mathcal{D}_{\mathbf{t}_{\text{weak}}^{\diamond};m}^{(4,n-1)}\ 1\big]$, $m = 1, 2, 3$, that will be decoded to $\mathcal{D}_{\mathbf{t}_1;4}^{(4,n)}$ (and there are some received vectors in the extended decoding region $\big[\mathcal{D}_{\mathbf{t}_{\text{weak}}^{\diamond};4}^{(4,n-1)}\ 0\big]$ that will be decoded to $\mathcal{D}_{\mathbf{t}_1;m}^{(4,n)}$, $m = 1, 2, 3$). The total probability increase $\Delta\Psi\big(\mathscr{C}_{\mathbf{t}_1}^{(4,n)}\big)$ is

$$\begin{aligned}
&\Delta\Psi\Big(\mathscr{C}_{\mathbf{t}_1}^{(4,n)}\Big) \\
&\quad= \Pr\Big(\big[\mathcal{D}_4^{(4,n-1)}\ 1\big] \\
&\qquad\qquad \cap \Big(\big[\mathcal{D}_1^{(4,n-1)}\ 1\big] \cup \big[\mathcal{D}_2^{(4,n-1)}\ 1\big] \cup \big[\mathcal{D}_3^{(4,n-1)}\ 1\big]\Big)\ \Big|\ \big[\mathbf{x}_4^{(n-1)}\ 1\big]\Big) && (143)\\
&\quad= \Pr\left(\overline{\mathcal{D}}_4^{(4,n-1)} \cap \left(\bigcup_{m=1}^{3} \overline{\mathcal{D}}_m^{(4,n-1)}\right)\ \middle|\ \mathbf{x}_4^{(n-1)}\right)(1-\delta) && (144)\\
&\quad= \Pr\left(\bigcup_{m=1}^{3} \big(\overline{\mathcal{D}}_m^{(4,n-1)} \cap \overline{\mathcal{D}}_4^{(4,n-1)}\big)\ \middle|\ \mathbf{x}_4^{(n-1)}\right)(1-\delta) && (145)\\
&\quad= \Big(\Pr\Big(\overline{\mathcal{D}}_1^{(4,n-1)} \cap \overline{\mathcal{D}}_4^{(4,n-1)}\ \Big|\ \mathbf{x}_4^{(n-1)}\Big) \\
&\qquad + \Pr\Big(\overline{\mathcal{D}}_2^{(4,n-1)} \cap \overline{\mathcal{D}}_4^{(4,n-1)}\ \Big|\ \mathbf{x}_4^{(n-1)}\Big) \\
&\qquad + \Pr\Big(\overline{\mathcal{D}}_3^{(4,n-1)} \cap \overline{\mathcal{D}}_4^{(4,n-1)}\ \Big|\ \mathbf{x}_4^{(n-1)}\Big) \\
&\qquad - \Pr\Big(\overline{\mathcal{D}}_1^{(4,n-1)} \cap \overline{\mathcal{D}}_2^{(4,n-1)} \cap \overline{\mathcal{D}}_4^{(4,n-1)}\ \Big|\ \mathbf{x}_4^{(n-1)}\Big) \\
&\qquad - \Pr\Big(\overline{\mathcal{D}}_1^{(4,n-1)} \cap \overline{\mathcal{D}}_3^{(4,n-1)} \cap \overline{\mathcal{D}}_4^{(4,n-1)}\ \Big|\ \mathbf{x}_4^{(n-1)}\Big) \\
&\qquad - \Pr\Big(\overline{\mathcal{D}}_2^{(4,n-1)} \cap \overline{\mathcal{D}}_3^{(4,n-1)} \cap \overline{\mathcal{D}}_4^{(4,n-1)}\ \Big|\ \mathbf{x}_4^{(n-1)}\Big) \\
&\qquad + \Pr\Big(\overline{\mathcal{D}}_1^{(4,n-1)} \cap \overline{\mathcal{D}}_2^{(4,n-1)} \cap \overline{\mathcal{D}}_3^{(4,n-1)} \cap \overline{\mathcal{D}}_4^{(4,n-1)}\ \Big|\ \mathbf{x}_4^{(n-1)}\Big)\Big)(1-\delta) && (146)\\
&\quad= \big(\delta^{n-1-t_6^{\diamond}} + \delta^{n-1-t_5^{\diamond}} + \delta^{n-1-t_3^{\diamond}} - \delta^{n-1} - \delta^{n-1} - \delta^{n-1} + \delta^{n-1}\big)(1-\delta) && (147)\\
&\quad= \big(\delta^{2k-1} + \delta^{2k-1} + \delta^{2k} - 2\delta^{n-1}\big)(1-\delta), && (148)
\end{aligned}$$

where (143) holds because the regions $\big[\mathcal{D}_4^{(4,n-1)}\ 1\big] \cap \big[\mathcal{D}_m^{(4,n-1)}\ 1\big]$, $m = 1, 2, 3$, are not disjoint; (144) is due to the definition of the closed decoding regions and because the BEC is a DMC; (146) follows directly from applying the inclusion–exclusion principle; finally, (147) follows from the same r-wise Hamming distances perspective as already used in the derivations of Theorem 49.

Appending $\mathbf{c}_2^{(4)}$: The derivations here are similar to the first case (or, indeed, also for the cases of appending $\mathbf{c}_4^{(4)}$ or $\mathbf{c}_7^{(4)}$), so we omit the details and directly

state the total probability increase:

$$\begin{aligned}
&\Delta\Psi\Big(\mathscr{C}_{\mathbf{t}_2}^{(4,n)}\Big)\\
&\quad= \big(\delta^{n-1-t_5^\diamond} + \delta^{n-1-t_6^\diamond} + \delta^{n-1-t_3^\diamond} - \delta^{n-1} - \delta^{n-1} - \delta^{n-1} + \delta^{n-1}\big)(1-\delta) \quad (149)\\
&\quad= \big(\delta^{2k-1} + \delta^{2k-1} + \delta^{2k} - 2\delta^{n-1}\big)(1-\delta). \quad (150)
\end{aligned}$$

Appending $\mathbf{c}_3^{(4)}$: If we append $\mathbf{c}_3^{(4)} = (0\ 0\ 1\ 1)^\mathsf{T}$, the new code parameters for blocklength n become

$$\mathbf{t}_3 = [0, 0, k+1, 0, k, k-1, 0]. \quad (151)$$

Since $x_{1,n} = x_{2,n} = 0$ and $x_{3,n} = x_{4,n} = 1$, again using an argument like in the first case, we find that there are some received vectors in the extended decoding regions $\big[\mathcal{D}_{\mathbf{t}_{\text{weak}}^\diamond;1}^{(4,n-1)}\ 1\big]$ and $\big[\mathcal{D}_{\mathbf{t}_{\text{weak}}^\diamond;2}^{(4,n-1)}\ 1\big]$ that will be decoded to either $\mathcal{D}_{\mathbf{t}_3;3}^{(4,n)}$ or $\mathcal{D}_{\mathbf{t}_3;4}^{(4,n)}$. Hence, we obtain a total probability increase

