Error Probability Analysis of Binary Asymmetric Channels

Intermediate Report of NSC Project

"Finite Blocklength Capacity"

Date:	31 May 2010
Project-Number:	NSC 97-2221-E-009-003-MY3
Project Duration:	1 August 2008 – 31 July 2011
Funded by:	National Science Council, Taiwan

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

Abstract

In his world-famous paper of 1948, Shannon defined *channel capacity* as the ultimate rate at which information can be transmitted over a communication channel with an error probability that will vanish if we allow the blocklength to get infinitely large. While this result is of tremendous theoretical importance, the reality of practical systems looks quite different: no communication system will tolerate an infinite delay caused by an extremely large blocklength, nor can it deal with the computational complexity of decoding such huge codewords. On the other hand, it is not necessary to have an error probability that is exactly zero either, a small, but finite value will suffice.

Therefore, the question arises what can be done in a practical scheme. In particular, what is the maximal rate at which information can be transmitted over a communication channel for a given fixed maximum blocklength (*i.e.*, a fixed maximum delay) if we allow a certain maximal probability of error? In this project, we have started to study these questions.

Block-codes with very short blocklength over the most general binary channel, the binary asymmetric channel (BAC), are investigated. It is shown that for only two possible messages, flip-flop codes are optimal, however, depending on the blocklength and the channel parameters, not necessarily the linear flip-flop code. Further it is shown that the optimal decoding rule is a threshold rule. Some fundamental dependencies of the best code on the channel are given.

In the special case of a Z-channel, the optimal code is derived for the cases of two, three, and four messages. In the situation of two and four messages, the optimal code is shown to be linear.

Keywords: Channel capacity, binary asymmetric channel (BAC), error probability, finite blocklengths, ML, optimal codes, Z-channel.

Contents

1 Introduction

The analytical study of optimal communication over a channel is very difficult even if we restrict ourselves to discrete memoryless channels (DMCs). Most known results are derived using the mathematical trick of considering some limits, in particular, usually it is assumed that the blocklength tends to infinity. The insights that have been achieved in this way are considerable, but it still remains an open question how far these asymptotic results can be applied to the practical scenario where the blocklength is strongly restricted.

Shannon proved in his ground-breaking work [1] that it is possible to find an information transmission scheme that can transmit messages at arbitrarily small error probability as long as the transmission rate in *bits per channel use* is below the so-called *capacity* of the channel. However, he did not provide a way on how to find such schemes, in particular he did not tell us much about the design of codes apart from the fact that good codes need to have large blocklength.

For many practical applications exactly this latter constraint is rather unfortunate as often we cannot tolerate too much delay (*e.g.*, inter-human communication, time-critical control and communication, *etc.*). Moreover, the system complexity usually will grow exponentially in the blocklength. So we see that having large blocklength might not be an option and we have to restrict the blocklength to some

reasonable size. The question now arises what can theoretically be said about the performance of communication systems with such restricted blocksize.

For these reasons we have started to investigate the fundamental behavior of communication in the extreme case of an ultra-short blocklength. We would like to ask questions like: What performance can we expect from codes of fixed, very short blocklength? What can we say about good design for such codes?

To simplify the problem, we currently focus on binary memoryless channels and start with the simplest type of communication: a code with two to four equally likely messages.

In the subsequent section we will review some basic definitions and channel models needed in the context of reliable communication. This section is mainly based Shannon's first land-mark paper [1]. In Section 3 we give some preliminary definitions and results; Section 4 summarizes our results; and we conclude in Section 5.

2 Definitions

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 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*

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

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*

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

2.2 Coding for DMC

Definition 3. *A* $(\mathcal{M}, n)$ coding scheme *for a DMC* $(\mathcal{X}, \mathcal{Y}, P_{Y|X})$ *consists of*

- *the* message set $\mathcal{M} = \{1, \ldots, \mathcal{M}\}$ *of* $\mathcal{M}$ *equally likely random messages* M*;*
- *the* $(\mathcal{M}, n)$ codebook *(or simply* code*) consisting of* $\mathcal{M}$ *length-*n *channel input sequences, called* codewords*;*
- *an* encoding function $f\colon \mathcal{M} \to \mathcal{X}^n$ *that assigns for every message* $m \in \mathcal{M}$ *a codeword* $\mathbf{x} = (x_1, \ldots, x_n)$*; and*
- *a* decoding function $g\colon \ : \mathcal{Y}^n \to \hat{\mathcal{M}}$ *that maps the received channel output* n*-sequence* $\mathbf{y}$ *to a guess* $\hat{m} \in \hat{\mathcal{M}}$*. (Usually, we have* $\hat{\mathcal{M}} = \mathcal{M}$*.)*

Note that an $(\mathcal{M}, n)$ code consist merely of a unsorted list of $\mathcal{M}$ codewords of length n, whereas an $(\mathcal{M}, n)$ coding scheme additionally also defines the encoding and decoding functions. Hence, the same code can be part of many different coding schemes.

Definition 4. *A code is called* linear *if the sum of any two codewords again is a codeword.*

Note that a linear code always contains the all-zero codeword.

The two main parameters of interest of a code are the number of possible messages $\mathcal{M}$ (the larger, the more information is transmitted) and the blocklength n (the shorter, the less time is needed to transmit the message):

- we have $\mathcal{M}$ equally likely messages, *i.e.*, the entropy is $H(M) = \log_2 \mathcal{M}$ bits and we need $\log_2 \mathcal{M}$ bits to describe the message in binary form;
- we need n transmissions of a channel input symbol X_k over the channel in order to transmit the complete message.

Hence, it makes sense to give the following definition.

Definition 5. *The* rate[1] *of a* $(\mathcal{M}, n)$ *code is defined as*

$$\mathcal{R} \triangleq \frac{\log_2 \mathcal{M}}{n} \text{ bits/transmission.} \tag{4}$$

It describes what amount of information (i.e., what part of the $\log_2 \mathcal{M}$ bits) is transmitted in each channel use.

However, this definition of a rate makes only sense if the message really arrives at the receiver, *i.e.*, if the receiver does not make a decoding error!

Definition 6. *Given that message* $M = m$ *has been sent, let* λ_m *be the* probability of a decoding error *of an* $(\mathcal{M}, n)$ *coding scheme:*

$$\lambda_m \triangleq \Pr[g(Y_1^n) \neq m \mid X_1^n = f(m)] = \sum_{\mathbf{y} \in \mathcal{Y}^n} p(\mathbf{y}|\mathbf{x}(m)) I\{g(\mathbf{y}) \neq m\}, \tag{5}$$

where $I\{\cdot\}$ *is the indicator function*

$$I\{\text{statement}\} \triangleq \begin{cases} 1 & \text{if statement is true,} \\ 0 & \text{if statement is wrong.} \end{cases}$$

[1] We define the rate here using a logarithm of base 2. However, we can use any logarithm as long as we adapt the units accordingly.

The maximum error probability $\lambda^{(n)}$ *of an* $(\mathcal{M}, n)$ *coding scheme is defined as*

$$\lambda^{(n)} \triangleq \max_{m \in \mathcal{M}} \lambda_m. \tag{6}$$

The average error probability $P_{\mathrm{e}}^{(n)}$ *of an* $(\mathcal{M}, n)$ *coding scheme is defined as*

$$P_{\mathrm{e}}^{(n)} \triangleq \frac{1}{\mathcal{M}} \sum_{m=1}^{\mathcal{M}} \lambda_m. \tag{7}$$

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

$$\psi_m \triangleq \Pr[g(Y_1^n) = m \mid X_1^n = f(m)] = \sum_{\mathbf{y} \in \mathcal{Y}^n} p(\mathbf{y}|\mathbf{x}(m)) I\{g(\mathbf{y}) = m\}. \tag{8}$$

The definitions of maximum success probability $\psi^{(n)}$ *and average success probability*[2] $P_{\mathrm{c}}^{(n)}$ *are accordingly.*

Note that for given a codebook $\mathcal{C}$*, we define the decoding region* $\mathcal{D}_i$ *corresponding to the* m*-th codewords,* $m = 1, 2, \ldots, \mathcal{M}$*, as*

$$\mathcal{D}_m \triangleq \{\mathbf{y} \colon g(\mathbf{y}) = m\}. \tag{9}$$

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

Theorem 7 (The Channel Coding Theorem for a DMC). *Define*

$$\mathsf{C} \triangleq \max_{P_X(\cdot)} I(X;Y) \tag{10}$$

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* $\mathsf{R} \leq \mathsf{C}$*.*

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.

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?

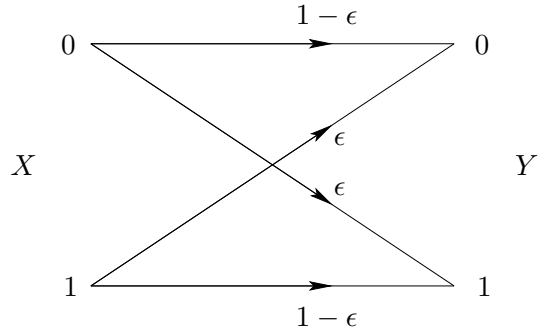

Figure 1: Binary symmetric channel (BSC).

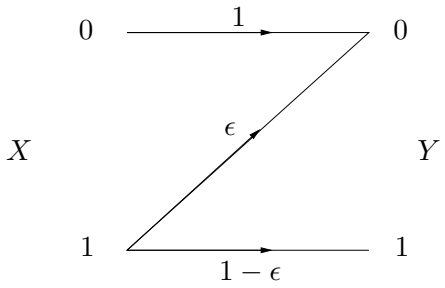

Figure 2: Z-channel.

2.3 Channel Model

In the following we will concentrate on the special cases of *binary* DMCs, *i.e.*, we restrict our channel alphabets to be binary.

The best known example of a binary DMC is the *binary symmetric channel (BSC)* shown in Figure 1. Another important special case of a binary DMC is the *Z-channel* shown in Fig 2.

The most general binary channel is a butterfly-channel with crossover probabilities that are not identical. In reference to the BSC we call this channel model *binary asymmetric channel (BAC)*, see Figure 3. Both BSC and Z-channel are special cases of the BAC.

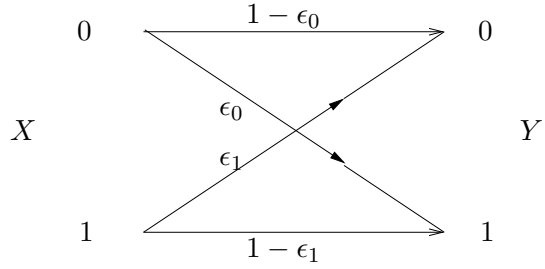

Figure 3: Binary asymmetric channel (BAC).

A BAC is specified by two parameters: ϵ_0 denoting the probability that a 0 is changed into a 1 and ϵ_1 denoting the probability that a 1 is changed into a 0.

For symmetry reasons and without loss of generality we can restrict the values of these parameters as follows:

$$0 \leq \epsilon_0 \leq \epsilon_1 \leq 1, \tag{11}$$

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

$$\epsilon_0 \leq 1 - \epsilon_0, \tag{12}$$

$$\epsilon_0 \leq 1 - \epsilon_1. \tag{13}$$

Note that in the case where $\epsilon_0 > \epsilon_1$ we simply can flip all zeros to ones and vice-versa to get an equivalent channel with $\epsilon_0 \leq \epsilon_1$. For the case where $\epsilon_0 > 1 - \epsilon_0$, we can flip the output Y, *i.e.*, change all output zeros to ones and ones to zeros, to get an equivalent channel with $\epsilon_0 \leq 1 - \epsilon_0$. Note that (12) can be simplified to $\epsilon_0 \leq \frac{1}{2}$. And for the case where $\epsilon_0 > 1 - \epsilon_1$, we can flip the input X to get an equivalent channel that satisfies $\epsilon_0 \leq 1 - \epsilon_1$.

We have depicted the region of possible choices of the parameters ϵ_0 and ϵ_1 in Figure 4. The region of interesting choices given by (11) and (12) is denoted by Ω.

