Optimal Reliability over a Class of Binary-Input Channels with Feedback

Mohammad Naghshvar, Michèle Wigger, and Tara Javidi

***Abstract*—This paper considers the problem of variable-length coding over a binary-input channel with noiseless feedback. A deterministic sequential coding scheme is proposed and shown to attain the optimal error exponent for any binary-input channel whose capacity is achieved by the uniform input distribution. The proposed scheme is deterministic and has only one phase of operation, in contrast to all previous coding schemes that achieve the optimal error exponent.**

***Index Terms*—Binary-input channel, reliability function, optimal error exponent, variable-length coding.**

I. Introduction

In his seminal paper [1], Burnashev provided upper and lower bounds on the minimum number of expected channel uses τ^* that are needed to convey a message (from a fixed message set of size M) with average probability of error smaller than some ϵ over a discrete memoryless channel (DMC) with feedback. The gap between the upper and lower bounds grows at a rate much slower than the lower bound (in terms of $\log M$ and $\log \frac{1}{\epsilon}$). Therefore, the bounds yield the optimal reliability function (also known as the error exponent)

$$E(R) := \lim_{\epsilon \to 0} \frac{-\log \epsilon}{\mathbb{E}[\tau^*]} = C_1 \left(1 - \frac{R}{C}\right), \tag{1}$$

where C denotes the capacity of the channel, $R \in [0, C]$, is the expected rate of the code, and C_1 is the maximum Kullback–Leibler (KL) divergence between the conditional output distributions given any two inputs.

Burnashev proved the upper bound using a two-phase coding scheme. In the first phase, referred to as the *communication* phase, the transmitter tries to increase the decoder's belief about the true message. At the end of this phase, the message with the highest posterior probability is selected as a candidate. The second phase, referred to as the *confirmation* phase, serves to verify the correctness of the output of phase one. Subsequently, in [2], [3], [4], alternative two-phase coding schemes attaining the optimal error exponent were provided. In [5], Burnashev's error exponent was shown to be attainable using a two-phase scheme for a binary symmetric channel (BSC) with an unknown crossover probability.

M. Naghshvar and T. Javidi are with the Department of Electrical and Computer Engineering, University of California San Diego, La Jolla, CA 92093 USA. (e-mail: naghshvar@ucsd.edu; tjavidi@ucsd.edu).

M. Wigger is with the Department of Communications and Electronics, Telecom ParisTech, Paris, France. (e-mail: michele.wigger@telecom-paristech.fr).

The work of M. Naghshvar and T. Javidi was partially supported by the industrial sponsors of UCSD Center for Wireless Communication (CWC), Information Theory and Applications Center (ITA), and Center for Networked Systems (CNS), as well as NSF Grants CCF-0729060 and CCF-1018722. The work of M. Wigger was partially supported by the city of Paris under the program "Emergences".

In [6], [7], see also [8], a sequential, one-phase scheme for transmission over a BSC with noiseless feedback was proposed. This scheme is briefly explained next. Each message is represented as a subinterval of size $\frac{1}{M}$ of the unit interval. After each transmission and given the channel output, the posterior probability of all subintervals are updated. In the next time slot, the transmitter sends 0 if the true message's corresponding subinterval is below the current median, or 1 if it is above. If the current median lies within the true message's subinterval, then the transmitter sends 0 with probability equal to the fraction of the interval above the median and 1 otherwise. As the rounds of transmission proceed, the posterior probability of the true message's subinterval most likely grows larger than $\frac{1}{2}$, which pushes the median within the message's subinterval and thus leads to a randomized encoding. Although this simple one-phase scheme achieves the capacity of a BSC, it is unclear whether it attains the optimal error exponent.

These previous results raise the question whether having two separate phases of operation and randomized encoding are necessary to achieve the optimal error exponent or not. The main contribution of this paper is to propose a deterministic one-phase coding scheme that achieves the optimal error exponent of any binary-input channel with noiseless feedback whose capacity is achieved by the uniform input distribution. The proposed coding scheme uses, in each transmission round, the posterior probability of the messages to partition them into two sets in a way that the probability of the presence of the true message in each set is as close as possible to 0.5. The transmitter then sends 0 or 1 depending on which set includes the true message. Our proposed coding technique differs from the sequential schemes in [6], [7], [8] in that here the encoding is deterministic and the channel inputs are not distributed according to the capacity-achieving input distribution $(0.5, 0.5)$. Nonetheless, we show that this scheme achieves both the capacity and the optimal error exponent.

The remainder of this paper is organized as follows. In Section II, we formulate the variable-length coding problem with noiseless feedback. Section III focuses on binary-input channels with noiseless feedback, explains the proposed coding scheme, and provides the main result of the paper. Finally, we conclude the paper with a discussion of the future work in Section IV.