$$\begin{aligned}
&\Delta\Psi\Big(\mathscr{C}_{\mathbf{t}_3}^{(4,n)}\Big)\\
&\quad= \Pr\Big(\Big(\big[\mathcal{D}_1^{(4,n-1)}\ 1\big] \cup \big[\mathcal{D}_2^{(4,n-1)}\ 1\big]\Big) \cap \big[\mathcal{D}_3^{(4,n-1)}\ 1\big]\Big|\big[\mathbf{x}_3^{(n-1)}\ 1\big]\Big)\\
&\qquad+ \Pr\Big(\Big(\big[\mathcal{D}_1^{(4,n-1)}\ 1\big] \cup \big[\mathcal{D}_2^{(4,n-1)}\ 1\big]\Big) \cap \big[\mathcal{D}_4^{(4,n-1)}\ 1\big]\Big|\big[\mathbf{x}_4^{(n-1)}\ 1\big]\Big)\\
&\qquad- \Pr\Bigg(\Big(\big[\mathcal{D}_1^{(4,n-1)}\ 1\big] \cup \big[\mathcal{D}_2^{(4,n-1)}\ 1\big]\Big)\\
&\qquad\qquad\cap \Big(\big[\mathcal{D}_3^{(4,n-1)}\ 1\big] \cap \big[\mathcal{D}_4^{(4,n-1)}\ 1\big]\Big)\Bigg|\big[\mathbf{x}_{\ell,\ell\in\{3,4\}}^{(n-1)}\ 1\big]\Bigg) \quad (152)\\
&\quad= \Bigg(\Pr\Big(\overline{\mathcal{D}}_1^{(4,n-1)} \cap \overline{\mathcal{D}}_3^{(4,n-1)}\Big|\mathbf{x}_3^{(n-1)}\Big)\\
&\qquad+ \Pr\Big(\overline{\mathcal{D}}_2^{(4,n-1)} \cap \overline{\mathcal{D}}_3^{(4,n-1)}\Big|\mathbf{x}_3^{(n-1)}\Big)\\
&\qquad- \Pr\Big(\overline{\mathcal{D}}_1^{(4,n-1)} \cap \overline{\mathcal{D}}_2^{(4,n-1)} \cap \overline{\mathcal{D}}_3^{(4,n-1)}\Big|\mathbf{x}_3^{(n-1)}\Big)\\
&\qquad+ \Pr\Big(\overline{\mathcal{D}}_1^{(4,n-1)} \cap \overline{\mathcal{D}}_4^{(4,n-1)}\Big|\mathbf{x}_4^{(n-1)}\Big)\\
&\qquad+ \Pr\Big(\overline{\mathcal{D}}_2^{(4,n-1)} \cap \overline{\mathcal{D}}_4^{(4,n-1)}\Big|\mathbf{x}_4^{(n-1)}\Big)\\
&\qquad- \Pr\Big(\overline{\mathcal{D}}_1^{(4,n-1)} \cap \overline{\mathcal{D}}_2^{(4,n-1)} \cap \overline{\mathcal{D}}_4^{(4,n-1)}\Big|\mathbf{x}_4^{(n-1)}\Big)\\
&\qquad- \Pr\Big(\overline{\mathcal{D}}_1^{(4,n-1)} \cap \overline{\mathcal{D}}_3^{(4,n-1)} \cap \overline{\mathcal{D}}_4^{(4,n-1)}\Big|\mathbf{x}_{\ell,\ell\in\{3,4\}}^{(n-1)}\Big)\\
&\qquad- \Pr\Big(\overline{\mathcal{D}}_2^{(4,n-1)} \cap \overline{\mathcal{D}}_3^{(4,n-1)} \cap \overline{\mathcal{D}}_4^{(4,n-1)}\Big|\mathbf{x}_{\ell,\ell\in\{3,4\}}^{(n-1)}\Big)\\
&\qquad+ \Pr\Big(\overline{\mathcal{D}}_1^{(4,n-1)} \cap \overline{\mathcal{D}}_2^{(4,n-1)} \cap \overline{\mathcal{D}}_3^{(4,n-1)} \cap \overline{\mathcal{D}}_4^{(4,n-1)}\Big|\mathbf{x}_{\ell,\ell\in\{3,4\}}^{(n-1)}\Big)\Bigg)(1-\delta) \quad (153)\\
&\quad= \big(\delta^{n-1-t_5^\diamond} + \delta^{n-1-t_6^\diamond} - \delta^{n-1} + \delta^{n-1-t_6^\diamond} + \delta^{n-1-t_5^\diamond} - \delta^{n-1}\\
&\qquad- \delta^{n-1} - \delta^{n-1} + \delta^{n-1}\big)(1-\delta) \quad (154)\\
&\quad= \big(\delta^{2k-1} + \delta^{2k} + \delta^{2k} + \delta^{2k-1} - 3\delta^{n-1}\big)(1-\delta), \quad (155)
\end{aligned}$$

where (152) holds because $\big(\big[\mathcal{D}_1^{(4,n-1)}\ 1\big] \cup \big[\mathcal{D}_2^{(4,n-1)}\ 1\big]\big) \cap \big[\mathcal{D}_3^{(4,n-1)}\ 1\big]$ and $\big(\big[\mathcal{D}_1^{(4,n-1)}\ 1\big] \cup \big[\mathcal{D}_2^{(4,n-1)}\ 1\big]\big) \cap \big[\mathcal{D}_4^{(4,n-1)}\ 1\big]$ are not necessary disjoint, and where we apply the inclusion–exclusion principle in (153); (154) again follows from the r-wise Hamming distances perspective.

Appending $\mathbf{c}_4^{(4)}$: We have a total probability increase

$$\begin{aligned}
&\Delta\Psi\Big(\mathscr{C}_{\mathbf{t}_4}^{(4,n)}\Big) \\
&= \big(\delta^{n-1-t_3^\diamond} + \delta^{n-1-t_6^\diamond} + \delta^{n-1-t_5^\diamond} - \delta^{n-1} - \delta^{n-1} - \delta^{n-1} + \delta^{n-1}\big)(1-\delta) \quad (156)\\
&= \big(\delta^{2k-1} + \delta^{2k} + \delta^{2k-1} - 2\delta^{n-1}\big)(1-\delta). \quad (157)
\end{aligned}$$

Appending $\mathbf{c}_5^{(4)}$: Using an argumentation similar to the case of appending $\mathbf{c}_3^{(4)}$, we have a total probability increase

$$\begin{aligned}
\Delta\Psi\Big(\mathscr{C}_{\mathbf{t}_5}^{(4,n)}\Big) &= \big(\delta^{n-1-t_3^\diamond} + \delta^{n-1-t_6^\diamond} - \delta^{n-1} + \delta^{n-1-t_6^\diamond} + \delta^{n-1-t_3^\diamond} - \delta^{n-1} \\
&\qquad - \delta^{n-1} - \delta^{n-1} + \delta^{n-1}\big)(1-\delta) \quad (158)\\
&= \big(\delta^{2k-1} + \delta^{2k} + \delta^{2k} + \delta^{2k-1} - 3\delta^{n-1}\big)(1-\delta). \quad (159)
\end{aligned}$$