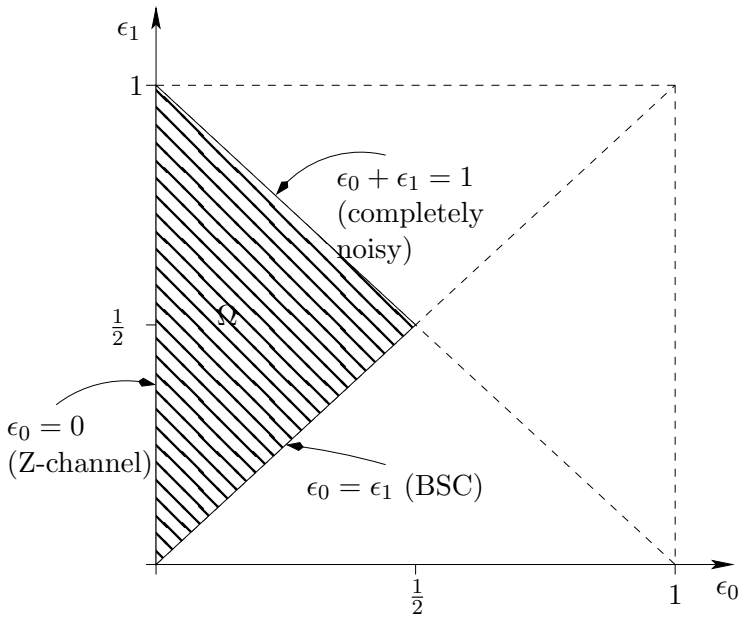

Figure 4: Region of possible choices of the channel parameters ϵ_0 and ϵ_1 of a BAC. The shaded area corresponds to the interesting area according to (11), (12) and (13).

Note that the BAC includes all well-known binary channel models: if $\epsilon_0 = \epsilon_1$, we have a BSC; and if $\epsilon_0 = 0$, we have a Z-channel. In the case when $\epsilon_0 = 1 - \epsilon_1$ we end up with a completely noisy channel of zero capacity: given $Y = y$, $X = 0$ and $X = 1$ are equally likely, *i.e.*, $X \perp\!\!\!\perp Y$.

3 Preliminaries

3.1 Capacity of the BAC

As mentioned above, without loss of generality, we only consider BACs with $0 \leq \epsilon_0 \leq \epsilon_1 \leq 1$. The capacity of a BAC is given by

$$C_{\text{BAC}} = \frac{\epsilon_0}{1 - \epsilon_0 - \epsilon_1} \cdot H_{\text{b}}(\epsilon_1) - \frac{1 - \epsilon_1}{1 - \epsilon_0 - \epsilon_1} \cdot H_{\text{b}}(\epsilon_0) + \log_2 \left(1 + 2^{\frac{H_{\text{b}}(\epsilon_0) - H_{\text{b}}(\epsilon_1)}{1 - \epsilon_0 - \epsilon_1}} \right) \tag{14}$$

bits, where $H_{\text{b}}(\cdot)$ is the binary entropy function defined as

$$H_{\text{b}}(p) \triangleq -p \log_2 p - (1 - p) \log_2 (1 - p).$$

The input distribution $P_X^*(\cdot)$ that achieves this capacity is given by

$$P_X^*(0) = 1 - P_X^*(1) = \frac{1 - \epsilon_1(1+z)}{(1-\epsilon_0-\epsilon_1)(1+z)} \tag{15}$$

with

$$z \triangleq 2^{\frac{H_{\mathrm{b}}(\epsilon_0)-H_{\mathrm{b}}(\epsilon_1)}{1-\epsilon_0-\epsilon_1}}. \tag{16}$$

3.2 Error Probability of the BSC

Consider the situation of a BSC and assume that we transmit the m-th codeword $\mathbf{x}_m$, $1 \leq m \leq \mathcal{M}$, and that we receive $\mathbf{y}$. The *maximum likelihood (ML)* decision is then

$$g(\mathbf{y}) \triangleq \arg \max_{1 \leq i \leq \mathcal{M}} P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y}|\mathbf{x}_i). \tag{17}$$

The average probability of error can be computed as

$$P_{\mathrm{e}} = \frac{1}{\mathcal{M}}(1-\epsilon)^n \sum_{\mathbf{y}} \sum_{\substack{i=1 \\ i \neq g(\mathbf{y})}}^{\mathcal{M}} \left(\frac{\epsilon}{1-\epsilon}\right)^{d_{\mathrm{H}}(\mathbf{x}_i,\mathbf{y})} \tag{18}$$

where $d_{\mathrm{H}}(\cdot,\cdot)$ is the Hamming distance.

Note that if we want to find the *best* average error probability, we need to check through **all possible** codes (including both linear and nonlinear codes). The complexity of such a search grows exponentially fast in n: for $\mathcal{M} = 4$ and

- for $n = 3$ there are $\binom{8}{4} = 70$ different codes;
- for $n = 4$ there are $\binom{16}{4} = 1820$ different codes;
- for $n = 5$ there are $\binom{32}{4} = 35960$ different codes, etc.

It turns out that for a given BSC, blocklength n, and number of message $\mathcal{M}$, there is a vast amount of different codes (linear and nonlinear) that are all optimal. This is not really surprising because the BSC is *strongly symmetric*.

3.3 Error Probability of the BAC

To simplify our notation we introduce $d_{\alpha\beta}(\mathbf{x}_i, \mathbf{y})$ to be the number of positions j where $x_i^{(j)} = \alpha$ and $y^{(j)} = \beta$, where as usual $\mathbf{x}_i$, $i \in \{1, 2, \ldots, \mathcal{M}\}$, is the sent codeword and $\mathbf{y}$ is the received sequence.

The conditional probability of the received vector given the sent codeword can now be written as

$$P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y}|\mathbf{x}_i) = (1-\epsilon_0)^{d_{00}(\mathbf{x}_i,\mathbf{y})} \cdot \epsilon_0^{d_{01}(\mathbf{x}_i,\mathbf{y})} \cdot \epsilon_1^{d_{10}(\mathbf{x}_i,\mathbf{y})} \cdot (1-\epsilon_1)^{d_{11}(\mathbf{x}_i,\mathbf{y})}. \tag{19}$$

Note that we can express these different $d_{\alpha\beta}$'s as follows:

$$d_{11}(\mathbf{x}_i, \mathbf{y}) = \frac{1}{2} w_{\mathrm{H}}(\mathbf{x}_i + \mathbf{y} - |\mathbf{x}_i - \mathbf{y}|), \tag{20}$$
$$d_{10}(\mathbf{x}_i, \mathbf{y}) = w_{\mathrm{H}}(I\{\mathbf{x}_i - \mathbf{y} > 0\}), \tag{21}$$
$$d_{01}(\mathbf{x}_i, \mathbf{y}) = w_{\mathrm{H}}(I\{\mathbf{y} - \mathbf{x}_i > 0\}), \tag{22}$$
$$d_{00}(\mathbf{x}_i, \mathbf{y}) = n - d_{11}(\mathbf{x}_i, \mathbf{y}) - d_{10}(\mathbf{x}_i, \mathbf{y}) - d_{01}(\mathbf{x}_i, \mathbf{y}), \tag{23}$$

where $w_{\mathrm{H}}(\mathbf{x})$ is the Hamming weight of $\mathbf{x}$.

The average error probability of a code $\mathcal{C}$ over a BAC (assuming equally likely messages) can be expressed as

$$P_{\mathrm{e}}(\mathcal{C}) = \frac{1}{\mathcal{M}}(1-\epsilon_0)^n \sum_{\mathbf{y}} \sum_{\substack{i=1 \\ i \neq g(\mathbf{y})}}^{\mathcal{M}} \left(\frac{\epsilon_0}{1-\epsilon_0}\right)^{d_{01}(\mathbf{x}_i,\mathbf{y})} \left(\frac{\epsilon_1}{1-\epsilon_0}\right)^{d_{10}(\mathbf{x}_i,\mathbf{y})} \left(\frac{1-\epsilon_1}{1-\epsilon_0}\right)^{d_{11}(\mathbf{x}_i,\mathbf{y})} \tag{24}$$

$$= \frac{1}{\mathcal{M}} \sum_{i=1}^{\mathcal{M}} \sum_{\substack{\mathbf{y} \\ g(\mathbf{y}) \neq i}} P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y}|\mathbf{x}_i), \tag{25}$$

where $g(\mathbf{y})$ is the ML decision (17) for the observation $\mathbf{y}$.

Note that a closer investigation shows that some of these optimal codes are linear, but some are not.

3.4 Error (and Success) Probability of the Z-Channel

A special case of the BAC is the Z-channel where we have $\epsilon_0 = 0$. By symmetry, assume that $\epsilon_1 \leq \frac{1}{2}$. Note that it is often easier to maximize the success probability instead of minimizing the error probability. For the convenience of later derivations, we now are going to derive its error and success probabilities:

$$P_{\mathrm{c}}(\mathcal{C}) = \frac{1}{\mathcal{M}} \sum_{i=1}^{\mathcal{M}} \sum_{\substack{\mathbf{y} \\ g(\mathbf{y})=i}} (1-\epsilon_1)^{w_{\mathrm{H}}(\mathbf{x}_i)} \left(\frac{\epsilon_1}{1-\epsilon_1}\right)^{d_{10}(\mathbf{x}_i,\mathbf{y})} \cdot I\left\{\text{if } x_i^{(j)} = 0 \implies y^{(j)} = 0, \forall\, j\right\}. \tag{26}$$

The error probability formula is accordingly

$$P_{\mathrm{e}}(\mathcal{C}) = \frac{1}{\mathcal{M}} \sum_{i=1}^{\mathcal{M}} \sum_{\substack{\mathbf{y} \\ g(\mathbf{y}) \neq i}} (1-\epsilon_1)^{w_{\mathrm{H}}(\mathbf{x}_i)} \left(\frac{\epsilon_1}{1-\epsilon_1}\right)^{d_{10}(\mathbf{x}_i,\mathbf{y})} \cdot I\left\{\text{if } x_i^{(j)} = 0 \implies y^{(j)} = 0, \forall\, j\right\}. \tag{27}$$

Note that the capacity-achieving distribution for $\epsilon_1 = \frac{1}{2}$ is

$$\Pr[X = 1] = \frac{2}{5}. \tag{28}$$

4 Main Results

4.1 Optimal Codes for the Case $\mathcal{M} = 2$

We start with the definition of a special class of codes: *flip-flop codes*.

Definition 8. *A code with two codewords ($\mathcal{M} = 2$) is called* ***flip-flop code*** *if one codeword is the flipped version of the other,* i.e., *if in each position where the first codeword has a 1, the second has a 0, and vice-versa.*

In particular, we define the ***flip-flop code of type*** t *as follows: for every* $t \in \{0, 1, \ldots, \lfloor \frac{n}{2} \rfloor\}$*, we have*

$$\mathcal{C}_{2,t}^{(n)} = \begin{pmatrix} \mathbf{x}_1 \\ \mathbf{x}_2 \end{pmatrix} \triangleq \begin{pmatrix} \mathbf{x} \\ \bar{\mathbf{x}} \end{pmatrix} \tag{29}$$

where

$$\mathbf{x}_1 = \mathbf{x} \triangleq 00\cdots0\underbrace{11\cdots1}_{w_{\mathrm{H}}(\mathbf{x})=t}, \tag{30}$$

$$\mathbf{x}_2 = \bar{\mathbf{x}} \triangleq 11\cdots100\cdots0. \tag{31}$$

Note that the parameter t *is the Hamming weight of the first codeword* $\mathbf{x}_1$*.*

Due to the memorylessness of the BAC, the order of the columns of any code is irrelevant. We therefore can restrict ourselves without loss of generality to flip-flop codes of type t to describe all possible flip-flop codes.

Also note that the only possible linear flip-flop code is $\mathcal{C}_{2,0}^{(n)}$. All other flip-flop codes are nonlinear.

We are now ready for the following result.

Proposition 9. *Consider the case* $\mathcal{M} = 2$*, and fix the blocklength* n*. Then, irrespective of the channel parameters* ϵ_0 *and* ϵ_1*, on a BAC there always exists a flip-flop code of type* t*,* $\mathcal{C}_{2,t}^{(n)}$*, for some choice of parameter* t*,* $0 \le t \le \lfloor \frac{n}{2} \rfloor$*, that is optimal in the sense that it minimizes the error probability.*

Proof. See Appendix A. □

This result is intuitively very pleasing because it seems to be a rather bad choice to have two codewords with the same symbol in a particular position. However, the proposition does not exclude the possibility that such a code might exist that also is optimal.

We would like to point out that the exact choice of t is not obvious and depends strongly on n, ϵ_0, and ϵ_1. As an example, the optimal choices of t are shown in Figure 5 for $n = 5$. We see that depending on the channel parameters, the optimal value of t changes. Note that on the boundaries the optimal choice is not unique: for a completely noisy BAC ($\epsilon_1 = 1 - \epsilon_0$), the choice of the codebook is irrelevant since the probability of error is $\frac{1}{2}$ in any case. For a BSC, $t = 0$, $t = 1$, or $t = 2$ are equivalent. And for a Z-channel we can prove that a linear code is always optimal.[3]

4.2 Optimal Codes for the Z-Channel

We next give the following generalization of the flip-flop code for $\mathcal{M} = 4$ codewords.