Notation: A random variable is denoted by an upper case letter (e.g. X) and its realization is denoted by a lower case letter (e.g. x). Similarly, a random vector and its realization are denoted by bold face symbols (e.g. $\mathbf{X}$ and $\mathbf{x}$). The entropy function on a vector $\boldsymbol{\rho} = (\rho_1, \rho_2, \ldots, \rho_M) \in [0,1]^M$ is defined as $H(\boldsymbol{\rho}) := \sum_{i=1}^{M} \rho_i \log(1/\rho_i)$, with the convention that $0 \log \frac{1}{0} = 0$. Finally, the *Kullback–Leibler (KL) divergence* between two probability distributions P_Z and P'_Z over a finite set $\mathcal{Z}$ is defined as $D(P_Z||P'_Z) := \sum_{z \in \mathcal{Z}} P_Z(z) \log \frac{P_Z(z)}{P'_Z(z)}$ with the convention $0 \log \frac{a}{0} = 0$ and $b \log \frac{b}{0} = \infty$ for $a, b \in [0,1]$ with $b \neq 0$.

II. Variable-Length Coding with Noiseless Feedback

Consider the problem of variable-length coding over a discrete memoryless channel (DMC) with noiseless feedback as depicted in Fig. 1. The DMC is described by finite input

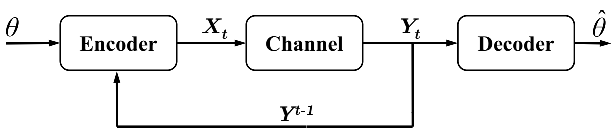

Fig. 1. A noisy memoryless channel with a noiseless causal feedback link.

and output sets $\mathcal{X}$ and $\mathcal{Y}$, and a collection of conditional probabilities $P(Y|X)$. Let C denote the Shannon capacity of this DMC:

$$C = \max_{P_X} I(X;Y),$$

and C_1 the Kullback–Leibler (KL) divergence between its two most distinguishable inputs:

$$C_1 = \max_{x, x' \in \mathcal{X}} D(P(Y|X=x)||P(Y|X=x')).$$

In variable-length coding, as opposed to fixed-length coding, the total transmission time τ is not known before the transmission starts but instead is a random stopping time that is decided at the receiver as a function of the observed channel outputs. Thanks to the noiseless feedback, the transmitter is also informed of the channel outputs and hence of the stopping time.

The transmitter wishes to communicate a message θ to the receiver, where θ is uniformly distributed over the message set $\Omega = \{1, 2, \ldots, M\}$. To this end, it produces channel inputs X_t for $t = 1, \ldots, \tau$, which it can compute as a function of the message θ and (thanks to the noiseless causal feedback) also of the past channel outputs $Y_1, \ldots, Y_{t-1}$:

$$X_t = e_t(\theta, Y_1, \ldots, Y_{t-1}), \quad t = 1, \ldots, \tau, \tag{2}$$

for some encoding function $e_t \colon \Omega \times \mathcal{Y}^{t-1} \to \mathcal{X}$.

After observing the τ channel outputs $Y_1, \ldots, Y_\tau$, the receiver guesses the message θ as

$$\hat{\theta} = d(Y_1, \ldots, Y_\tau), \tag{3}$$

for some decoding function $d \colon \mathcal{Y}^\tau \to \Omega$. The probability of error of the scheme is thus

$$\mathrm{Pe} := \Pr(\hat{\theta} \neq \theta).$$

For a fixed DMC and for a given $\epsilon > 0$, the goal is to find encoding and decoding rules as in (2) and (3), and a stopping time τ such that the probability of error satisfies $\mathrm{Pe} \leq \epsilon$ and the expected number of channel uses $\mathbb{E}[\tau]$ is minimized. Let τ^* denote the random stopping time that achieves this minimum.

In his seminal paper [1], Burnashev provided upper and lower bounds on the minimum expected number of channel uses $\mathbb{E}[\tau^*]$ for a large class of DMCs and arbitrary $\epsilon > 0$.

Fact 1 (Theorems 1 and 2 of [1])**.** *For any DMC with $0 < C_1 < \infty$ and positive capacity $C > 0$:*

$$\mathbb{E}[\tau^*] \geq \left(\frac{\log M}{C} + \frac{\log \frac{1}{\epsilon}}{C_1} \right) (1 - o(1)), \tag{4}$$

and

$$\mathbb{E}[\tau^*] \leq \left(\frac{\log M}{C} + \frac{\log \frac{1}{\epsilon}}{C_1} \right) (1 + o(1)), \tag{5}$$

where $o(1) \to 0$ as $\epsilon/M \to 0$.