Appending $\mathbf{c}_6^{(4)}$: We have a total probability increase

$$\begin{aligned}
\Delta\Psi\Big(\mathscr{C}_{\mathbf{t}_6}^{(4,n)}\Big) &= \big(\delta^{n-1-t_3^\diamond} + \delta^{n-1-t_5^\diamond} - \delta^{n-1} + \delta^{n-1-t_3^\diamond} + \delta^{n-1-t_5^\diamond} - \delta^{n-1} \\
&\qquad - \delta^{n-1} - \delta^{n-1} + \delta^{n-1}\big)(1-\delta) \quad (160)\\
&= \big(\delta^{2k-1} + \delta^{2k-1} + \delta^{2k-1} + \delta^{2k-1} - 3\delta^{n-1}\big)(1-\delta). \quad (161)
\end{aligned}$$

Appending $\mathbf{c}_7^{(4)}$: We have a total probability increase

$$\begin{aligned}
&\Delta\Psi\Big(\mathscr{C}_{\mathbf{t}_7}^{(4,n)}\Big) \\
&= \big(\delta^{n-1-t_3^\diamond} + \delta^{n-1-t_5^\diamond} + \delta^{n-1-t_6^\diamond} - \delta^{n-1} - \delta^{n-1} - \delta^{n-1} + \delta^{n-1}\big)(1-\delta) \quad (162)\\
&= \big(\delta^{2k-1} + \delta^{2k-1} + \delta^{2k} - 2\delta^{n-1}\big)(1-\delta). \quad (163)
\end{aligned}$$

Using the fact that δ^d is strictly decreasing in d for $0 < \delta < 1$, we can conclude that

$$\operatorname*{argmax}_{1\le j\le 7} \Delta\Psi\Big(\mathscr{C}_{\mathbf{t}_j}^{(4,n)}\Big) = 6. \quad (164)$$

This completes the proof. The proofs for $n \bmod 3 = 1$ or 2 are similar.

B Appendix: Proof of Theorem 53

The proof of Theorem 53 is based on the exact average success probability for a BEC as a function of the code parameters $\mathbf{t}$ for a blocklength $n = \sum_{j=1}^{\mathrm{J}} t_j$. This problem is then transformed into a discrete multivariate constrained optimization problem.

We define the constrained region of all possible code parameters $\mathbf{t}$ as

$$\mathcal{T}^{(\mathrm{M})} \triangleq \left\{ \mathbf{t} \in \mathbb{N}_0^{\mathrm{J}} \colon \sum_{j=1}^{\mathrm{J}} t_j = n \right\}, \quad (165)$$

where $\mathbb{N}_0$ is the set of all nonnegative integers. Our goal is to find the globally optimized code parameters $\mathbf{t}^*$ that satisfy

$$\mathbf{t}^* = \operatorname*{argmin}_{\mathbf{t}\in\mathcal{T}^{(\mathrm{M})}} P_{\mathrm{e}}\Big(\mathscr{C}_{\mathbf{t}}^{(\mathrm{M},n)}\Big). \quad (166)$$

Applying Theorem 49 for $\mathsf{M}=3$ or $\mathsf{M}=4$, we have

$$3P_{\mathrm{e}}\left(\mathscr{C}_{\mathbf{t}}^{(3,n)}\right) = \delta^{n-t_1}+\delta^{n-t_2}+\delta^{n-t_3}-\delta^{n}; \tag{167}$$

$$\begin{aligned}4P_{\mathrm{e}}\left(\mathscr{C}_{\mathbf{t}}^{(4,n)}\right) &= \delta^{n-(t_1+t_2+t_3)}+\delta^{n-(t_1+t_4+t_5)}+\delta^{n-(t_1+t_6+t_7)}\\ &\quad+\delta^{n-(t_2+t_4+t_6)}+\delta^{n-(t_2+t_5+t_7)}+\delta^{n-(t_3+t_4+t_7)}\\ &\quad-\delta^{n-t_1}-\delta^{n-t_2}-\delta^{n-t_4}-\delta^{n-t_7}+\delta^{n}.\end{aligned} \tag{168}$$

Since we consider the optimization problem for any fixed blocklength n and hence δ^n is a constant, we can reformulate the discrete multivariate constrained minimization problem as follows:

$$\begin{aligned}&\text{minimize } f^{(\mathsf{M})}(\mathbf{t}) \triangleq \frac{\mathsf{M}\,P_{\mathrm{e}}\left(\mathscr{C}_{\mathbf{t}}^{(\mathsf{M},n)}\right)}{\delta^n}+(-1)^{\mathsf{M}+1}\\ &\text{subject to} \qquad \mathbf{t}\in\mathcal{T}^{(\mathsf{M})}\end{aligned} \tag{169}$$

where the minimization objective functions for $\mathsf{M}=3$ or $\mathsf{M}=4$ are

$$f^{(3)}(\mathbf{t}) = \delta^{-t_1}+\delta^{-t_2}+\delta^{-t_3} \tag{170}$$

and

$$\begin{aligned}f^{(4)}(\mathbf{t}) &= \delta^{-t_1-t_2-t_3}+\delta^{-t_1-t_4-t_5}+\delta^{-t_1-t_6-t_7}+\delta^{-t_2-t_4-t_6}+\delta^{-t_2-t_5-t_7}\\ &\quad+\delta^{-t_3-t_4-t_7}-\delta^{-t_1}-\delta^{-t_2}-\delta^{-t_4}-\delta^{-t_7},\end{aligned} \tag{171}$$

respectively. Next, we define

$$u_j \triangleq \delta^{-t_j}, \quad \forall\, 1\le j\le \mathsf{J}. \tag{172}$$

Note that $1\le u_j\le \delta^{-n}$ for $0<\delta<1$. We apply this definition to (170), (171) and define further

$$g^{(\mathsf{M})}(\mathbf{u}) \triangleq f^{(\mathsf{M})}(\mathbf{t}). \tag{173}$$

The corresponding constrained region (165) then reads

$$\mathcal{U}^{(\mathsf{M})} \triangleq \left\{\mathbf{u}\in\mathbb{R}^{\mathsf{J}}\colon u_j\ge 1 \text{ and } \prod_{j=1}^{\mathsf{J}} u_j = \delta^{-n}\right\}. \tag{174}$$

Note that $\mathcal{T}^{(\mathsf{M})}$ is a convex set, but $\mathcal{U}^{(\mathsf{M})}$ is not.

We firstly consider the easier case of $\mathsf{M}=3$. Taking the locally optimal code parameters $\mathbf{t}^{\diamond}$ from Theorem 52, we will now prove that they are actually globally optimal for (170). Using $t_3=n-t_1-t_2$, we have

$$f^{(3)}(\mathbf{t}) = \delta^{-t_1}+\delta^{-t_2}+\delta^{t_1+t_2-n} \tag{175}$$

$$\ge 2\sqrt{\delta^{-t_1}\delta^{-t_2}}+\delta^{t_1+t_2-n} \tag{176}$$

$$\triangleq 2\delta^{-t}+\delta^{2t-n} \tag{177}$$

$$\triangleq h(t), \tag{178}$$

where (176) holds because the arithmetic mean (AM) is never smaller than the geometric mean (GM), and in (177) we define $t\triangleq(t_1+t_2)/2$. It can be seen that

the function $2\delta^{-t}+\delta^{n-2t}$ is convex in t. Hence, its global minimum $3\delta^{-n/3}$ is given for the t satisfying

$$\frac{\partial}{\partial t}\left(2\delta^{-t}+\delta^{2t-n}\right)\stackrel{!}{=}0, \tag{179}$$

i.e., the global minimizer of $h(t)$ is $t^*=\frac{n}{3}$. However, one must be aware that the minimizer of $f^{(3)}(\mathbf{t})$ must be a positive integer. So, if $n=3k$, taking $t_1^*=t_2^*=t_3^*=t^*$ trivially achieves the global minimum of $h(t)$, i.e., $3\delta^{-n/3}$. In the following we will investigate the discrete minimizer t^* for $h(t)$ for the case of $n=3k+1$. The case $n=3k+2$ is similar and omitted.