Definition 10. *A* ***two-pair flip-flop code*** *with* $\mathcal{M} = 4$ *codewords consists of two combined flip-flop codes. In particular, we define the* ***two-pair flip-flop code of type*** t *to be the linear code that combines* $\mathcal{C}_{2,0}^{(n)}$ *and* $\mathcal{C}_{2,t}^{(n)}$*: for every* $t \in \{1, \ldots, \lfloor \frac{n}{2} \rfloor\}$*, we have*

$$\mathcal{C}_{4,t}^{(n)} = \begin{pmatrix} \mathbf{x}_1 \\ \mathbf{x}_2 \\ \mathbf{x}_3 \\ \mathbf{x}_4 \end{pmatrix} \triangleq \begin{pmatrix} \mathbf{0} \\ \mathbf{x} \\ \bar{\mathbf{x}} \\ \mathbf{1} \end{pmatrix} \tag{32}$$

[3] As seen next in Section 4.2, a linear code is also optimal for the Z-channel for the case $\mathcal{M} = 4$.

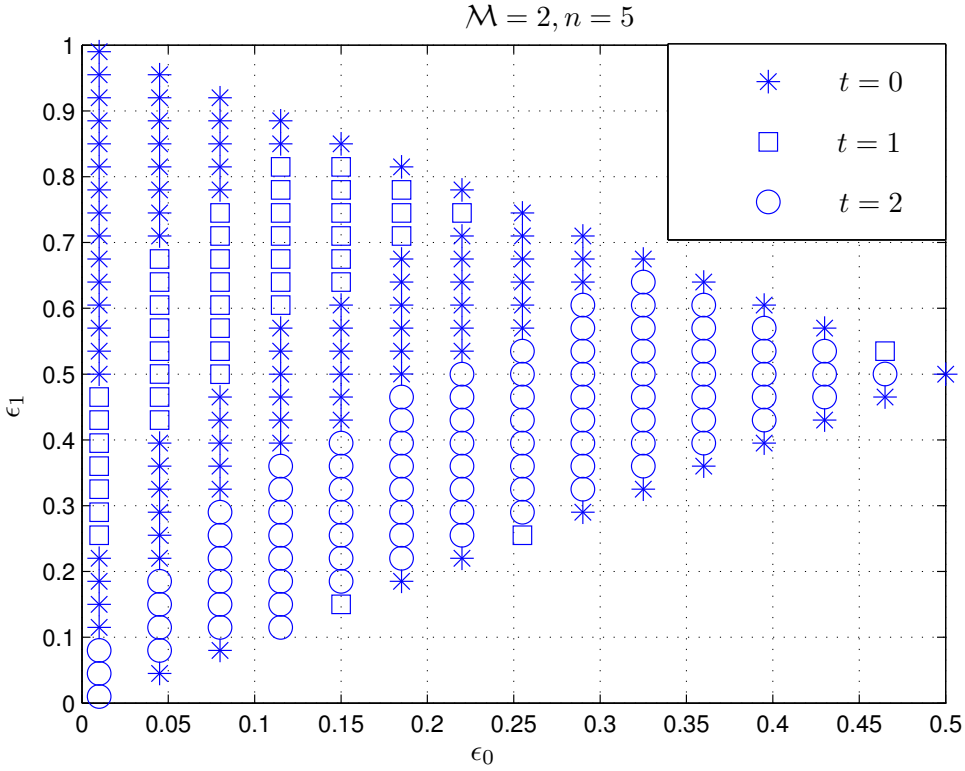

Figure 5: Optimal codebooks on a BAC: the optimal choice of the parameter t for different values of ϵ_0 and ϵ_1 for a fixed blocklength $n = 5$.

where $\mathbf{x}$ *is defined in* (30). *I.e., in* $\mathcal{C}_{4,t}^{(n)}$ *there are* $(n-t)$ *columns* $(0\ 0\ 1\ 1)^{\mathsf{T}}$ *and* t *columns* $(0\ 1\ 0\ 1)^{\mathsf{T}}$.

Based on this definition and the peculiar behavior of the Z-channel that ensures that $P_{Y|X}(1|0) = 0$, it is now possible to prove the following lemma.

Lemma 11. *For a Z-channel and for a given two-pair flip-flop code of type* t, $\mathcal{C}_{4,t}^{(n)}$, *with* $1 \leq t \leq \lfloor \frac{n}{2} \rfloor$, *the decoding regions of the codewords* $\mathbf{x}_i$ *are*

$$\mathcal{D}_{4,t,1}^{(n)} = \left\{ \mathbf{0}^{(n)} \right\}, \tag{33}$$

$$\mathcal{D}_{4,t,2}^{(n)} = \left\{ \mathbf{y}^{(n)} \colon \mathbf{y}^{(n)} = [\mathbf{0}^{(n-t)} \mathbf{y}^{(t)}] \text{ with } w_{\mathrm{H}}(\mathbf{y}^{(t)}) = t, t-1, \ldots, 1 \right\}, \tag{34}$$

$$\mathcal{D}_{4,t,3}^{(n)} = \Big\{ \mathbf{y}^{(n)} \colon \mathbf{y}^{(n)} = [\mathbf{y}^{(n-t)} \mathbf{0}^{(t)}] \text{ with } w_{\mathrm{H}}(\mathbf{y}^{(n-t)}) = (n-t), (n-t)-1, \ldots, 1 \Big\}, \tag{35}$$

$$\mathcal{D}_{4,t,4}^{(n)} = \{0,1\}^n \setminus \bigcup_{i=1}^{3} \mathcal{D}_{4,t,i}^{(n)}. \tag{36}$$

Moreover,

$$\left| \mathcal{D}_{4,t,1}^{(n)} \right| = 1, \tag{37}$$

$$\left| \mathcal{D}_{4,t,2}^{(n)} \right| = \sum_{d=0}^{t-1} \binom{t}{d} = 2^t - 1, \tag{38}$$

$$\left|\mathcal{D}_{4,t,3}^{(n)}\right| = \sum_{d=0}^{(n-t)-1} \binom{n-t}{d} = 2^{(n-t)-1}, \tag{39}$$

$$\left|\mathcal{D}_{4,t,4}^{(n)}\right| = \sum_{d=0}^{n-1} \left[\binom{n}{d} - \binom{n-t}{d-t} - \binom{t}{d-(n-t)}\right] = 2^n - 2^t - 2^{n-t} + 1. \tag{40}$$

Note that the parameter d in the summations stands for the Hamming distance between the received vector and the particular codeword $d_{10}(\mathbf{x}_i, \mathbf{y})$.

The success probability for a given $\mathcal{C}_{4,t}^{(n)}$ code is

$$4P_{\mathrm{c}}(\mathcal{C}_{4,t}^{(n)}) = \sum_{m=1}^{4} \psi_{m,i}^{(n)} \tag{41}$$

$$\begin{aligned} &= 1 + \sum_{d=0}^{t-1} \binom{t}{d} (1-\epsilon_1)^{t-d} \cdot \epsilon_1^d + \sum_{d=0}^{(n-t)-1} \binom{(n-t)}{d} (1-\epsilon_1)^{(n-t)-d} \cdot \epsilon_1^d \\ &\quad + \sum_{d=0}^{n-1} \left[\binom{n}{d} - \binom{(n-t)}{d-t} - \binom{t}{d-(n-t)}\right] (1-\epsilon_1)^{n-d} \cdot \epsilon_1^d, \end{aligned} \tag{42}$$

where the last term in the summation of RHS can also be written as

$$\sum_{i=1}^{n-t} \sum_{j=1}^{t} \binom{(n-t)}{i} \binom{t}{j} (1-\epsilon_1)^{i+j} \cdot \epsilon_1^{n-i-j}. \tag{43}$$

Proof. Due to our construction of the two-pair flip-flop code of type t, we always have that one codeword is the flipped version of one of the other, and by the ML decoding rule (17), we only can decode a vector $\mathbf{y}$ to a codeword such that there are no flips from 0 to 1. From $P_{Y|X}(0|0) = 1$, the first codeword will always be transmitted to $\mathbf{0}^{(n)}$. Hence, $\mathcal{D}_{4,t,1}^{(n)}$ only consists of the all-zero vector.

For any $\mathbf{y} \in \mathcal{D}_{4,t,2}^{(n)}$, given in (34),

$$\begin{aligned} &\max\left\{P_{Y|X}^n(\mathbf{y}|\mathbf{x}_1), P_{Y|X}^n(\mathbf{y}|\mathbf{x}_2), P_{Y|X}^n(\mathbf{y}|\mathbf{x}_3), P_{Y|X}^n(\mathbf{y}|\mathbf{x}_4)\right\} \\ &\quad = \max\left\{0, P_{Y|X}^n(\mathbf{y}|\mathbf{x}_2), 0, P_{Y|X}^n(\mathbf{y}|\mathbf{x}_4)\right\} && (44) \\ &\quad = P_{Y|X}^n(\mathbf{y}|\mathbf{x}_2) && (45) \\ &\quad = (1-\epsilon_1)^{t-d}\epsilon_1^d, && (46) \end{aligned}$$

where $1 \le d \le t-1$, since $0 < \epsilon_1 \le \frac{1}{2}$ and $w_{\mathrm{H}}(\mathbf{x}_4) = n > t \ge w_{\mathrm{H}}(\mathbf{x}_2)$.

The same argument can be applied to the decoding region $\mathcal{D}_{4,t,3}^{(n)}$, and $\mathcal{D}_{4,t,4}^{(n)}$ must be $\{0,1\}^n \setminus \bigcup_{i=1}^{3} \mathcal{D}_{4,t,i}^{(n)}$. □

By Lemma 11, now we have the following theorem proving the optimal code structure on the Z-channel for $\mathcal{M} = 4$.

Theorem 12. *Fix a blocklength $n \ge 2$. Then on the Z-channel under four hypotheses $\mathcal{M} = 4$, the two-pair flip-flop code of type $\lfloor \frac{n}{2} \rfloor$ is optimal in ML-sense.*

Note that the success probability formula is given in (41) where we choose $t = \lfloor \frac{n}{2} \rfloor$. Note further that this means that for the Z-channel always an optimal code can be found that is linear.

Proof of Theorem 12. Our proof is based on induction on n. Since $2^2 = 4$ and there are only four possible different rows when $n = 2$, the optimal code for $n = 2$ is

$$\mathcal{C}_{4,1}^{(2)} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \\ 1 & 0 \\ 1 & 1 \end{pmatrix}. \tag{47}$$

Next assume that for blocklength n, $\mathcal{C}_{4,\lfloor \frac{n}{2} \rfloor}^{(n)}$ is optimal. Then, from Claim 13 below, this assumption still holds for $n+1$. This then proves the theorem. □

Claim 13. *Let's add one new column to the two-pair flip-flop code of type* $\lfloor \frac{n}{2} \rfloor$, $\mathcal{C}_{4,\lfloor \frac{n}{2} \rfloor}^{(n)}$, *to generate a new code of length* $n+1$. *The optimal (in the sense of resulting in the smallest probability of error) choice among all possible* $2^{\mathsf{M}}-1-1 = 14$ *columns is*

$$\begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}. \tag{48}$$

Proof. Note that there are 14 possible columns that we could choose as the $(n+1)$-th column:

$$\begin{gathered} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \\ \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \end{pmatrix}. \end{gathered} \tag{49}$$

The choice of the all-zero or all-one column clearly is suboptimal because in this case an optimal decoder will simply ignore the $(n+1)$-th received digit.

Hence, our new code is

$$\begin{pmatrix} [\mathbf{0}\ x_{1,n+1}] \\ [\mathbf{x}\ x_{2,n+1}] \\ [\bar{\mathbf{x}}\ x_{3,n+1}] \\ [\mathbf{1}\ x_{4,n+1}] \end{pmatrix} \tag{50}$$

where $x_{i,n+1} \in \{0,1\}$ and the $\mathbf{x}$ is given in (30) with

$$t \triangleq \left\lfloor \frac{n}{2} \right\rfloor. \tag{51}$$

Note that in the remainder of this proof t can be read as shorthand for $\lfloor \frac{n}{2} \rfloor$.