Defining the rate as

$$R := \frac{\log M}{\mathbb{E}[\tau^*]},$$

we obtain from these bounds the optimal variable-length coding error exponent:

Fact 2 (Theorem 3 of [1])**.** *In the presence of noiseless feedback, the optimal variable-length error exponent of a DMC with $0 < C_1 < \infty$ is:*

$$E(R) := \lim_{\epsilon \to 0} \frac{-\log \epsilon}{\mathbb{E}[\tau^*]} = C_1 \left(1 - \frac{R}{C} \right). \tag{6}$$

Burnashev proved the upper bound (5) using the following two-phase scheme [1]. While in the first phase (*communication phase*) the transmitter iteratively refines the receiver's belief about the true message, in the second phase (*confirmation phase*) it simply communicates whether the receiver's highest belief after the first phase corresponds to the true message. In [2], [4], it was shown that the sequential scheme in the first phase can be exchanged by any capacity achieving block coding scheme.

Inequality (4) was proved in [1] using a Martingale argument, and it was reproved in an alternative way in [9], [10] that parallels the two-phase coding scheme in [2]. In [11], using the dynamic programming representation of the problem, a concise and more intuitive proof of lower bound (4) was provided.

III. Binary-Input Channels with Symmetric Capacity-Achieving Input Distribution

We focus on channels with binary inputs, i.e., $|\mathcal{X}| = 2$, with finite and positive C, C_1, and with a uniform capacity-achieving input distribution. This is a general class of channels which includes the binary symmetric channel (BSC) with cross-over probability $p \in (0,1)$, as well as the non-symmetric channel in Fig. 2 for $\eta \in (0,1)$. For ease of notation, in the following we let $\mathcal{X} = \{0, 1\}$, and assume that $C_1 = D(P(Y|X=0)||P(Y|X=1))$.

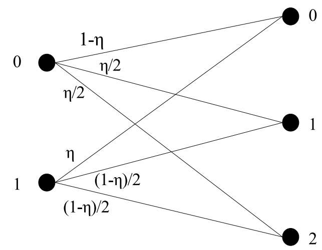

Fig. 2. Binary-input ternary-output channel with capacity-achieving input distribution $(0.5, 0.5)$.

Before describing and analyzing our scheme in Sections III-A and III-B, we give some definitions. For each $t = 0, 1, \ldots, \tau$ and each possible message $i \in \Omega$, let $\rho_i(t)$ be the receiver's posterior (or belief) about $\theta = i$ after observing $Y^t := (Y_1, \ldots, Y_t)$:

$$\rho_i(t) := \Pr(\theta = i | Y^t), \tag{7}$$

where $Y^0 = \emptyset$, and thus $\rho_i(0) = \Pr(\theta = i)$ denotes the receiver's initial belief of $\theta = i$ before the transmission starts. (In our communication setup described in Section II we have $\rho_i(0) = \frac{1}{M}$ for all $i \in \Omega$. The scheme and its analysis however also hold for general initial beliefs.) Let further

$$\boldsymbol{\rho}(t) := (\rho_1(t), \ldots, \rho_M(t)), \quad t = 0, 1, \ldots, \tau.$$

For shortness we will also write $\boldsymbol{\rho}$ for $\boldsymbol{\rho}(0)$ and ρ_i for $\rho_i(0)$.

A. Variable-Length Coding Scheme

The encoder applies a sequential encoding rule that at each time $t = 1, \ldots, \tau$ depends only on the message θ and the current belief state $\boldsymbol{\rho}(t-1)$. (Notice that thanks to the noiseless feedback, before producing the time-t input, also the encoder can compute $\boldsymbol{\rho}(t-1)$.) The encoder first partitions the set of messages Ω into two non-empty sets $S_0(t-1)$ and $S_1(t-1)$ such that

$$\sum_{i \in S_0(t-1)} \rho_i(t-1) \geq \sum_{j \in S_1(t-1)} \rho_j(t-1), \tag{8}$$

and for any other partition $\{\hat{S}_0, \hat{S}_1\}$

$$\begin{aligned} &\sum_{i \in S_0(t-1)} \rho_i(t-1) - \sum_{j \in S_1(t-1)} \rho_j(t-1) \\ &\qquad \leq \left| \sum_{i \in \hat{S}_0} \rho_i(t-1) - \sum_{j \in \hat{S}_1} \rho_j(t-1) \right|. \end{aligned} \tag{9}$$

In other words, it partitions Ω into sets $S_0(t-1)$ and $S_1(t-1)$ such that the a posteriori probability that message θ lies in each of the two sets given Y^{t-1} is as close as possible to $(0.5, 0.5)$, the capacity-achieving distribution. Then, it sends $X_t = 0$ if $\theta \in S_0(t-1)$ and $X_t = 1$ otherwise.