Since the function $h(t)$ is convex, the minimizer should be equal to k or $k+1$. Therefore,

$$\begin{aligned}\min\{h(k),h(k+1)\}&=\min\left\{2\delta^{-k}+\delta^{-(k+1)},2\delta^{-(k+1)}+\delta^{-(k-1)}\right\} &(180)\\ &=2\delta^{-k}+\delta^{-(k+1)} &(181)\\ &=h(k). &(182)\end{aligned}$$

Here we again use the AM–GM inequality to show that $2\delta^{-k}<\delta^{-(k+1)}+\delta^{-(k-1)}$. Thus the discrete global minimizer for $h(t)$ is $t^*=k$. Finally, since the inequality of (176) is achievable by $[t_1,t_2,t_3]=[k,k,k+1]$, we can conclude that a discrete global minimizer for $f^{(3)}(\mathbf{t})$ is $\mathbf{t}^*=[k,k,k+1]$.

Note that in Theorem 53, we only re-order the code parameters to be $\mathbf{t}^*=[k+1,k,k]$, i.e., it is not difficult to see that the performances of these two codes are equivalent; so the optimal codes are not unique when $n=3k+1$.

In the case of $\mathsf{M}=4$—again trying to prove that the locally optimal code parameters from Theorem 52 are also globally optimal—we must first prove that the globally optimal code parameters $\mathbf{t}^*$ must satisfy $t_1^*=t_2^*=t_4^*=t_7^*=0$ with arbitrary blocklength n. This turns out to be quite technical.

Let us consider the transformed function $g^{(4)}(\mathbf{u})$ on the constrained set $\mathcal{U}^{(4)}$:

$$\begin{aligned}g^{(4)}(\mathbf{u})&=u_1u_2u_3+u_1u_4u_5+u_1u_6u_7+u_2u_4u_6+u_2u_5u_7+u_3u_4u_7\\&\quad-(u_1+u_2+u_4+u_7) &(183)\\&=u_1(u_2u_3+u_4u_5+u_6u_7-1)+u_2u_4u_6+u_2u_5u_7+u_3u_4u_7\\&\quad-(u_2+u_4+u_7) &(184)\\&\geq u_1\Big(3(u_2u_3u_4u_5u_6u_7)^{\frac{1}{3}}-1\Big)+u_2u_4u_6+u_2u_5u_7+u_3u_4u_7\\&\quad-(u_2+u_4+u_7) &(185)\\&=u_1\left(3\left(\frac{\delta^{-n}}{u_1}\right)^{\frac{1}{3}}-1\right)+u_2u_4u_6+u_2u_5u_7+u_3u_4u_7-(u_2+u_4+u_7) &(186)\\&=\left(3\delta^{-\frac{n}{3}}u_1^{\frac{2}{3}}-u_1\right)+u_2u_4u_6+u_2u_5u_7+u_3u_4u_7-(u_2+u_4+u_7). &(187)\end{aligned}$$

Here, (185) follows from the AM–GM inequality, where equality holds if

$$u_2u_3=u_4u_5=u_6u_7. \tag{188}$$

In (186), we use the fact that $\prod_{j=1}^7 u_j=\delta^{-n}$. The first term on the RHS of (187) is concave, nondecreasing in u_1 for $1\leq u_1\leq\delta^{-n}$, and independent of the other variables $u_2,\ldots,u_7$. This implies that if we want to minimizes (187), we should have $u_1^*=1$ and the minimization is irrelevant to $u_2^*,\ldots,u_7^*$. To achieve equality

in (185), we only need to satisfy the condition (188), which means that $u_1^* = 1$ is both the discrete global minimizer of the RHS of (187) and $g^{(4)}(\mathbf{u})$. Using the same argument, we can also show that the discrete global optimizer $\mathbf{u}^*$ must satisfy that $u_1^* = u_2^* = u_4^* = u_7^* = 1$, i.e., $t_1^* = t_2^* = t_4^* = t_7^* = 0$.

So the discrete multivariate constrained optimization problem is reduced to

$$\min_{\mathbf{t}_{\text{weak}} \in \mathcal{T}^{(4)}} f^{(4)}(\mathbf{t}_{\text{weak}}) = \min_{\mathbf{t}_{\text{weak}} \in \mathcal{T}^{(4)}} \big(2\delta^{-t_3} + 2\delta^{-t_5} + 2\delta^{-t_6} - 4\big), \tag{189}$$

where

$$\mathcal{T}^{(4)} \triangleq \left\{ \mathbf{t}_{\text{weak}} \in \mathbb{N}_0^{\text{L}} \colon t_j \geq 0,\ j \in \{3,5,6\},\ \text{and} \sum_{j \in \{3,5,6\}} t_j = n \right\}. \tag{190}$$

This problem can be solved in an analogous way as for $\mathsf{M} = 3$. We obtain

$$\mathbf{t}^* = \mathbf{t}_{\text{weak}}^* = \big[t_3^*, t_5^*, t_6^*\big] = \left[\left\lfloor \frac{n+2}{3} \right\rfloor, \left\lfloor \frac{n+1}{3} \right\rfloor, \left\lfloor \frac{n}{3} \right\rfloor \right]. \tag{191}$$

C Appendix: Proof of Theorem 55

We first consider the case of $\mathsf{M} = 5$. Based on (169) and (173), we have

$$\begin{aligned} g^{(5)}(\mathbf{u}) = {} & \big(u_1u_2u_3u_4u_5u_6u_7 + u_1u_2u_3u_8u_9u_{10}u_{11} + u_1u_4u_5u_8u_9u_{12}u_{13} \\ & + u_2u_4u_6u_8u_{10}u_{12}u_{14} + u_1u_2u_3u_{12}u_{13}u_{14}u_{15} + u_1u_4u_5u_{10}u_{11}u_{14}u_{15} \\ & + u_2u_4u_6u_9u_{11}u_{13}u_{15} + u_1u_6u_7u_8u_9u_{14}u_{15} + u_2u_5u_7u_8u_{10}u_{13}u_{15} \\ & + u_3u_4u_7u_8u_{11}u_{12}u_{15}\big) \\ & - \big(u_1u_2u_3 + u_1u_4u_5 + u_2u_4u_6 + u_1u_8u_9 + u_2u_8u_{10} + u_4u_8u_{12} \\ & \quad + u_1u_{14}u_{15} + u_2u_{13}u_{15} + u_4u_{11}u_{15} + u_7u_8u_{15}\big) \\ & + \big(u_1 + u_2 + u_4 + u_8 + u_{15}\big). \end{aligned} \tag{192}$$

Recall that in the double summation in (103), we denote by $\sum_{\mathcal{I} \subseteq \{1,\ldots,\mathsf{M}\}, |\mathcal{I}|=r} \delta^{d_{\mathcal{I}}^{(\mathsf{M},n)}}$ the *r-wise series* of a specific parameter vector $\mathbf{t}$. Observe that in (192), each nonweak flip variable (i.e., u_1, u_2, u_4, u_8, and u_{15}) shows up six times in the 2-wise series (terms in the first bracket), four times in the 3-wise series (terms in the second bracket), and only once in the 4-wise series (terms in the last bracket). Note that each term in the 2-wise series contains $\binom{5-2}{2} + \binom{5-2}{3} = 4$ weak flip variables and $\binom{5-2}{1} = 3$ nonweak flip variables, each term in the 3-wise series contains $\binom{5-3}{2} = 1$ weak flip variables and $\binom{5-3}{1} = 2$ nonweak flip variables, and each term in the 4-wise series contains only $\binom{5-4}{1} = 1$ nonweak flip variable.