We now extend the decoding regions given by Lemma 11 by one bit:

$$[\mathcal{D}_{4,t,1}^{(n)}\ 0] \cup [\mathcal{D}_{4,t,1}^{(n)}\ 1] = \left\{ [\mathbf{0}^{(n)}\ 0], [\mathbf{0}^{(n)}\ 1] \right\}, \tag{52}$$

$$\begin{aligned} [\mathcal{D}_{4,t,2}^{(n)}\ 0] \cup [\mathcal{D}_{4,t,2}^{(n)}\ 1] = \Big\{ & \mathbf{y}^{(n+1)} \colon \mathbf{y}^{(n+1)} = [\mathbf{0}^{(n-t)}\ \mathbf{y}^{(t)}\ 0] \text{ or } [\mathbf{0}^{(n-t)}\ \mathbf{y}^{(t)}\ 1] \text{ with} \\ & w_{\mathrm{H}}(\mathbf{y}^{(t)}) = t, t-1, \ldots, 1 \Big\}, \end{aligned} \tag{53}$$

$$[\mathcal{D}_{4,t,3}^{(n)}\ 0] \cup [\mathcal{D}_{4,t,3}^{(n)}\ 1] = \Big\{\mathbf{y}^{(n+1)} \colon \mathbf{y}^{(n+1)} = [\mathbf{y}^{(n-t)}\ \mathbf{0}^{(t)}\ 0] \text{ or } [\mathbf{y}^{(n-t)}\ \mathbf{0}^{(t)}\ 1] \text{ with } w_{\mathrm{H}}(\mathbf{y}^{(n-t)}) = (n-t), (n-t)-1, \ldots, 1\Big\}, \tag{54}$$

$$[\mathcal{D}_{4,t,4}^{(n)}\ 0] \cup [\mathcal{D}_{4,t,4}^{(n)}\ 1] = \Big\{\mathbf{y}^{(n+1)} \colon \mathbf{y}^{(n+1)} = [\mathbf{y}^{(n)}\ 0] \text{ or } [\mathbf{y}^{(n)}\ 1] \text{ with } \mathbf{y}^{(n)} \in \mathcal{D}_{4,t,4}^{(n)}\Big\}. \tag{55}$$

Observe that these new decoding regions retain the same success probability $\psi_{4,t,i}^{(n+1)} = \psi_{4,t,i}^{(n)} \cdot 1$, because

$$P_{Y|X}(0|x_{n+1,i}) + P_{Y|X}(0|x_{n+1,i}) = 1. \tag{56}$$

However, it is quite clear that these new regions are in general not the optimal decision regions anymore for the new code. So the question is how to fix them to make them optimal again (and thereby also finding out how to optimally choose $x_{n+1,i}$).

Firstly note that if $x_{n+1,i} = 0$, adding a 0 to the received vector $\mathbf{y}^{(n)}$ will not change the decision i because 0 is the correct outcome anyway. Similarly, if $x_{n+1,i} = 1$, adding a 1 to the vector $\mathbf{y}^{(n)}$ will not change the decision i.

Secondly, we claim that even if $x_{n+1,i} = 1$, all received vectors $\mathbf{y}^{(n+1)} \in [\mathcal{D}_{4,t,i}^{(n)}\ 0]$ still will be decoded to i. To see this, let's have a look at the four cases separately:

- $[\mathcal{D}_{4,t,1}^{(n)}\ 0]$: The decoding region $[\mathcal{D}_{4,t,1}^{(n)}\ 0]$ only contains one vector: the all-zero vector. We have
$$P_{Y|X}^{n+1}\big(\mathbf{0}^{(n+1)} \,\big|\, \mathbf{x}_1^{(n+1)} = \mathbf{0}^{(n)}1\big) = \epsilon_1 \geq P_{Y|X}^{n+1}\big(\mathbf{0}^{(n+1)} \,\big|\, \mathbf{x}_j^{(n+1)}\big), \quad \forall\, j = 2,3,4, \tag{57}$$
independent of the choices of $x_{j,n+1}$, $j = 2, 3, 4$. Hence, we decide for $i = 1$.

- $[\mathcal{D}_{4,t,2}^{(n)}\ 0]$: All vectors in $[\mathcal{D}_{4,t,2}^{(n)}\ 0]$ contain ones in positions that make it impossible to decode it as $i = 1$ or $i = 3$. On the other hand, $i = 4$ obviously is less likely than $i = 2$, *i.e.*, we decide $i = 2$.

- $[\mathcal{D}_{4,t,3}^{(n)}\ 0]$: All vectors in $[\mathcal{D}_{4,t,3}^{(n)}\ 0]$ contain ones in positions that make it impossible to decode it as $i = 1$ or $i = 2$. On the other hand, $i = 4$ obviously is less likely than $i = 3$, *i.e.*, we decide $i = 3$.

- $[\mathcal{D}_{4,t,4}^{(n)}\ 0]$: Finally, all vectors in $[\mathcal{D}_{4,t,4}^{(n)}\ 0]$ contain ones in positions that make it impossible to decode it as $i = 1$, $i = 2$, or $i = 3$. It only remains to decide $i = 4$.

So, it only remains to investigate the decision made about the vectors in $[\mathcal{D}_{4,t,i}^{(n)}\ 1]$ if $x_{i,n+1} = 0$. Note that we do not need to bother about $[\mathcal{D}_{4,t,4}^{(n)}\ 1]$ as it is impossible to receive such a vector because for all $\mathbf{y} \in \mathcal{D}_{4,t,4}^{(n)}$

$$P_{Y|X}^{n}(\mathbf{y}^{(n)}|\mathbf{0}^{(n)}) = P_{Y|X}^{n}(\mathbf{y}^{(n)}|\mathbf{0}^{(n-t)}\mathbf{1}^{(t)}) = P_{Y|X}^{n}(\mathbf{y}^{(n)}|\mathbf{1}^{(n-t)}\mathbf{0}^{(t)}) = 0. \tag{58}$$

For $i = 1$, 2, or 3, if $x_{i,n+1} = 0$, the received vectors in $[\mathcal{D}_{4,t,i}^{(n)}\ 1]$ will change to another decoding region not equal to i because $P_{Y|X}(1|0) = 0$.

- $[\mathcal{D}_{4,t,1}^{(n)}\ 1]$: If we assign these vectors (actually, it's only one) to the new decoding region $\mathcal{D}_{4,t,2}^{(n+1)}$, the conditional success probability is
$$P_{\mathrm{c},2} = \sum_{\mathbf{y}^{(n)} \in \mathcal{D}_{4,t,1}^{(n)}} P_{Y|X}^{n+1}\big([\mathbf{y}^{(n)}\ 1] \,\big|\, [\mathbf{0}^{(n-t)}\mathbf{1}^{t}\ 1]\big) \cdot (x_{2,n+1} - x_{1,n+1})^{+} \tag{59}$$
$$= \epsilon_1^t(1-\epsilon_1) \cdot (x_{2,n+1} - x_{1,n+1})^{+}, \tag{60}$$

where

$$(x)^+ = \begin{cases} x & \text{if } x \geq 0, \\ 0 & \text{if } x < 0. \end{cases} \tag{61}$$

Note that $x_{2,n+1}$ must be 1 if it shall be possible for this event to occur!

Similarly, we compute

$$P_{\mathrm{c},3} = \sum_{\mathbf{y}^{(n)} \in \mathcal{D}_{4,t,1}^{(n)}} P_{Y|X}^{n+1}\left([\mathbf{y}^{(n)}\ 1] \,\middle|\, [\mathbf{1}^{(n-t)}\mathbf{0}^t\ 1]\right) \cdot (x_{3,n+1} - x_{1,n+1})^+ \tag{62}$$

$$= \epsilon_1^{(n-t)}(1-\epsilon_1) \cdot (x_{3,n+1} - x_{1,n+1})^+; \tag{63}$$

$$P_{\mathrm{c},4} = \sum_{\mathbf{y}^{(n)} \in \mathcal{D}_{4,t,1}^{(n)}} P_{Y|X}^{n+1}\left([\mathbf{y}^{(n)}\ 1] \,\middle|\, [\mathbf{1}^{(n)}\ 1]\right) \cdot (x_{4,n+1} - x_{1,n+1})^+ \tag{64}$$

$$= \epsilon_1^{n}(1-\epsilon_1) \cdot (x_{4,n+1} - x_{1,n+1})^+. \tag{65}$$

From $\epsilon_1^t \geq \epsilon_1^{(n-t)} > \epsilon_1^n$ we see that $P_{\mathrm{c},2}$ gives the highest increase, followed by $P_{\mathrm{c},3}$ and then $P_{\mathrm{c},4}$. Hence, we should write them as follows:

$$P_{\mathrm{c},2} = \epsilon_1^{t}(1-\epsilon_1) \cdot (x_{2,n+1} - x_{1,n+1})^+, \tag{66}$$

$$P_{\mathrm{c},3} = \epsilon_1^{(n-t)}(1-\epsilon_1) \cdot (x_{3,n+1} - x_{2,n+1} - x_{1,n+1})^+, \tag{67}$$

$$P_{\mathrm{c},4} = \epsilon_1^{n}(1-\epsilon_1) \cdot (x_{4,n+1} - x_{3,n+1} - x_{2,n+1} - x_{1,n+1})^+. \tag{68}$$

- $[\mathcal{D}_{4,t,2}^{(n)}\ 1]$: In this case only $\mathcal{D}_{4,t,4}^{(n+1)}$ will yield a nonzero conditional success probability:

$$P_{\mathrm{c},4} = \sum_{\mathbf{y}^{(n)} \in \mathcal{D}_{4,t,2}^{(n)}} P_{Y|X}^{n+1}\left([\mathbf{y}^{(n)}\ 1] \,\middle|\, [\mathbf{1}^{(n)}\ 1]\right) \cdot (x_{4,n+1} - x_{2,n+1})^+ \tag{69}$$

$$= \sum_{d=0}^{t-1} \binom{t}{d} (1-\epsilon_1)^{t-d} \epsilon_1^{(n-t)+d}(1-\epsilon_1) \cdot (x_{4,n+1} - x_{2,n+1})^+ \tag{70}$$

$$= \epsilon_1^{(n-t)}\left(1-\epsilon_1^t\right)(1-\epsilon_1) \cdot (x_{4,n+1} - x_{2,n+1})^+ \tag{71}$$

$$= \left(\epsilon_1^{(n-t)} - \epsilon_1^n\right)(1-\epsilon_1) \cdot (x_{4,n+1} - x_{2,n+1})^+. \tag{72}$$

- $[\mathcal{D}_{4,t,3}^{(n)}\ 1]$: Again, only $\mathcal{D}_{4,t,4}^{(n+1)}$ will yield a nonzero conditional success probability:

$$P_{\mathrm{c},4} = \sum_{\mathbf{y}^{(n)} \in \mathcal{D}_{4,t,3}^{(n)}} P_{Y|X}^{n+1}\left([\mathbf{y}^{(n)}\ 1] \,\middle|\, [\mathbf{1}^{(n)}\ 1]\right) \cdot (x_{4,n+1} - x_{3,n+1})^+ \tag{73}$$

$$= \sum_{d=0}^{(n-t)-1} \binom{n-t}{d} (1-\epsilon_1)^{(n-t)-d} \epsilon_1^{t+d}(1-\epsilon_1) \cdot (x_{4,n+1} - x_{3,n+1})^+ \tag{74}$$

$$= \epsilon_1^{t}\left(1-\epsilon_1^{(n-t)}\right)(1-\epsilon_1) \cdot (x_{4,n+1} - x_{3,n+1})^+ \tag{75}$$

$$= \left(\epsilon_1^t - \epsilon_1^n\right)(1-\epsilon_1) \cdot (x_{4,n+1} - x_{3,n+1})^+. \tag{76}$$

From $\epsilon_1^t \geq \epsilon_1^{(n-t)} > \epsilon_1^n$, we can therefore now conclude that the best solution for the choice of $x_{i,n+1}$ yielding the largest increase in success probability in (66), (67),

(68), (72), and (76) is as follows:

$$\begin{cases} x_{2,n+1} - x_{1,n+1} = 1 \\ x_{4,n+1} - x_{2,n+1} = 0 \\ x_{4,n+1} - x_{3,n+1} = 1 \end{cases} \quad \Longrightarrow \quad \begin{cases} x_{1,n+1} = 0 \\ x_{2,n+1} = 1 \\ x_{3,n+1} = 0 \\ x_{4,n+1} = 1 \end{cases} \tag{77}$$

This will cause an increase of

$$\epsilon_1^t(1-\epsilon_1) + (\epsilon_1^t - \epsilon_1^n)(1-\epsilon_1). \tag{78}$$

Note that for n even with $t = \frac{n}{2}$, adding the column (47) to the code $\mathcal{C}_{4,\frac{n}{2}}^{(n)}$ will result in a code that is equivalent to $\mathcal{C}_{4,\lfloor\frac{n+1}{2}\rfloor}^{(n+1)}$ by just exchanging the roles of the second and third codeword and re-order the columns.

