On Ultra-Short Block-Codes on the Binary Asymmetric Channel

Po-Ning Chen, Hsuan-Yin Lin, and Stefan M. Moser
Department of Electrical Engineering
National Chiao Tung University
Hsinchu 30010, Taiwan
Email: qponing@mail.nctu.edu.tw, {lin.hsuanyin,stefan.moser}@ieee.org

***Abstract*—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 codes are optimal, however, depending on the blocklength and the channel parameters, not necessarily the linear flip code. Further it is shown that the optimal decoding rule is a threshold rule. Finally some fundamental dependencies of the best code on the channel are given.**

I. Introduction

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 channels and start with the simplest type of communication: a code with only two possible, equally likely messages.

II. Channel Model

The most general binary channel is a butterfly-channel with crossover probabilities that are not identical. In reference to the standard *binary symmetric channel (BSC)* we call this channel model *binary asymmetric channel (BAC)*. See Fig. 1

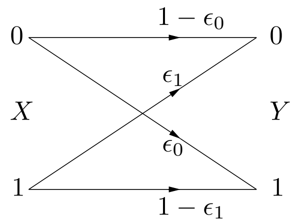

Fig. 1. The binary asymmetric channel (BAC).

for a graphical representation. 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:

$$0 \le \epsilon_0 \le \epsilon_1 \le 1, \tag{1}$$

$$\epsilon_0 \le 1 - \epsilon_1. \tag{2}$$

We have depicted the region of possible choices of the parameters ϵ_0 and ϵ_1 in Fig. 2. The region of interest given by (1) and (2) is denoted by Ω.

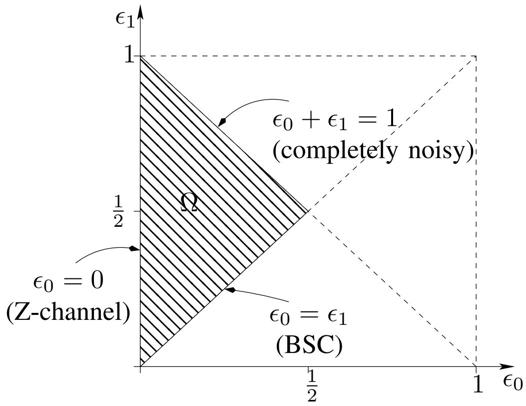

Fig. 2. Region of possible choices of the channel parameters ϵ_0 and ϵ_1 of a BAC. The shaded area corresponds to the area of interest according to (1) and (2).

This work has been supported by the National Science Council under NSC 97-2221-E-009-003-MY3.

III. Main Results

A. Optimal Codes

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

Definition 1: A code with two codewords is called **flip 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 code of type** t as follows: for every $t \in \left\{0, 1, \ldots, \left\lfloor \frac{n}{2} \right\rfloor\right\}$, we have

$$\mathcal{C}_t = \begin{pmatrix} \mathbf{x}_1 \\ \mathbf{x}_2 \end{pmatrix} \triangleq \begin{pmatrix} \mathbf{x} \\ \bar{\mathbf{x}} \end{pmatrix}, \tag{3}$$

where

$$\mathbf{x}_1 = \mathbf{x} \triangleq 00\cdots0\underbrace{11\cdots1}_{w_{\mathrm{H}}(\mathbf{x})=t}, \tag{4}$$

$$\mathbf{x}_2 = \bar{\mathbf{x}} \triangleq 11\cdots100\cdots0. \tag{5}$$

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 codes of type t to describe all possible flip codes.

We are now ready for the following result.

Proposition 2: Fix the blocklength n. Then, irrespective of the channel parameters ϵ_0 and ϵ_1, on a BAC there always exists a flip code of type t, $\mathcal{C}_t$, for some choice of $0 \leq t \leq \left\lfloor \frac{n}{2} \right\rfloor$ that is optimal in the sense that it minimizes the error probability.

We next would like to point out that the exact choice of t, however, is not obvious and depends strongly on n, ϵ_0, and ϵ_1. As an example the optimal choices of t are shown in Fig. 3 for $n = 5$. We see that depending on the channel parameters, the optimal value of t changes.

B. Optimal Decision Rule

In any system with only two possible messages the optimal *maximum likelihood (ML)* receiver can be easily described by the *log-likelihood ratio (LLR)*. In the situation of a flip code of type t, $\mathcal{C}_t$, the LLR is given as

$$\mathrm{LLR}_t^{(n)}(\epsilon_0, \epsilon_1, d) = (t-d)\log\left(\frac{1-\epsilon_1}{\epsilon_0}\right) + (n-t-d)\log\left(\frac{1-\epsilon_0}{\epsilon_1}\right), \tag{6}$$

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

$$d \triangleq d_{\mathrm{H}}(\mathbf{x}_1, \mathbf{y}). \tag{7}$$

Proposition 3 (Optimal Decision Rule has a Threshold): For a fixed flip code $\mathcal{C}_t^{(n)}$ 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 decision rule can be stated as

$$g(\mathbf{y}) = \begin{cases} 1 & \text{if } 0 \leq d \leq \ell, \\ 2 & \text{if } \ell + 1 \leq d \leq n. \end{cases} \tag{8}$$

The threshold ℓ depends on (ϵ_0, ϵ_1).

C. Optimal Codes for a Fixed Decision Rule

Theorem 4: Fix blocklength n. Under a particular *fixed decision rule* ℓ, the flip codebook of type t is optimal if (ϵ_0, ϵ_1) belongs to

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

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

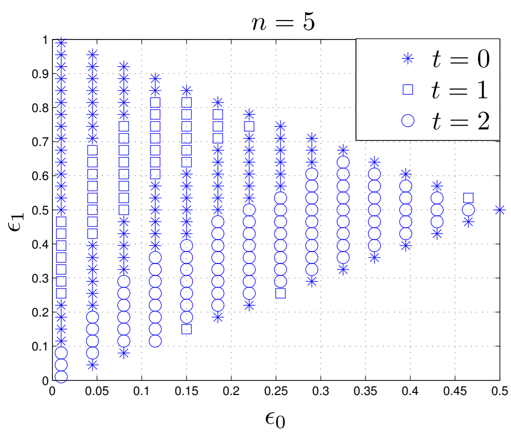

Fig. 3. Optimal codebooks on a BAC: the optimal choice of the parameter t for different values of ϵ_0 and ϵ_1 for a fixed blocklength $n = 5$.

IV. 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 codes of type t, where the optimal t depends on the channel and the blocklength. We have then investigated the optimal decision rule and proven that it is a threshold rule.

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.

To find the exact choice of t, we have given part of a solution for the suboptimal case when we fix the decision rule: we have given a condition that shows whether a t is optimal or not, but we are still not able to determine the correct t directly from the parameters $(n, \epsilon_0, \epsilon_1, \ell)$.

References

[1] C. E. Shannon, "A mathematical theory of communication," *Bell System Techn. J.*, vol. 27, pp. 379–423 and 623–656, Jul. and Oct. 1948.