Now we pick the first nonweak variable u_1 and rewrite $g^{(5)}(\mathbf{u})$ as follows:

$$\begin{aligned} g^{(5)}(\mathbf{u}) = {} & u_1\Big(u_2u_3u_4u_5u_6u_7 + u_2u_3u_8u_9u_{10}u_{11} + u_4u_5u_8u_9u_{12}u_{13} \\ & \quad + u_2u_3u_{12}u_{13}u_{14}u_{15} + u_4u_5u_{10}u_{11}u_{14}u_{15} + u_6u_7u_8u_9u_{14}u_{15} \\ & \quad - \big(u_2u_3 + u_4u_5 + u_8u_9 + u_{14}u_{15}\big) + 1\Big) \\ & + u_2u_4u_6u_8u_{10}u_{12}u_{14} + u_2u_4u_6u_9u_{11}u_{13}u_{15} + u_2u_5u_7u_8u_{10}u_{13}u_{15} \\ & + u_3u_4u_7u_8u_{11}u_{12}u_{15} \\ & - \big(u_2u_4u_6 + u_2u_8u_{10} + u_4u_8u_{12} + u_2u_{13}u_{15} + u_4u_{11}u_{15} + u_7u_8u_{15}\big) \\ & + \big(u_2 + u_4 + u_8 + u_{15}\big) \end{aligned} \tag{193}$$

$$
\begin{aligned}
&\geq u_2u_3u_4u_5u_6u_7 + u_2u_3u_8u_9u_{10}u_{11} + u_4u_5u_8u_9u_{12}u_{13} \\
&\quad + u_2u_3u_{12}u_{13}u_{14}u_{15} + u_4u_5u_{10}u_{11}u_{14}u_{15} + u_6u_7u_8u_9u_{14}u_{15} \\
&\quad - \big(u_2u_3 + u_4u_5 + u_8u_9 + u_{14}u_{15}\big) + 1 \\
&\quad + u_2u_4u_6u_8u_{10}u_{12}u_{14} + u_2u_4u_6u_9u_{11}u_{13}u_{15} + u_2u_5u_7u_8u_{10}u_{13}u_{15} \\
&\quad + u_3u_4u_7u_8u_{11}u_{12}u_{15} \\
&\quad - \big(u_2u_4u_6 + u_2u_8u_{10} + u_4u_8u_{12} + u_2u_{13}u_{15} + u_4u_{11}u_{15} + u_7u_8u_{15}\big) \\
&\quad + \big(u_2 + u_4 + u_8 + u_{15}\big) && (194) \\
&= g^{(5)}\big(\mathbf{u}_{\mathcal{J}\setminus\{1\}}\big), && (195)
\end{aligned}
$$

where in the slightly sloppy notation of $g^{(5)}\big(\mathbf{u}_{\mathcal{J}\setminus\tilde{\mathcal{J}}}\big)$, we assume that all missing arguments $\mathbf{u}_{\tilde{\mathcal{J}}}$ of $g^{(5)}(\cdot)$ are implicitly set to 1, i.e., $u_j = 1$ for all $j \in \tilde{\mathcal{J}}$. In addition, the inequality (194) holds because $u_1 = \delta^{-t_1} \geq 1$ and because the expression inside the first bracket of (193) can be shown to be nonnegative:

$$
\begin{aligned}
&u_2u_3u_4u_5u_6u_7 + u_2u_3u_8u_9u_{10}u_{11} + u_4u_5u_8u_9u_{12}u_{13} \\
&+ u_2u_3u_{12}u_{13}u_{14}u_{15} + u_4u_5u_{10}u_{11}u_{14}u_{15} + u_6u_7u_8u_9u_{14}u_{15} \\
&- \big(u_2u_3 + u_4u_5 + u_8u_9 + u_{14}u_{15}\big) + 1 \\
&\quad = w_1w_2w_3 + w_1w_4w_5 + w_2w_4w_6 + w_1w_6w_7 + w_2w_5w_7 + w_3w_4w_7 \\
&\qquad - (w_1 + w_2 + w_4 + w_7) + 1 && (196) \\
&\quad = w_1(w_2w_3 - 1) + w_2(w_4w_6 - 1) + w_4(w_3w_7 - 1) + w_7(w_1w_6 - 1) \\
&\qquad + w_1w_4w_5 + w_2w_5w_7 + 1 && (197) \\
&\quad \geq 0, && (198)
\end{aligned}
$$

where we have defined for simplicity

$$
\begin{aligned}
&w_1 \triangleq u_2u_3 \qquad w_2 \triangleq u_4u_5 \qquad w_3 \triangleq u_6u_7 \qquad w_4 \triangleq u_8u_9 \\
&w_5 \triangleq u_{10}u_{11} \qquad w_6 \triangleq u_{12}u_{13} \qquad w_7 \triangleq u_{14}u_{15}
\end{aligned} \tag{199}
$$

and where we note that $w_i \geq 1$, $i = 1, \ldots, 7$. Note that (196) is actually identical to $g^{(4)}(\mathbf{w}) + (-1)^4$ as defined in (183) and therefore it must be nonnegative by definition.

It is then not difficult to see that for an appropriate definition of $\mathbf{w}$ as in (199), we could factorize $g^{(5)}(\mathbf{u})$ as

$$
g^{(5)}(\mathbf{u}) = u_j \cdot \big(g^{(4)}(\mathbf{w}) + (-1)^4\big) + \text{remaining terms consisting only of } \mathbf{u}_{\mathcal{J}\setminus\{j\}} \tag{200}
$$

for $j = 1, 2, 4, 8, 15$.