For n odd with $t = \lfloor\frac{n}{2}\rfloor$, adding the column (47) to the code $\mathcal{C}_{4,\lfloor\frac{n}{2}\rfloor}^{(n)}$ results in $\mathcal{C}_{4,\frac{n+1}{2}}^{(n+1)}$. □

Corollary 14. *Fix $t \triangleq \lfloor\frac{n}{2}\rfloor$. Whenever there are three hypotheses $\mathcal{M} = 3$, the codebook $\mathcal{C}_{3,t}^{(n)}$ consisting of $n-t$ columns*

$$\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \tag{79}$$

and t columns arbitrarily chosen from

$$\left\{ \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \right\} \tag{80}$$

is optimal on the Z-channel. In particular, the success probability of this optimal code is

$$\begin{aligned} 3P_{\mathrm{c}}(\mathcal{C}_{3,t}^{(n)}) &= 1 + \sum_{d=0}^{t-1} \binom{t}{d} (1-\epsilon_1)^{t-d} \cdot \epsilon_1^d \\ &\quad + \sum_{d=0}^{n-1} \left[\binom{n}{d} - \binom{t}{d-(n-t)} \right] (1-\epsilon_1)^{n-d} \cdot \epsilon_1^d \qquad (81) \\ &= 1 + \sum_{d=0}^{t-1} \binom{t}{d} (1-\epsilon_1)^{t-d} \epsilon_1^d + \sum_{d=0}^{(n-t)-1} \binom{n-t}{d} (1-\epsilon_1)^{(n-t)-d} \cdot \epsilon_1^d. \qquad (82) \end{aligned}$$

Proof. This can be proved by the same argument as used in Theorem 12. We observe that

$$\begin{pmatrix} 0 & 0 \\ 0 & 1 \\ 1 & 1 \end{pmatrix} \equiv \begin{pmatrix} 0 & 0 \\ 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{83}$$

are optimal codebooks for $n = 2$. An optimal way of extending these codes is then to add the following columns

$$\begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \text{ or } \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}. \tag{84}$$

□

Corollary 15. *Whenever there are two hypotheses $\mathcal{M} = 2$, the optimal codebook for the Z-channel is the flip-flop codebook of type* 0.

Proof. Omitted. □

Now we go back to the analysis of the optimal code on BAC for $\mathcal{M} = 2$.

4.3 Optimal Decision Rule on BAC for $\mathcal{M} = 2$

In any system with only two possible messages the optimal ML receiver can easily be described by the *log likelihood ratio (LLR)*:

$$\mathrm{LLR}(\mathbf{y}) \triangleq \log\left(\frac{P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y}|\mathbf{x}_1)}{P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y}|\mathbf{x}_2)}\right). \tag{85}$$

If $\mathrm{LLR}(\mathbf{y}) > 0$, then the receiver decides for 1, while if $\mathrm{LLR}(\mathbf{y}) < 0$, it decides for 2. In the situation of $\mathrm{LLR}(\mathbf{y}) = 0$, both decisions are equally good.

In the situation of a flip-flop code of type t, $\mathcal{C}_{2,t}^{(n)}$, the LLR is given as

$$\mathrm{LLR}_t^{(n)}(\epsilon_0, \epsilon_1, d) \triangleq (t-d)\log\left(\frac{1-\epsilon_1}{\epsilon_0}\right) + (n-t-d)\log\left(\frac{1-\epsilon_0}{\epsilon_1}\right), \tag{86}$$

where d is defined to be the Hamming distance between the received vector and the ***first*** codeword:

$$d \triangleq d_{\mathrm{H}}(\mathbf{x}_1, \mathbf{y}). \tag{87}$$

Note that $0 \le d \le n$ depends on the received vector, while t and n are code parameters, and ϵ_0 and ϵ_1 are channel parameters.

Hence, the optimal decision rule can be expressed in terms of d.

Proposition 16. *We list some properties of* $\mathrm{LLR}_t^{(n)}(\epsilon_0, \epsilon_1, d)$*:*

1. *If* $\epsilon_0 + \epsilon_1 = 1$*, then* $\mathrm{LLR}_t^{(n)}(\epsilon_0, \epsilon_1, d) = 0$ *for all* d*.*
2. $\mathrm{LLR}_t^{(n)}(\epsilon_0, \epsilon_1, d)$ *is a decreasing function in* d*:*

$$\mathrm{LLR}_t^{(n)}(\epsilon_0, \epsilon_1, d) \ge \mathrm{LLR}_t^{(n)}(\epsilon_0, \epsilon_1, d+1), \quad \forall\, 0 \le d \le n-1. \tag{88}$$

3. *For* $d \le t$ *and* $d > \left\lfloor \frac{n}{2} \right\rfloor$ *the* $\mathrm{LLR}_t^{(n)}$ *is always larger or smaller than zero, respectively:*

$$\mathrm{LLR}_t^{(n)}(\epsilon_0, \epsilon_1, d) \begin{cases} \ge 0 & \text{for } 0 \le d \le t, \\ \lesseqgtr 0 & \text{for } t < d \le \left\lfloor \frac{n}{2} \right\rfloor, \text{ depending on } \epsilon_0,\, \epsilon_1, \\ \le 0 & \text{for } \left\lfloor \frac{n}{2} \right\rfloor < d \le n. \end{cases} \tag{89}$$

4. $\mathrm{LLR}_t^{(n)}(\epsilon_0, \epsilon_1, d)$ *is an increasing function in* n*, when we fix* d*,* ϵ_0*, and* ϵ_1*.*
5. $\mathrm{LLR}_t^{(n)}(\epsilon_0, \epsilon_1, d)$ *is an increasing function in* t *when we fix* n*,* d*,* ϵ_0*, and* ϵ_1*.*
6. *For* $0 \le d \le n-1$*,*

$$\mathrm{LLR}_t^{(n+1)}(\epsilon_0, \epsilon_1, d+1) < \mathrm{LLR}_t^{(n)}(\epsilon_0, \epsilon_1, d). \tag{90}$$

Proof. Omitted. □

From these properties we immediately obtain an interesting result about the optimal decision rule.

Proposition 17 (Optimal Decision Rule has a Threshold). *For a fixed flip-flop code $\mathcal{C}_{2,t}^{(n)}$ and a fixed BAC $(\epsilon_0, \epsilon_1) \in \Omega$, there exists a* threshold ℓ, $t \leq \ell \leq \left\lfloor \frac{n-1}{2} \right\rfloor$, *such that the optimal ML decision rule can be stated as*

$$g(\mathbf{y}) = \begin{cases} 1 & \text{if } 0 \leq d \leq \ell, \\ 2 & \text{if } \ell + 1 \leq d \leq n. \end{cases} \tag{91}$$

The threshold ℓ depends on (ϵ_0, ϵ_1), but similar channels will usually have the same threshold. We define the region of channel parameters with identical threshold as follows:

$$\Omega_{\ell,t}^{(n)} \triangleq \left\{ (\epsilon_0, \epsilon_1) \,\middle|\, \mathrm{LLR}_t^{(n)}(\epsilon_0, \epsilon_1, \ell) \geq 0 \right\} \bigcap \left\{ (\epsilon_0, \epsilon_1) \,\middle|\, \mathrm{LLR}_t^{(n)}(\epsilon_0, \epsilon_1, \ell + 1) \leq 0 \right\}. \tag{92}$$

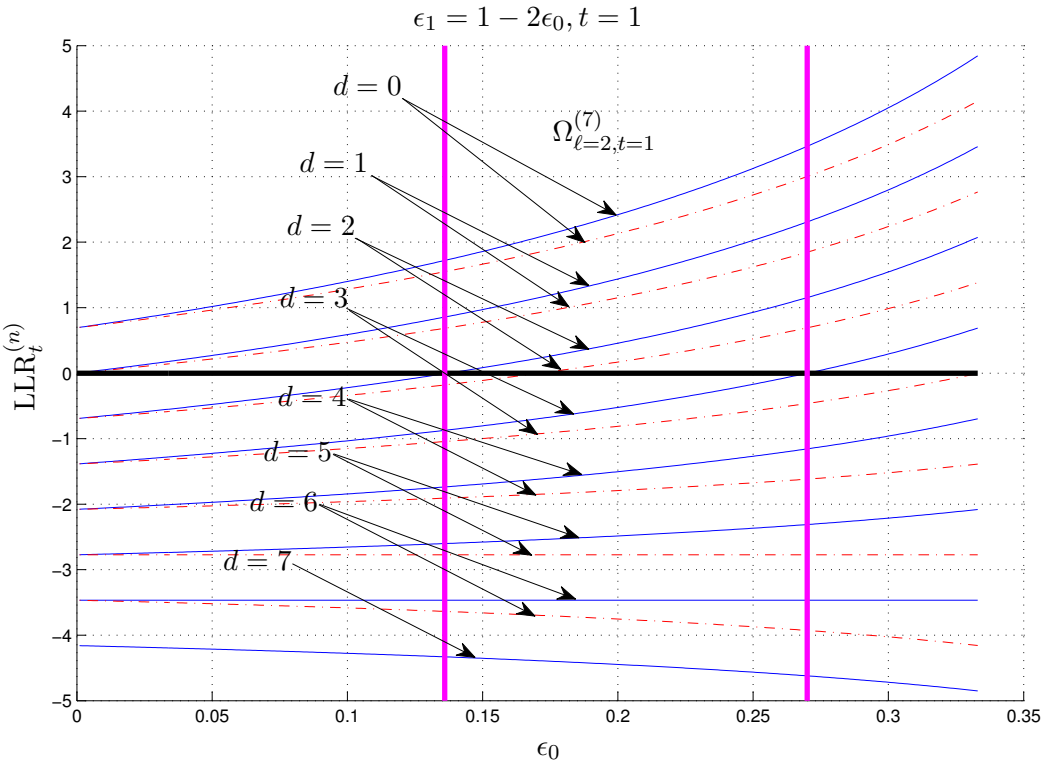

Figure 6: The log likelihood function depicted as a function of (ϵ_0, ϵ_1) for different values of d. To simplify the plot, only ϵ_0 is depicted with ϵ_1 being a fixed function of ϵ_0. The solid blue lines depict the case $n = 7$, the dashed red lines $n = 6$. The code is fixed to be $t = 1$. We see that for $n = 7$ and $\epsilon_0 \in [0.136, 0.270]$ the threshold is $\ell = 2$.

In Figure 6 an example of this threshold behavior is shown. For $\epsilon_0 \in [0.136, 0.270]$ we see that $\mathrm{LLR}_1^{(7)}(\epsilon_0, 1-2\epsilon_0, d) \geq 0$ for $d = 0$, $d = 1$, and $d = 2$, while $\mathrm{LLR}_1^{(7)}(\epsilon_0, 1-2\epsilon_0, d) < 0$ for $d \geq 3$. Hence, $\ell = 2$.

4.4 Optimal Codes for a Fixed Decision Rule on BAC for $\mathcal{M} = 2$

Our original goal was to find the optimal code for a given channel (ϵ_0, ϵ_1). This now corresponds to finding an optimal t. Unfortunately, this still is difficult because the changes between the different regions in Figure 5 are caused by two different effects: either the optimal code $\mathcal{C}_{2,t}^{(n)}$ remains fixed, but the threshold ℓ changes, or the optimal choice of t changes. Hence, we have two different optimization problems: finding the optimal decision rule for a given code (i.e., the optimal threshold ℓ) and finding the optimal code for a given decision rule (i.e., the optimal t). To gain a clearer picture, we will next concentrate on the second optimization only: we fix a decision rule, i.e., we fix a threshold ℓ irrespective of t or (ϵ_0, ϵ_1), and then try to find the optimal code t.

The following lemma investigates the error probability of two flip-flop codes of type t and $t+1$, respectively, for a fixed decision rule ℓ.

Lemma 18. *Fix a blocklength n, a channel $(\epsilon_0, \epsilon_1) \in \Omega$, and a decision rule threshold ℓ. Then for any integer t, $0 \leq t \leq \lfloor \frac{n}{2} \rfloor$, the roots of*

$$2P_{\mathrm{e}}(\mathcal{C}_{2,t}^{(n)})_\ell - 2P_{\mathrm{e}}(\mathcal{C}_{2,t+1}^{(n)})_\ell \tag{93}$$

are identical to the roots of

$$\mathrm{LLR}_t^{(n-1)}\left(\epsilon_0, \epsilon_1, d^{(n-1)} = \ell\right). \tag{94}$$

Moreover, for a fixed ϵ_0, there exists at most one $\epsilon_1 \leq \frac{1}{2}$ such that (93) *equals to zero; and for a fixed $\epsilon_1 \leq \frac{1}{2}$, there exists at most one ϵ_0 such that* (93) *equals to zero.*

Proof. See Appendix B. □

From Proposition 16 we know that $\mathrm{LLR}_t^{(n-1)}(\epsilon_0, \epsilon_1, d)$ has at most one root. Therefore, we can now easily state some conditions on t such that $\mathcal{C}_{2,t}^{(n)}$ is optimal.

Theorem 19. *Fix blocklength n. Under a particular fixed decision rule ℓ, the flip-flop codebooks of type t is optimal if (ϵ_0, ϵ_1) belong to*

$$\left\{(\epsilon_0, \epsilon_1) \;\middle|\; \mathrm{LLR}_t^{(n-1)}(\epsilon_0, \epsilon_1, \ell) > 0 \wedge \mathrm{LLR}_{t-1}^{(n-1)}(\epsilon_0, \epsilon_1, \ell) < 0\right\}. \tag{95}$$

If the region is empty, then t is not optimal for any channel.

Proof. See Appendix B. □

Now we have the exact associated region of channels of an optimal flip-flop code of type t. It says that while $\epsilon_0 \leq \min\{\epsilon_1, 1-\epsilon_1\}$, the error probability formulas between t and $t+1$ have at most one crossing point as ϵ_0 increases or ϵ_1 decreases. For an illustration see Figure 7.

Example 20 (Applcation of Theorem 19)**.** We will now illustrate Theorem 19 by an example. Fix $n = 7$, $\ell^{(n)} = 2$, $\epsilon_1 = 0.5$, and let ϵ_0 increase. See Figure 8.

Starting with $t = 3$, we check that

$$\mathrm{LLR}_2^{(6)}(\epsilon_0, \epsilon_1, 2) > 0, \tag{96}$$

for all (ϵ_0, ϵ_1), *i.e.*, $P_{\mathrm{e}}(\mathcal{C}_{2,2}^{(7)}) < P_{\mathrm{e}}(\mathcal{C}_{2,3}^{(7)})$.

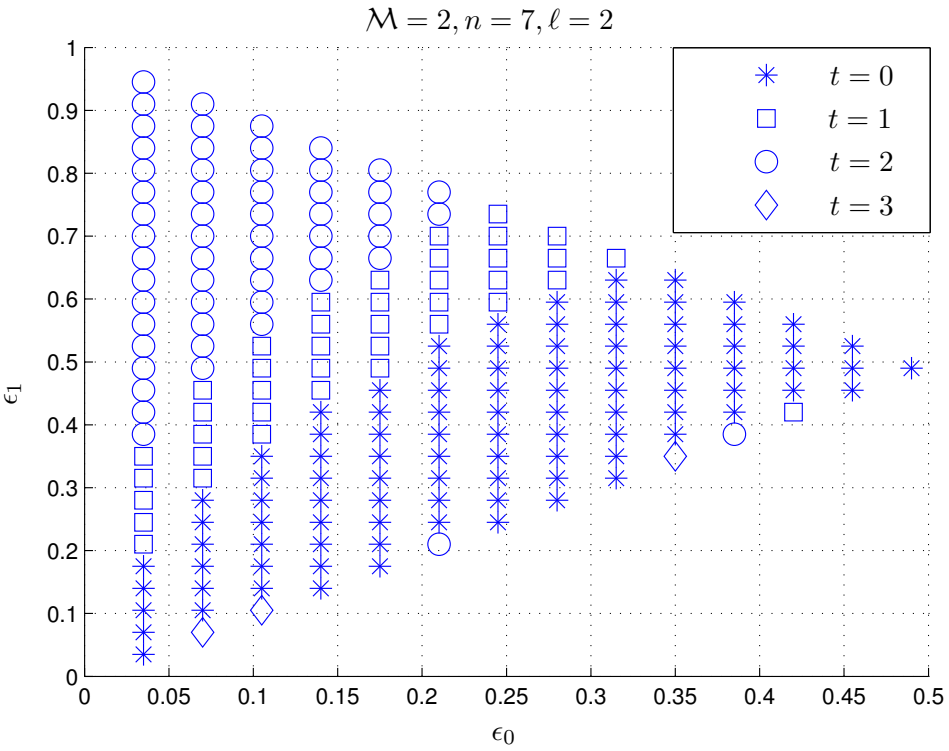

Figure 7: Optimal codebooks on a BAC for a fixed decision rule: for all possible (ϵ_0, ϵ_1) this plot shows the optimal choice of the code parameter t. The blocklength is $n = 7$ and the decision rule is $\ell = 2$.

Next, choose $t = 2$:

$$\mathrm{LLR}_1^{(6)}(\epsilon_0, \epsilon_1, 2) < 0 \tag{97}$$

for small ϵ_0, *i.e.*, the code $\mathcal{C}_{2,2}^{(7)}$ is optimal for those ϵ_0. When increasing ϵ_0 further, as soon as $\mathrm{LLR}_1^{(6)}(\epsilon_0, \epsilon_1, 2) = 0$, there is a change again and we choose $t = 1$. Finally, the last change happens at the root of $\mathrm{LLR}_0^{(6)}(\epsilon_0, \epsilon_1, 2) = 0$.

So there are three optimal codes in the region of Ω:

- $t = 2$ is optimal in $\left\{\epsilon_0 \,\middle|\, \mathrm{LLR}_2^{(6)}(\epsilon_0, \epsilon_1, 2) > 0 \wedge \mathrm{LLR}_1^{(6)}(\epsilon_0, \epsilon_1, 2) < 0\right\}$;
- $t = 1$ is optimal in $\left\{\epsilon_0 \,\middle|\, \mathrm{LLR}_1^{(6)}(\epsilon_0, \epsilon_1, 2) > 0 \wedge \mathrm{LLR}_0^{(6)}(\epsilon_0, \epsilon_1, 2) < 0\right\}$;
- $t = 0$ is optimal in $\left\{\epsilon_0 \,\middle|\, \mathrm{LLR}_0^{(6)}(\epsilon_0, \epsilon_1, 2) > 0\right\}$.

5 Discussion & Conclusion

We have investigated very short block-codes with two messages on the most general binary channel, the *binary asymmetric channel* (BAC). We have shown that in contrast to capacity that always can be achieved with linear codes, the best codes in the sense that they achieve the smallest average probability of error for a fixed blocklength, often are not linear.

We have proven that in the case of only two messages $\mathcal{M} = 2$, the optimal codes must be flip-flop codes of type t, where the optimal t depends on the channel and

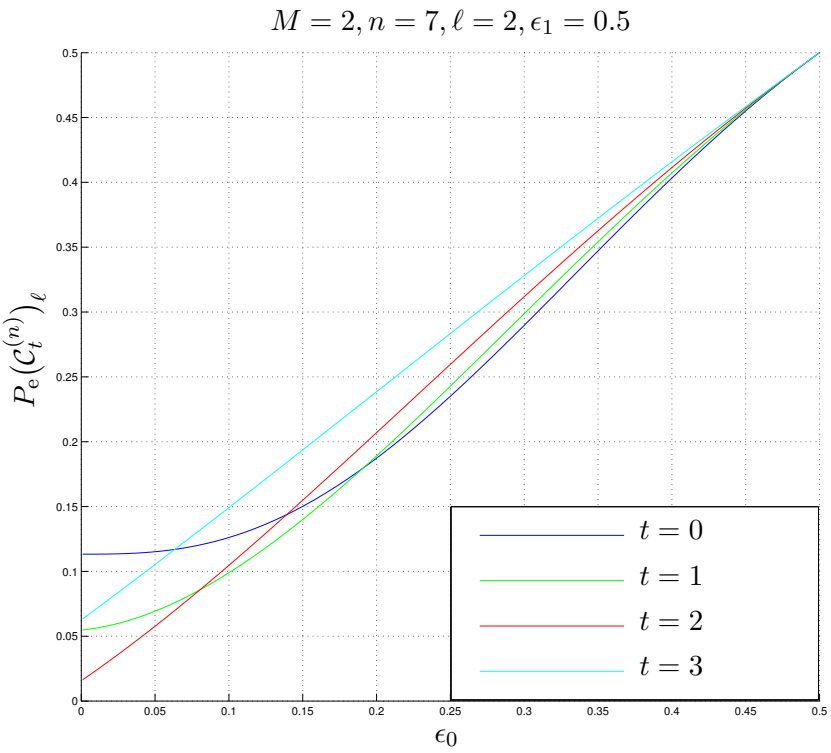

Figure 8: The error probability of all possible flip-flop codes $\mathcal{C}_t^{(n)}$ as a function of the channel parameter ϵ_0. The blocklength is chosen to be $n = 7$, and $\epsilon_1 = \frac{1}{2}$ is fixed. The decision rule is fixed to $\ell = 2$. For a particular ϵ_0, the optimal code is the one with the smallest error probability value.

the blocklength. We have then investigated the optimal decision rule and proven that it is a threshold rule.

In the special case of a Z-channel, we have shown that the optimal codes are two-pair flip-flop codes for the case of $\mathcal{M} = 4$, and derivatives of it for $\mathcal{M} = 3$.

The derivation of the optimal coding scheme is difficult because two independent effects interfere with each other: the optimal choice of the code t for a fixed decision rule ℓ, and the optimal choice of the decision rule ℓ for a fixed code t.

References

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

A Appendix: Derivation of Proposition 9

Assume that the optimal code for blocklength n is not a flip-flop code. Then the code has a number m of positions where both codewords have the same symbol. The optimal decoder will ignore these m positions completely. Hence, the performance of this code will be identical to a flip-flip code of length $n - m$.

We therefore only need to show that increasing n will always allow us to find a new flip-flop code with a better performance. In other words, Proposition 9 is proven once we have shown that

$$P_{\mathrm{e}}\big(\mathcal{C}_{2,t}^{(n-1)}\big) \geq \max\left\{P_{\mathrm{e}}\big(\mathcal{C}_{2,t}^{(n)}\big), P_{\mathrm{e}}\big(\mathcal{C}_{2,t+1}^{(n)}\big)\right\}. \tag{98}$$

Here we have used the following notation:

$$\mathcal{C}_{2,t}^{(n-1)} = \begin{pmatrix} \mathbf{x}^{(n-1)} \\ \bar{\mathbf{x}}^{(n-1)} \end{pmatrix} \tag{99}$$

is a length-$(n-1)$ flip-flop code of some type t, and

$$\mathcal{C}_{2,t}^{(n)} = \begin{pmatrix} [\mathbf{x}^{(n-1)}\, 0] \\ [\bar{\mathbf{x}}^{(n-1)}\, 1] \end{pmatrix}, \quad \mathcal{C}_{2,t+1}^{(n)} = \begin{pmatrix} [\mathbf{x}^{(n-1)}\, 1] \\ [\bar{\mathbf{x}}^{(n-1)}\, 0] \end{pmatrix} \tag{100}$$

are two length-n flip-flop codes derived from $\mathcal{C}_{2,t}^{(n-1)}$.

As shown in Proposition 17, the optimal decision rule for any flip-flop code is a threshold rule with some threshold ℓ: the decision rule for received $\mathbf{y}$ only depends on d such that

$$g(\mathbf{y}) = \begin{cases} \mathbf{x} & \text{if } 0 \leq d \leq \ell, \\ \bar{\mathbf{x}} & \text{if } \ell + 1 \leq d \leq n, \end{cases} \tag{101}$$

where we use $g(\cdot)$ to denote the ML decoding rule.

The threshold satisfies $0 \leq \ell \leq \lfloor \frac{n-1}{2} \rfloor$. Note that when $\ell = \lfloor \frac{n-1}{2} \rfloor$, the decision rule is equivalent to a *majority rule*. Also note that when n is even and $d = \frac{n}{2}$, the decisions for $\mathbf{x}$ and $\bar{\mathbf{x}}$ are equally likely, *i.e.*, without loss of generality we then always decode to $\bar{\mathbf{x}}$.

So let the threshold for $\mathcal{C}_{2,t}^{(n-1)}$ be $\ell^{(n-1)}$. We will now argue that the threshold for $\mathcal{C}_{2,t}^{(n)}$ and $\mathcal{C}_{2,t+1}^{(n)}$ according to (100) must satisfy

$$\ell^{(n-1)} \leq \ell^{(n)} \leq \ell^{(n-1)} + 1. \tag{102}$$

Consider firstly the code $\mathcal{C}_{2,t}^{(n)}$ and assume by contradiction for the moment that $\ell^{(n)} < \ell^{(n-1)}$. Then pick a received $\mathbf{y}^{(n-1)}$ with $d^{(n-1)} = \ell^{(n-1)}$ that (for the code $\mathcal{C}_{2,t}^{(n-1)}$) is decoded to $\mathbf{x}^{(n-1)}$. The received length-n vector $\mathbf{y}^{(n)} = [\mathbf{y}^{(n-1)}\, 0]$ has $d^{(n)} = \ell^{(n-1)} > \ell^{(n)}$, *i.e.*, it will be now decoded to $\bar{\mathbf{x}}^{(n)}$. This however is a contradiction to the assumption that the ML decision for the code $\mathcal{C}_{2,t}^{(n-1)}$ was $\mathbf{x}^{(n-1)}$.

Secondly, again considering code $\mathcal{C}_{2,t}^{(n)}$, assume by contradiction that $\ell^{(n)} > \ell^{(n-1)} + 1$. Pick a received $\mathbf{y}^{(n-1)}$ with $d^{(n-1)} = \ell^{(n-1)} + 1$ that (for the code $\mathcal{C}_{2,t}^{(n-1)}$) is decoded to $\bar{\mathbf{x}}^{(n-1)}$. The received length-n vector $\mathbf{y}^{(n)} = [\mathbf{y}^{(n-1)}\, 1]$ has $d^{(n)} = \ell^{(n-1)} + 2 < \ell^{(n)} + 1$, *i.e.*, it will be now decoded to $\mathbf{x}^{(n)}$. This however is a contradiction to the assumption that the ML decision for the code $\mathcal{C}_{2,t}^{(n-1)}$ was $\bar{\mathbf{x}}^{(n-1)}$.