We continue with $g^{(5)}\big(\mathbf{u}_{\mathcal{J}\setminus\{1\}}\big)$ in a similar fashion as in (193)–(199) by factoring out u_2:

$$
\begin{aligned}
g^{(5)}(\mathbf{u}_{\mathcal{J}\setminus\{1\}}) = u_2\Big(&u_3u_4u_5u_6u_7 + u_3u_8u_9u_{10}u_{11} + u_4u_6u_8u_{10}u_{12}u_{14} \\
&+ u_3u_{12}u_{13}u_{14}u_{15} + u_4u_6u_9u_{11}u_{13}u_{15} + u_5u_7u_8u_{10}u_{13}u_{15} \\
&- \big(u_3 + u_4u_6 + u_8u_{10} + u_{13}u_{15}\big) + 1\Big) \\
&+ u_4u_5u_8u_9u_{12}u_{13} + u_4u_5u_{10}u_{11}u_{14}u_{15} + u_6u_7u_8u_9u_{14}u_{15} \\
&+ u_3u_4u_7u_8u_{11}u_{12}u_{15} \\
&- \big(u_4u_5 + u_8u_9 + u_{14}u_{15} + u_4u_8u_{12} + u_4u_{11}u_{15} + u_7u_8u_{15}\big) \\
&+ 1 + (u_4 + u_8 + u_{15})
\end{aligned} \tag{201}
$$

$$
\begin{aligned}
&\geq u_3u_4u_5u_6u_7 + u_3u_8u_9u_{10}u_{11} + u_4u_6u_8u_{10}u_{12}u_{14} \\
&\quad + u_3u_{12}u_{13}u_{14}u_{15} + u_4u_6u_9u_{11}u_{13}u_{15} + u_5u_7u_8u_{10}u_{13}u_{15} \\
&\quad - \big(u_3 + u_4u_6 + u_8u_{10} + u_{13}u_{15}\big) + 1 \\
&\quad + u_4u_5u_8u_9u_{12}u_{13} + u_4u_5u_{10}u_{11}u_{14}u_{15} + u_6u_7u_8u_9u_{14}u_{15} \\
&\quad + u_3u_4u_7u_8u_{11}u_{12}u_{15} \\
&\quad - \big(u_4u_5 + u_8u_9 + u_{14}u_{15} + u_4u_8u_{12} + u_4u_{11}u_{15} + u_7u_8u_{15}\big) \\
&\quad + 1 + (u_4 + u_8 + u_{15}) && (202) \\
&= g^{(5)}\big(\mathbf{u}_{\mathcal{J}\setminus\{1,2\}}\big). && (203)
\end{aligned}
$$

Again, the inequality (202) holds because $u_2 \geq 1$ and because the first bracket of (201) is nonnegative:

$$
\begin{aligned}
&u_3u_4u_5u_6u_7 + u_3u_8u_9u_{10}u_{11} + u_4u_6u_8u_{10}u_{12}u_{14} \\
&+ u_3u_{12}u_{13}u_{14}u_{15} + u_4u_6u_9u_{11}u_{13}u_{15} + u_5u_7u_8u_{10}u_{13}u_{15} \\
&- \big(u_3 + u_4u_6 + u_8u_{10} + u_{13}u_{15}\big) + 1 \\
&\quad = w_1w_2w_3 + w_1w_4w_5 + w_2w_4w_6 + w_1w_6w_7 + w_2w_5w_7 + w_3w_4w_7 \\
&\qquad - (w_1 + w_2 + w_4 + w_7) + 1 && (204) \\
&\quad \geq 0. && (205)
\end{aligned}
$$

Note that $w_1 = u_3$ now because we have set $u_1 = 1$ in the previous step.

We continue in this fashion for the remaining nonweak flip variables and find the following sequence of inequalities:

$$
\begin{aligned}
g^{(5)}(\mathbf{u}) &\geq g^{(5)}\big(\mathbf{u}_{\mathcal{J}\setminus\{1\}}\big) && (206) \\
&\geq g^{(5)}\big(\mathbf{u}_{\mathcal{J}\setminus\{1,2\}}\big) && (207) \\
&\geq g^{(5)}\big(\mathbf{u}_{\mathcal{J}\setminus\{1,2,4\}}\big) && (208) \\
&\geq g^{(5)}\big(\mathbf{u}_{\mathcal{J}\setminus\{1,2,4,8\}}\big) && (209) \\
&\geq g^{(5)}\big(\mathbf{u}_{\mathcal{J}\setminus\{1,2,4,8,15\}}\big) && (210) \\
&= u_3u_5u_6u_7 + u_3u_9u_{10}u_{11} + u_3u_{12}u_{13}u_{14} + u_3u_7u_{11}u_{12} + u_5u_9u_{12}u_{13} \\
&\quad + u_5u_{10}u_{11}u_{14} + u_5u_7u_{10}u_{13} + u_6u_9u_{11}u_{13} + u_6u_{10}u_{12}u_{14} + u_6u_7u_9u_{14} \\
&\quad - \big(u_3 + u_5 + u_6 + u_7 + u_9 + u_{10} + u_{11} + u_{12} + u_{13} + u_{14}\big) + 5 && (211) \\
&\triangleq g^{(5)}_{\text{weak}}(\mathbf{u}_{\text{weak}}) + 5, && (212)
\end{aligned}
$$

where the inequalities hold with equality if, and only if, $u_1 = u_2 = u_4 = u_8 = u_{15} = 1$.

Next, we investigate the ten terms of the 2-wise series in (211):

$$
\begin{aligned}
&u_3u_5u_6u_7 + u_3u_9u_{10}u_{11} + u_3u_{12}u_{13}u_{14} + u_3u_7u_{11}u_{12} \\
&+ u_5u_9u_{12}u_{13} + u_5u_{10}u_{11}u_{14} + u_5u_7u_{10}u_{13} \\
&+ u_6u_9u_{11}u_{13} + u_6u_{10}u_{12}u_{14} + u_6u_7u_9u_{14} \\
&\quad \geq 10\big(u_3^4u_5^4u_6^4u_7^4u_9^4u_{10}^4u_{11}^4u_{12}^4u_{13}^4u_{14}^4\big)^{\frac{1}{10}} && (213) \\
&\quad = 10\big(\delta^{-4n}\big)^{\frac{1}{10}} && (214) \\
&\quad = 10\delta^{-\frac{2}{5}n}, && (215)
\end{aligned}
$$

where (215) holds because $\prod_{j=1}^{\mathrm{J}} u_j = \delta^{-n}$ and because $u_1 = u_2 = u_4 = u_8 = u_{15} = 1$.

Note that the inequality (213) holds with equality if, and only if,

$$\begin{aligned} u_3u_5u_6u_7 = u_3u_9u_{10}u_{11} = u_3u_{12}u_{13}u_{14} = u_3u_7u_{11}u_{12} \\ = u_5u_9u_{12}u_{13} = u_5u_{10}u_{11}u_{14} = u_5u_7u_{10}u_{13} \\ = u_6u_9u_{11}u_{13} = u_6u_{10}u_{12}u_{14} = u_6u_7u_9u_{14}. \end{aligned} \tag{216}$$

From these equalities, we could pick, for example, the following

$$u_3u_5u_6u_7 = u_3u_7u_{11}u_{12} \tag{217}$$

$$u_5u_9u_{12}u_{13} = u_6u_9u_{11}u_{13} \tag{218}$$

and note that since $u_j \geq 1$, $\forall\, j \in \mathcal{J}$, we have

$$u_5u_6 = u_{11}u_{12}, \tag{219}$$

$$u_5u_{12} = u_6u_{11} \tag{220}$$

and hence

$$\frac{u_5}{u_{11}} = \frac{u_{12}}{u_6} = \frac{u_{11}}{u_5}. \tag{221}$$

This implies that $u_5^2 = u_{11}^2$, i.e., $u_5 = u_{11}$ and $u_6 = u_{12}$. In a similar fashion, it can then be seen that the unique solution to (216) subject to the constraints $\prod_{j=1}^{\mathsf{J}} u_j = \delta^{-10\kappa}$ and $u_1 = u_2 = u_4 = u_8 = u_{15} = 1$ is

$$u_3 = u_5 = u_6 = u_7 = u_9 = u_{10} = u_{11} = u_{12} = u_{13} = u_{14} = \delta^{-\kappa}. \tag{222}$$