The same arguments also hold for the other code $\mathcal{C}_{2,t+1}^{(n)}$. Hence, we see that there are only two possible changes with respect to the decoding rule to be considered.

We will next use this fact to prove that $P_{\mathrm{e}}\big(\mathcal{C}_{2,t}^{(n-1)}\big) \geq P_{\mathrm{e}}\big(\mathcal{C}_{2,t}^{(n)}\big)$.

The error probability is given by

$$P_{\mathrm{e}} = \frac{1}{2} \sum_{\substack{\mathbf{y} \\ g(\mathbf{y})=\bar{\mathbf{x}}}} P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y}|\mathbf{x}) + \frac{1}{2} \sum_{\substack{\mathbf{y} \\ g(\mathbf{y})=\mathbf{x}}} P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y}|\bar{\mathbf{x}}). \tag{103}$$

For $\mathcal{C}_{2,t}^{(n-1)}$ this can be written as follows:

$$\begin{aligned}
2P_{\mathrm{e}}\big(\mathcal{C}_{2,t}^{(n-1)}\big) = & \sum_{\substack{\mathbf{y}^{(n-1)} \\ \ell^{(n-1)}+1 \leq d^{(n-1)} \leq n-1}} P_{Y|X}^{n-1}\big(\mathbf{y}^{(n-1)} \,\big|\, \mathbf{x}^{(n-1)}\big) \\
& + \sum_{\substack{\mathbf{y}^{(n-1)} \\ 0 \leq d^{(n-1)} \leq \ell^{(n-1)}}} P_{Y|X}^{n-1}\big(\mathbf{y}^{(n-1)} \,\big|\, \bar{\mathbf{x}}^{(n-1)}\big) \qquad (104) \\
= & \sum_{\substack{\mathbf{y}^{(n-1)} \\ \ell^{(n-1)}+1 \leq d^{(n-1)} \leq n-1}} P_{Y|X}^{n-1}\big(\mathbf{y}^{(n-1)} \,\big|\, \mathbf{x}^{(n-1)}\big) P_{Y|X}(1|0) \\
& + \sum_{\substack{\mathbf{y}^{(n-1)} \\ \ell^{(n-1)}+1 \leq d^{(n-1)} \leq n-1}} P_{Y|X}^{n-1}\big(\mathbf{y}^{(n-1)} \,\big|\, \mathbf{x}^{(n-1)}\big) P_{Y|X}(0|0) \\
& + \sum_{\substack{\mathbf{y}^{(n-1)} \\ 0 \leq d^{(n-1)} \leq \ell^{(n-1)}}} P_{Y|X}^{n-1}\big(\mathbf{y}^{(n-1)} \,\big|\, \bar{\mathbf{x}}^{(n-1)}\big) P_{Y|X}(1|1) \\
& + \sum_{\substack{\mathbf{y}^{(n-1)} \\ 0 \leq d^{(n-1)} \leq \ell^{(n-1)}}} P_{Y|X}^{n-1}\big(\mathbf{y}^{(n-1)} \,\big|\, \bar{\mathbf{x}}^{(n-1)}\big) P_{Y|X}(0|1) \qquad (105) \\
= & \sum_{\substack{\mathbf{y}^{(n-1)} \\ \ell^{(n-1)}+2 \leq d^{(n)} \leq n}} P_{Y|X}^{n}\big([\mathbf{y}^{(n-1)}\, 1] \,\big|\, \mathbf{x}^{(n)}\big) \\
& + \sum_{\substack{\mathbf{y}^{(n-1)} \\ \ell^{(n-1)}+1 \leq d^{(n)} \leq n-1}} P_{Y|X}^{n}\big([\mathbf{y}^{(n-1)}\, 0] \,\big|\, \mathbf{x}^{(n)}\big) \\
& + \sum_{\substack{\mathbf{y}^{(n-1)} \\ 1 \leq d^{(n)} \leq \ell^{(n-1)}+1}} P_{Y|X}^{n}\big([\mathbf{y}^{(n-1)}\, 1] \,\big|\, \bar{\mathbf{x}}^{(n)}\big)
\end{aligned}$$

$$+ \sum_{\substack{\mathbf{y}^{(n-1)} \\ 0 \le d^{(n)} \le \ell^{(n-1)}}} P_{Y|X}^n\big([\mathbf{y}^{(n-1)}\, 0] \,\big|\, \bar{\mathbf{x}}^{(n)}\big). \tag{106}$$

Here, in (105) we use the fact that $P_{Y|X}(1|0) + P_{Y|X}(0|0) = 1$ and $P_{Y|X}(1|1) + P_{Y|X}(0|1) = 1$; and in (106) we combine the terms together using the definition of $\mathcal{C}_{2,t}^{(n)}$ according to (24).

We can now distinguish the two cases (102):

(i) If the decision rule is unchanged, *i.e.*, $\ell^{(n)} = \ell^{(n-1)}$, we only need to take care of the third summation in (106) that contains some terms that will now be decoded differently:

$$\begin{aligned}
&\sum_{\substack{\mathbf{y}^{(n-1)} \\ 1 \le d^{(n)} \le \ell^{(n-1)}+1}} P_{Y|X}^n\big([\mathbf{y}^{(n-1)}\, 1] \,\big|\, \bar{\mathbf{x}}^{(n)}\big) \\
&\quad = \sum_{\substack{\mathbf{y}^{(n-1)} \\ d^{(n)} = \ell^{(n-1)}+1}} P_{Y|X}^n\big([\mathbf{y}^{(n-1)}\, 1] \,\big|\, \bar{\mathbf{x}}^{(n)}\big) \\
&\qquad + \sum_{\substack{\mathbf{y}^{(n-1)} \\ 1 \le d^{(n)} \le \ell^{(n-1)}}} P_{Y|X}^n\big([\mathbf{y}^{(n-1)}\, 1] \,\big|\, \bar{\mathbf{x}}^{(n)}\big).
\end{aligned} \tag{107}$$

Since we have assumed that $\ell^{(n)} = \ell^{(n-1)}$, we know that for all $\mathbf{y}^{(n-1)}$ with $d^{(n-1)} = \ell^{(n-1)}$ the length-n received vector $[\mathbf{y}^{(n-1)}\, 1]$ has $d^{(n)} = \ell^{(n-1)} + 1 = \ell^{(n)} + 1$ and will be decoded to $\bar{\mathbf{x}}^{(n)}$. Hence we must have

$$\frac{P_{Y|X}^n\big([\mathbf{y}^{(n-1)}\, 1] \,\big|\, \mathbf{x}^{(n)}\big)}{P_{Y|X}^n\big([\mathbf{y}^{(n-1)}\, 1] \,\big|\, \bar{\mathbf{x}}^{(n)}\big)} \le 1. \tag{108}$$

Hence, we have

$$\begin{aligned}
2P_{\mathrm{e}}\big(\mathcal{C}_{2,t}^{(n-1)}\big) \ge &\sum_{\substack{\mathbf{y}^{(n-1)} \\ \ell^{(n-1)}+2 \le d^{(n)} \le n}} P_{Y|X}^n\big([\mathbf{y}^{(n-1)}\, 1] \,\big|\, \mathbf{x}^{(n)}\big) \\
&+ \sum_{\substack{\mathbf{y}^{(n-1)} \\ \ell^{(n-1)}+1 \le d^{(n)} \le n-1}} P_{Y|X}^n\big([\mathbf{y}^{(n-1)}\, 0] \,\big|\, \mathbf{x}^{(n)}\big) \\
&+ \sum_{\substack{\mathbf{y}^{(n-1)} \\ d^{(n)} = \ell^{(n-1)}+1}} P_{Y|X}^n\big([\mathbf{y}^{(n-1)}\, 1] \,\big|\, \mathbf{x}^{(n)}\big) \\
&+ \sum_{\substack{\mathbf{y}^{(n-1)} \\ 1 \le d^{(n)} \le \ell^{(n-1)}}} P_{Y|X}^n\big([\mathbf{y}^{(n-1)}\, 1] \,\big|\, \bar{\mathbf{x}}^{(n)}\big) \\
&+ \sum_{\substack{\mathbf{y}^{(n-1)} \\ 0 \le d^{(n)} \le \ell^{(n-1)}}} P_{Y|X}^n\big([\mathbf{y}^{(n-1)}\, 0] \,\big|\, \bar{\mathbf{x}}^{(n)}\big)
\end{aligned} \tag{109}$$

$$\begin{aligned}
= &\sum_{\substack{\mathbf{y}^{(n)} \\ \ell^{(n-1)}+1 \le d^{(n)} \le n}} P_{Y|X}^n\big(\mathbf{y}^{(n)} \,\big|\, \mathbf{x}^{(n)}\big) \\
&+ \sum_{\substack{\mathbf{y}^{(n)} \\ 0 \le d^{(n)} \le \ell^{(n-1)}}} P_{Y|X}^n\big(\mathbf{y}^{(n)} \,\big|\, \bar{\mathbf{x}}^{(n)}\big)
\end{aligned} \tag{110}$$

$$= 2P_{\mathrm{e}}\big(\mathcal{C}_{2,t}^{(n)}\big). \tag{111}$$

(ii) If the decision rule is changed such that $\ell^{(n)} = \ell^{(n-1)} + 1$, we need to take care of the second summation in (106) that contains some terms that will now be decoded differently:

$$\begin{aligned}
&\sum_{\substack{\mathbf{y}^{(n-1)} \\ \ell^{(n-1)}+1 \le d^{(n)} \le n-1}} P_{Y|X}^n\big([\mathbf{y}^{(n-1)}\, 0] \,\big|\, \mathbf{x}^{(n)}\big) \\
&\quad = \sum_{\substack{\mathbf{y}^{(n-1)} \\ d^{(n)} = \ell^{(n-1)}+1}} P_{Y|X}^n\big([\mathbf{y}^{(n-1)}\, 0] \,\big|\, \mathbf{x}^{(n)}\big) \\
&\qquad + \sum_{\substack{\mathbf{y}^{(n-1)} \\ \ell^{(n-1)}+2 \le d^{(n)} \le n-1}} P_{Y|X}^n\big([\mathbf{y}^{(n-1)}\, 0] \,\big|\, \mathbf{x}^{(n)}\big). \qquad (112)
\end{aligned}$$

Since we have assumed that $\ell^{(n)} = \ell^{(n-1)} + 1$, we know that for all $\mathbf{y}^{(n-1)}$ with $d^{(n-1)} = \ell^{(n-1)} + 1$ the length-n received vector $[\mathbf{y}^{(n-1)}\, 0]$ has $d^{(n)} = \ell^{(n-1)} + 1 = \ell^{(n)}$ and will be decoded to $\mathbf{x}^{(n)}$. Hence we must have

$$\frac{P_{Y|X}^n\big([\mathbf{y}^{(n-1)}\, 0] \,\big|\, \mathbf{x}^{(n)}\big)}{P_{Y|X}^n\big([\mathbf{y}^{(n-1)}\, 0] \,\big|\, \bar{\mathbf{x}}^{(n)}\big)} \ge 1. \qquad (113)$$

The rest of the argument now is analogous to case (i).

This proves that $P_{\mathrm{e}}\big(\mathcal{C}_{2,t}^{(n-1)}\big) \ge P_{\mathrm{e}}\big(\mathcal{C}_{2,t}^{(n)}\big)$. The remaining proof of $P_{\mathrm{e}}\big(\mathcal{C}_{2,t}^{(n-1)}\big) \ge P_{\mathrm{e}}\big(\mathcal{C}_{2,t+1}^{(n)}\big)$ is similar and omitted.

B Appendix: Proof of Lemma 18 and Theorem 19

We derive the the error probability expressions for $\mathcal{C}_{2,t}^{(n)}$ and $\mathcal{C}_{2,t+1}^{(n)}$ based on $\mathcal{C}_{2,t}^{(n-1)}$ by adding a column $(0\ 1)^{\mathsf{T}}$ or $(1\ 0)^{\mathsf{T}}$, respectively. Let the threshold for $\mathcal{C}_{2,t}^{(n-1)}$ be $\ell^{(n-1)}$. Then we know from (102) that $\ell \triangleq \ell^{(n)} = \ell^{(n-1)}$ or $\ell^{(n-1)} + 1$, depending on the particular values of n, t, ϵ_0, and ϵ_1. Let's first assume that $\ell = \ell^{(n-1)}$:

$$\begin{aligned}
2P_{\mathrm{e}}\big(\mathcal{C}_{2,t}^{(n)}\big)_{\ell=\ell^{(n-1)}} &= \sum_{\substack{\mathbf{y}^{(n-1)} \\ \ell^{(n-1)}+1 \le d^{(n-1)} \le n-1}} P_{Y|X}^n\big([\mathbf{y}^{(n-1)}\, 0] \,\big|\, [\mathbf{x}^{(n-1)}\, 0]\big) \\
&\quad + \sum_{\substack{\mathbf{y}^{(n-1)} \\ \ell^{(n-1)} \le d^{(n-1)} \le n-1}} P_{Y|X}^n\big([\mathbf{y}^{(n-1)}\, 1] \,\big|\, [\mathbf{x}^{(n-1)}\, 0]\big) \\
&\quad + \sum_{\substack{\mathbf{y}^{(n-1)} \\ 0 \le d^{(n-1)} \le \ell^{(n-1)}}} P_{Y|X}^n\big([\mathbf{y}^{(n-1)}\, 0] \,\big|\, [\bar{\mathbf{x}}^{(n-1)}\, 1]\big) \\
&\quad + \sum_{\substack{\mathbf{y}^{(n-1)} \\ 0 \le d^{(n-1)} \le \ell^{(n-1)}-1}} P_{Y|X}^n\big([\mathbf{y}^{(n-1)}\, 1] \,\big|\, [\bar{\mathbf{x}}^{(n-1)}\, 1]\big) \qquad (114) \\
&= \sum_{\substack{\mathbf{y}^{(n-1)} \\ \ell^{(n-1)}+1 \le d^{(n-1)} \le n-1}} P_{Y|X}^{n-1}\big(\mathbf{y}^{(n-1)} \,\big|\, \mathbf{x}^{(n-1)}\big)(1 - \epsilon_0 + \epsilon_0) \\
&\quad + \sum_{\substack{\mathbf{y}^{(n-1)} \\ d^{(n-1)} = \ell^{(n-1)}}} P_{Y|X}^{n-1}\big(\mathbf{y}^{(n-1)} \,\big|\, \mathbf{x}^{(n-1)}\big)\epsilon_0
\end{aligned}$$

$$+ \sum_{\substack{\mathbf{y}^{(n-1)} \\ 0 \le d^{(n-1)} \le \ell^{(n-1)}-1}} P_{Y|X}^{n-1}\big(\mathbf{y}^{(n-1)} \,\big|\, \bar{\mathbf{x}}^{(n-1)}\big)(\epsilon_1 + 1 - \epsilon_1)$$
$$+ \sum_{\substack{\mathbf{y}^{(n-1)} \\ d^{(n-1)} = \ell^{(n-1)}}} P_{Y|X}^{n-1}\big(\mathbf{y}^{(n-1)} \,\big|\, \bar{\mathbf{x}}^{(n-1)}\big)\epsilon_1 \tag{115}$$

and similarly

$$\begin{aligned}
2P_{\mathrm{e}}\big(\mathcal{C}_{2,t+1}^{(n)}\big)_{\ell=\ell^{(n-1)}} &= \sum_{\substack{\mathbf{y}^{(n-1)} \\ \ell^{(n-1)}+1 \le d^{(n-1)} \le n-1}} P_{Y|X}^{n}\big([\mathbf{y}^{(n-1)}\,1] \,\big|\, [\mathbf{x}^{(n-1)}\,1]\big) \\
&\quad + \sum_{\substack{\mathbf{y}^{(n-1)} \\ \ell^{(n-1)} \le d^{(n-1)} \le n-1}} P_{Y|X}^{n}\big([\mathbf{y}^{(n-1)}\,0] \,\big|\, [\mathbf{x}^{(n-1)}\,1]\big) \\
&\quad + \sum_{\substack{\mathbf{y}^{(n-1)} \\ 0 \le d^{(n-1)} \le \ell^{(n-1)}}} P_{Y|X}^{n}\big([\mathbf{y}^{(n-1)}\,1] \,\big|\, [\bar{\mathbf{x}}^{(n-1)}\,0]\big) \\
&\quad + \sum_{\substack{\mathbf{y}^{(n-1)} \\ 0 \le d^{(n-1)} \le \ell^{(n-1)}-1}} P_{Y|X}^{n}\big([\mathbf{y}^{(n-1)}\,0] \,\big|\, [\bar{\mathbf{x}}^{(n-1)}\,0]\big) \qquad (116) \\
&= \sum_{\substack{\mathbf{y}^{(n-1)} \\ \ell^{(n-1)}+1 \le d^{(n-1)} \le n-1}} P_{Y|X}^{n-1}\big(\mathbf{y}^{(n-1)} \,\big|\, \mathbf{x}^{(n-1)}\big)(1 - \epsilon_1 + \epsilon_1) \\
&\quad + \sum_{\substack{\mathbf{y}^{(n-1)} \\ d^{(n-1)} = \ell^{(n-1)}}} P_{Y|X}^{n-1}\big(\mathbf{y}^{(n-1)} \,\big|\, \mathbf{x}^{(n-1)}\big)\epsilon_1 \\
&\quad + \sum_{\substack{\mathbf{y}^{(n-1)} \\ 0 \le d^{(n-1)} \le \ell^{(n-1)}-1}} P_{Y|X}^{n-1}\big(\mathbf{y}^{(n-1)} \,\big|\, \bar{\mathbf{x}}^{(n-1)}\big)(\epsilon_0 + 1 - \epsilon_0) \\
&\quad + \sum_{\substack{\mathbf{y}^{(n-1)} \\ d^{(n-1)} = \ell^{(n-1)}}} P_{Y|X}^{n-1}\big(\mathbf{y}^{(n-1)} \,\big|\, \bar{\mathbf{x}}^{(n-1)}\big)\epsilon_0. \qquad (117)
\end{aligned}$$

Subtracting (117) from (115) yields

$$\begin{aligned}
&2P_{\mathrm{e}}\big(\mathcal{C}_{2,t}^{(n)}\big)_{\ell=\ell^{(n-1)}} - 2P_{\mathrm{e}}\big(\mathcal{C}_{2,t+1}^{(n)}\big)_{\ell=\ell^{(n-1)}} \\
&\quad = \sum_{\substack{\mathbf{y}^{(n-1)} \\ d^{(n-1)} = \ell^{(n-1)}}} P_{Y|X}^{n-1}\big(\mathbf{y}^{(n-1)} \,\big|\, \mathbf{x}^{(n-1)}\big)\epsilon_0 + \sum_{\substack{\mathbf{y}^{(n-1)} \\ d^{(n-1)} = \ell^{(n-1)}}} P_{Y|X}^{n-1}\big(\mathbf{y}^{(n-1)} \,\big|\, \bar{\mathbf{x}}^{(n-1)}\big)\epsilon_1 \\
&\qquad - \sum_{\substack{\mathbf{y}^{(n-1)} \\ d^{(n-1)} = \ell^{(n-1)}}} P_{Y|X}^{n-1}\big(\mathbf{y}^{(n-1)} \,\big|\, \mathbf{x}^{(n-1)}\big)\epsilon_1 - \sum_{\substack{\mathbf{y}^{(n-1)} \\ d^{(n-1)} = \ell^{(n-1)}}} P_{Y|X}^{n-1}\big(\mathbf{y}^{(n-1)} \,\big|\, \bar{\mathbf{x}}^{(n-1)}\big)\epsilon_0 \qquad (118) \\
&\quad = \sum_{\substack{\mathbf{y}^{(n-1)} \\ d^{(n-1)} = \ell^{(n-1)}}} \Big(P_{Y|X}^{n-1}\big(\mathbf{y}^{(n-1)} \,\big|\, \bar{\mathbf{x}}^{(n-1)}\big) - P_{Y|X}^{n-1}\big(\mathbf{y}^{(n-1)} \,\big|\, \mathbf{x}^{(n-1)}\big)\Big)(\epsilon_1 - \epsilon_0) \qquad (119) \\
&\quad = \sum_{\substack{\mathbf{y}^{(n-1)} \\ d^{(n-1)} = \ell^{(n-1)}}} P_{Y|X}^{n-1}\big(\mathbf{y}^{(n-1)} \,\big|\, \bar{\mathbf{x}}^{(n-1)}\big)\left(1 - \frac{P_{Y|X}^{n-1}\big(\mathbf{y}^{(n-1)} \,\big|\, \mathbf{x}^{(n-1)}\big)}{P_{Y|X}^{n-1}\big(\mathbf{y}^{(n-1)} \,\big|\, \bar{\mathbf{x}}^{(n-1)}\big)}\right)(\epsilon_1 - \epsilon_0) \qquad (120)
\end{aligned}$$

$$= \sum_{\substack{\mathbf{y}^{(n-1)} \\ d^{(n-1)}=\ell^{(n-1)}}} P_{Y|X}^{n-1}\big(\mathbf{y}^{(n-1)} \,\big|\, \bar{\mathbf{x}}^{(n-1)}\big) \left(1 - e^{\mathrm{LLR}_t^{(n-1)}\left(\epsilon_0,\epsilon_1,\ell^{(n-1)}\right)}\right)(\epsilon_1 - \epsilon_0) \tag{121}$$

$$= \left(1 - e^{\mathrm{LLR}_t^{(n-1)}\left(\epsilon_0,\epsilon_1,\ell^{(n-1)}\right)}\right)(\epsilon_1 - \epsilon_0) \sum_{\substack{\mathbf{y}^{(n-1)} \\ d^{(n-1)}=\ell^{(n-1)}}} P_{Y|X}^{n-1}\big(\mathbf{y}^{(n-1)} \,\big|\, \bar{\mathbf{x}}^{(n-1)}\big). \tag{122}$$

Similarly, we can derive this difference in the case when $\ell = \ell^{(n-1)} + 1$:

$$2P_{\mathrm{e}}\big(\mathcal{C}_{2,t}^{(n)}\big)_{\ell=\ell^{(n-1)}+1} - 2P_{\mathrm{e}}\big(\mathcal{C}_{2,t+1}^{(n)}\big)_{\ell=\ell^{(n-1)}+1}$$

$$= \sum_{\substack{\mathbf{y}^{(n-1)} \\ d^{(n-1)}=\ell^{(n-1)}+1}} \left(P_{Y|X}^{n-1}\big(\mathbf{y}^{(n-1)} \,\big|\, \bar{\mathbf{x}}^{(n-1)}\big) - P_{Y|X}^{n-1}\big(\mathbf{y}^{(n-1)} \,\big|\, \mathbf{x}^{(n-1)}\big)\right)(\epsilon_1 - \epsilon_0) \tag{123}$$

$$= \left(1 - e^{\mathrm{LLR}_t^{(n-1)}\left(\epsilon_0,\epsilon_1,\ell^{(n-1)}+1\right)}\right)(\epsilon_1 - \epsilon_0) \sum_{\substack{\mathbf{y}^{(n-1)} \\ d^{(n-1)}=\ell^{(n-1)}+1}} P_{Y|X}^{n-1}\big(\mathbf{y}^{(n-1)} \,\big|\, \bar{\mathbf{x}}^{(n-1)}\big). \tag{124}$$

Hence, we see that unless $\epsilon_0 = \epsilon_1$, in which case the difference is always zero, $2P_{\mathrm{e}}\big(\mathcal{C}_{2,t}^{(n)}\big)_\ell - 2P_{\mathrm{e}}\big(\mathcal{C}_{2,t+1}^{(n)}\big)_\ell$ can only be zero if

$$\mathrm{LLR}_t^{(n-1)}\left(\epsilon_0, \epsilon_1, \ell\right) = 0. \tag{125}$$

From the definition of the log likelihood ratio in (86) we see that if we fix ϵ_0, then there exists at most one ϵ_1 such that (125) is satisfied. The same is true if we fix ϵ_1 and search for an ϵ_0.

Moreover, note that if

$$\mathrm{LLR}_t^{(n-1)}\left(\epsilon_0, \epsilon_1, \ell\right) > 0, \tag{126}$$

then

$$P_{\mathrm{e}}\big(\mathcal{C}_{2,t}^{(n)}\big)_\ell < P_{\mathrm{e}}\big(\mathcal{C}_{2,t+1}^{(n)}\big)_\ell. \tag{127}$$

As we know from Proposition 16 that $\mathrm{LLR}_t^{(n-1)}\left(\epsilon_0, \epsilon_1, \ell\right)$ is increasing in t, this means that if both (126) and

$$\mathrm{LLR}_{t-1}^{(n-1)}\left(\epsilon_0, \epsilon_1, \ell\right) < 0 \tag{128}$$

are satisfied, the code $\mathcal{C}_{2,t}^{(n)}$ is optimal for the given channel (ϵ_0, ϵ_1) and blocklength n under the fixed decision rule ℓ.