Thus, we have derived the following lower bound:

$$g^{(5)}(\mathbf{u}) \geq 10\delta^{-\frac{2}{5}n} - \big(u_3 + u_5 + u_6 + u_7 + u_9 + u_{10} + u_{11} + u_{12} + u_{13} + u_{14}\big) + 5 \tag{223}$$

with equality if $u_1 = u_2 = u_4 = u_8 = u_{15} = 1$ and (222) is satisfied. Subject to $u_3u_5u_6u_7u_9u_{10}u_{11}u_{12}u_{13}u_{14} =$ constant, this lower bound is minimized if all u_j take on the same value.

In conclusion, (222) in combination with $u_1 = u_2 = u_4 = u_8 = u_{15} = 1$ is the global minimizer of $g^{(5)}(\mathbf{u})$, i.e., the fair weak flip code parameters

$$t_3^* = t_5^* = t_6^* = t_7^* = t_9^* = t_{10}^* = t_{11}^* = t_{12}^* = t_{13}^* = t_{14}^* = \kappa. \tag{224}$$

and $t_1^* = t_2^* = t_4^* = t_8^* = t_{15}^* = 0$ are globally optimal.

The proof in the case of $\mathsf{M} = 6$ can be derived in an analogous way, although one needs more steps in the lower-bounding. We observe that each term in the 2-wise series contains $\binom{6-2}{3} = 4$ weak flip variables, $\binom{6-2}{1} = 4$ nonweak flip variables corresponding to the columns with Hamming weight equal to 1 or 5, and $\binom{6-2}{2} + \binom{6-2}{4} = 7$ nonweak flip variables corresponding to the columns with Hamming weight equal to 2 or 4; each term in the 3-wise series contains $\binom{6-3}{3} = 1$ weak flip variables, $\binom{6-3}{1} = 3$ nonweak flip variables corresponding to the columns with Hamming weight equal to 1 or 5, and $\binom{6-3}{2} = 3$ nonweak flip variables corresponding to the columns with Hamming weight equal to 2 or 4; each term in the 4-wise series contains $\binom{6-4}{1} = 2$ nonweak flip variables corresponding to the columns with Hamming weight equal to 1 or 5, and $\binom{6-4}{2} = 1$ nonweak flip variables corresponding to the columns with

Hamming weight equal to 2 or 4; and each term in the 5-wise series contains $\binom{6-5}{1} = 1$ nonweak flip variables corresponding to the columns with Hamming weight equal to 1 or 5.

First we consider the nonweak flip variables corresponding to columns with Hamming weight equal to 1 or 5 and collect these $\binom{5}{1} + \binom{5}{5} = 6$ indices in

$$\mathcal{J}_1 \triangleq \{1, 2, 4, 8, 16, 31\}. \tag{225}$$

Using a completely analogous approach as in the case of $\mathsf{M} = 5$, we can show that

$$\begin{aligned} g^{(6)}(\mathbf{u}) &= u_j \cdot \big(g^{(5)}(\mathbf{w}) + (-1)^5\big) + \text{remaining terms consisting only of } \mathbf{u}_{\mathcal{J}\setminus\{j\}} && (226)\\ &\geq g^{(6)}\big(\mathbf{u}_{\mathcal{J}\setminus\{j\}}\big) && (227)\end{aligned}$$

for $j \in \mathcal{J}_1$. Accordingly, it can be shown that

$$g^{(6)}(\mathbf{u}) \geq g^{(6)}\big(\mathbf{u}_{\mathcal{J}\setminus\mathcal{J}_1}\big), \tag{228}$$

where (228) holds with equality if, and only if, $u_j = 1$, $\forall\, j \in \mathcal{J}_1$.

Secondly, we consider the other nonweak flip variables corresponding to columns with Hamming weight equal to 2 or 4 and collect the $\binom{5}{2} + \binom{5}{4} = 15$ indices in

$$\mathcal{J}_2 \triangleq \{3, 5, 6, 9, 10, 12, 15, 17, 18, 20, 23, 24, 27, 29, 30\}. \tag{229}$$

Keeping $u_j = 1$, $\forall\, j \in \mathcal{J}_1$, we obtain from Theorem 49,

$$\begin{aligned} &g^{(6)}(\mathbf{u})\\ &\quad\geq g^{(6)}\big(\mathbf{u}_{\mathcal{J}\setminus\mathcal{J}_1}\big) && (230)\\ &\quad= u_3u_5u_6u_7u_9u_{10}u_{11}u_{12}u_{13}u_{14}u_{15} + u_3u_5u_6u_7u_{17}u_{18}u_{19}u_{20}u_{21}u_{22}u_{23}\\ &\qquad+ u_3u_9u_{10}u_{11}u_{17}u_{18}u_{19}u_{24}u_{25}u_{26}u_{27} + u_3u_5u_6u_7u_{24}u_{25}u_{26}u_{27}u_{28}u_{29}u_{30}\\ &\qquad+ u_3u_9u_{10}u_{11}u_{20}u_{21}u_{22}u_{23}u_{28}u_{29}u_{30} + u_3u_{12}u_{13}u_{14}u_{15}u_{17}u_{18}u_{19}u_{28}u_{29}u_{30}\\ &\qquad+ u_3u_7u_{11}u_{12}u_{15}u_{19}u_{20}u_{23}u_{24}u_{27}u_{28} + u_5u_9u_{12}u_{13}u_{20}u_{17}u_{21}u_{24}u_{25}u_{28}u_{29}\\ &\qquad+ u_5u_9u_{12}u_{13}u_{18}u_{19}u_{22}u_{23}u_{26}u_{27}u_{30} + u_5u_{10}u_{11}u_{14}u_{15}u_{17}u_{20}u_{21}u_{26}u_{27}u_{30}\\ &\qquad+ u_5u_7u_{10}u_{13}u_{15}u_{18}u_{21}u_{23}u_{24}u_{26}u_{29} + u_6u_{10}u_{12}u_{14}u_{18}u_{20}u_{22}u_{24}u_{26}u_{28}u_{30}\\ &\qquad+ u_6u_{10}u_{12}u_{14}u_{17}u_{19}u_{21}u_{23}u_{25}u_{27}u_{29} + u_6u_9u_{11}u_{13}u_{15}u_{18}u_{20}u_{22}u_{25}u_{27}u_{29}\\ &\qquad+ u_6u_7u_9u_{14}u_{15}u_{17}u_{22}u_{23}u_{24}u_{25}u_{30}\\ &\qquad- \big(u_3u_5u_6u_7 + u_3u_9u_{10}u_{11} + u_3u_{17}u_{18}u_{19} + u_3u_{28}u_{29}u_{30} + u_5u_9u_{12}u_{13}\\ &\qquad\quad+ u_5u_{17}u_{20}u_{21} + u_5u_{26}u_{27}u_{30} + u_6u_{10}u_{12}u_{14} + u_6u_{18}u_{20}u_{22}\\ &\qquad\quad+ u_6u_{25}u_{27}u_{29} + u_9u_{17}u_{24}u_{25} + u_9u_{22}u_{23}u_{30} + u_{10}u_{18}u_{24}u_{26}\\ &\qquad\quad+ u_{10}u_{21}u_{23}u_{29} + u_{12}u_{20}u_{24}u_{28} + u_{12}u_{19}u_{23}u_{27} + u_7u_{15}u_{23}u_{24}\\ &\qquad\quad+ u_{11}u_{15}u_{20}u_{27} + u_{13}u_{15}u_{28}u_{29} + u_{14}u_{15}u_{17}u_{30}\big)\\ &\qquad+ \big(u_3 + u_5 + u_6 + u_9 + u_{10} + u_{12} + u_{15} + u_{17} + u_{18} + u_{20} + u_{23} + u_{24}\\ &\qquad\quad+ u_{27} + u_{29} + u_{30}\big) - 6. && (231)\end{aligned}$$

We again use a similar approach and factor out u_3 from $g^{(6)}\big(\mathbf{u}_{\mathcal{J}\setminus\mathcal{J}_1}\big)$:

$$\begin{aligned} &g^{(6)}\big(\mathbf{u}_{\mathcal{J}\setminus\mathcal{J}_1}\big)\\ &\quad= u_3 \cdot \Big(u_5u_6u_7u_9u_{10}u_{11}u_{12}u_{13}u_{14}u_{15} + u_5u_6u_7u_{17}u_{18}u_{19}u_{20}u_{21}u_{22}u_{23}\\ &\qquad+ u_9u_{10}u_{11}u_{17}u_{18}u_{19}u_{24}u_{25}u_{26}u_{27} + u_5u_6u_7u_{24}u_{25}u_{26}u_{27}u_{28}u_{29}u_{30}\end{aligned}$$

$$
\begin{aligned}
&\quad + u_9u_{10}u_{11}u_{20}u_{21}u_{22}u_{23}u_{28}u_{29}u_{30} + u_{12}u_{13}u_{14}u_{15}u_{17}u_{18}u_{19}u_{28}u_{29}u_{30} \\
&\quad - \big(u_5u_6u_7 + u_9u_{10}u_{11} + u_{17}u_{18}u_{19} + u_{28}u_{29}u_{30}\big) + 1 \\
&\quad + u_7u_{11}u_{12}u_{15}u_{19}u_{20}u_{23}u_{24}u_{27}u_{28}\Big) \\
&\quad + \text{remaining terms depending only on } \mathbf{u}_{\mathcal{J}\setminus(\mathcal{J}_1\cup\{3\})} && (232)\\
&\triangleq u_3\cdot\Big(g^{(4)}(\mathbf{w}) + (-1)^4 + u_7u_{11}u_{12}u_{15}u_{19}u_{20}u_{23}u_{24}u_{27}u_{28}\Big) \\
&\quad + \text{remaining terms depending only on } \mathbf{u}_{\mathcal{J}\setminus(\mathcal{J}_1\cup\{3\})} && (233)\\
&\geq g^{(4)}(\mathbf{w}) + (-1)^4 + u_7u_{11}u_{12}u_{15}u_{19}u_{20}u_{23}u_{24}u_{27}u_{28} \\
&\quad + \text{remaining terms depending only on } \mathbf{u}_{\mathcal{J}\setminus(\mathcal{J}_1\cup\{3\})}, && (234)
\end{aligned}
$$

where we have defined

$$
\begin{aligned}
&w_1 \triangleq u_5u_6u_7 && w_2 \triangleq u_9u_{10}u_{11} && w_3 \triangleq u_{12}u_{13}u_{14}u_{15} \\
&w_4 \triangleq u_{17}u_{18}u_{19} && w_5 \triangleq u_{20}u_{21}u_{22}u_{23} && w_6 \triangleq u_{24}u_{25}u_{26}u_{27} \\
&w_7 \triangleq u_{28}u_{29}u_{30}
\end{aligned} \qquad (235)
$$

and where (234) holds because $u_3 \geq 1$ and because the bracket in (233) is nonnegative.

We continue in the same fashion and show that

$$
\begin{aligned}
g^{(6)}(\mathbf{u}) &\geq g^{(6)}\big(\mathbf{u}_{\mathcal{J}\setminus\mathcal{J}_1}\big) && (236)\\
&\geq g^{(6)}\big(\mathbf{u}_{\mathcal{J}\setminus(\mathcal{J}_1\cup\mathcal{J}_2)}\big) && (237)\\
&= u_7u_{11}u_{13}u_{14} + u_7u_{19}u_{21}u_{22} + u_7u_{25}u_{26}u_{28} + u_7u_{14}u_{22}u_{25} \\
&\quad + u_7u_{13}u_{21}u_{26} + u_7u_{11}u_{19}u_{28} + u_{11}u_{19}u_{25}u_{26} + u_{11}u_{21}u_{22}u_{28} \\
&\quad + u_{11}u_{14}u_{21}u_{26} + u_{11}u_{13}u_{22}u_{25} + u_{13}u_{21}u_{25}u_{28} + u_{13}u_{19}u_{22}u_{26} \\
&\quad + u_{13}u_{14}u_{19}u_{28} + u_{14}u_{22}u_{26}u_{28} + u_{14}u_{19}u_{21}u_{25} \\
&\quad - \big(2u_7 + 2u_{11} + 2u_{13} + 2u_{14} + 2u_{19} + 2u_{21} + 2u_{22} + 2u_{25} + 2u_{26} + 2u_{28}\big) \\
&\quad + 15 - 6 && (238)\\
&\triangleq g^{(6)}_{\text{weak}}(\mathbf{u}_{\text{weak}}) + 15 - 6, && (239)
\end{aligned}
$$

where the inequalities in (236) and (237) hold with equality if, and only if, $u_j = 1$, $\forall\, j \in \mathcal{J}_1 \cup \mathcal{J}_2$.

Finally, the remaining steps in the derivation are equivalent to the case of $\mathsf{M} = 5$. Using the AM–GM inequality over all terms of the 2-wise series, we have

$$
\begin{aligned}
g^{(6)}_{\text{weak}}(\mathbf{u}_{\text{weak}}) \geq\ & 15\big(u_7^6u_{11}^6u_{13}^6u_{14}^6u_{19}^6u_{21}^6u_{22}^6u_{25}^6u_{26}^6u_{28}^6\big)^{\frac{1}{15}} \\
&- \big(2u_7 + 2u_{11} + 2u_{13} + 2u_{14} + 2u_{19} + 2u_{21} + 2u_{22} + 2u_{25} \\
&\quad + 2u_{26} + 2u_{28}\big) + 9. && (240)
\end{aligned}
$$

This lower bound is maximized and at the same time also achieved if $u_j = 1$, $\forall\, j \in \mathcal{J}_1 \cup \mathcal{J}_2$, and

$$
u_7 = u_{11} = u_{13} = u_{14} = u_{19} = u_{21} = u_{22} = u_{25} = u_{26} = u_{28} = \delta^{-\kappa}. \qquad (241)
$$