The transmission is stopped as soon as one of the posteriors becomes larger than $1 - \epsilon$, where $\epsilon > 0$ is the desired probability of error. Thus,

$$\tau := \min \left\{ t : \max_{i \in \Omega} \rho_i(t) \geq 1 - \epsilon \right\}. \tag{10}$$

The receiver produces as its guess the message with the highest posterior:

$$\hat{\theta} = \arg\max_{i \in \Omega} \rho_i(\tau).$$

Remark 1. Our scheme differs from the previous one-phase sequential schemes in [6], [7], [8] in that here the encoding process is completely deterministic. By insisting on a deterministic encoding, we can match our scheme's inputs only *approximately* to the capacity-achieving input distribution of $(0.5, 0.5)$. On the other hand, the proposed deterministic encoding is such that once a particular message's posterior passes a certain threshold, the transmitter assigns this message exclusively to one of the two inputs. This is critical for achieving the optimal error exponent.

B. Performance Analysis

By construction, our scheme satisfies the constraint on the probability of error:

$$\mathrm{Pe} = \mathbb{E}[1 - \max_{j \in \Omega} \rho_j(\tau)] \leq \epsilon.$$

Next we show that the expected stopping time $\mathbb{E}[\tau]$ satisfies the following proposition.

Proposition 1. *There exists a K' independent of the number of messages M and the error probability ϵ such that for an initial belief $\boldsymbol{\rho}$ the scheme in Section III-A satisfies*

$$\mathbb{E}[\tau] \leq \frac{H(\boldsymbol{\rho})}{C} + \frac{\log \frac{1}{\epsilon}}{C_1} + K'.$$

Corollary 1. *When the initial belief $\boldsymbol{\rho}$ is uniform as assumed in Section II, our scheme satisfies*

$$\mathbb{E}[\tau] \leq \frac{\log M}{C} + \frac{\log \frac{1}{\epsilon}}{C_1} + K'.$$

Remark 2. Corollary 1 implies that our coding scheme achieves the optimal error exponent in (6) for binary-input channels with symmetric capacity-achieving input distribution. The proposed scheme is deterministic and has only one phase of operation, in contrast to all previous coding schemes known to achieve the optimal error exponent.

Proof of Proposition 1: Let τ_i, $i \in \Omega$, be Markov stopping times defined as follows:[1]

$$\tau_i = \min \{ t : \rho_i(t) \geq 1 - \epsilon \}.$$

The expected stopping time of our scheme satisfies:

$$\begin{aligned} \mathbb{E}[\tau] &= \sum_{i=1}^{M} \rho_i \mathbb{E}[\tau | \theta = i] \\ &\leq \sum_{i=1}^{M} \rho_i \mathbb{E}[\tau_i | \theta = i], \end{aligned} \tag{11}$$

where the last inequality follows because $\tau \leq \tau_i$ for all $i \in \Omega$.

[1] For this definition to make sense (and which we only need in the analysis) we assume that the transmitter continues to transmit even after time τ using the same encoding rule as before.

Now, let $\mathcal{F}_t$ denote the history of the receiver's knowledge up to time t, i.e., $\mathcal{F}_t = \sigma\{Y^t\}$. Moreover, for each $i \in \Omega$ and each time $t = 0, 1, \ldots, \tau_i$, define

$$U_i(t) := \log \frac{\rho_i(t)}{1 - \rho_i(t)}.$$

In Appendix A, we show that for $t = 0, 1, \ldots, \tau_i - 1$:

$$\mathbb{E}\left[U_i(t+1) | \mathcal{F}_t, \theta = i\right] \geq \begin{cases} U_i(t) + C & \text{if } U_i(t) < 0 \\ U_i(t) + C_1 & \text{if } U_i(t) \geq 0 \end{cases}. \tag{12}$$

Since C and C_1 are both positive, conditioned on $\theta = i$, the sequence $\{U_i(t)\}_{t=0}^{\tau_i}$ forms a submartingale with respect to the filtration $\{\mathcal{F}_t\}$. Furthermore, $C_1 \geq C$ and (as shown in Appendix B)

$$|U_i(t+1) - U_i(t)| \leq \max_{y \in \mathcal{Y}} \log \frac{\max_{x \in \mathcal{X}} P(Y = y | X = x)}{\min_{x \in \mathcal{X}} P(Y = y | X = x)}, \tag{13}$$

which is finite because $C_1 < \infty$ implies that for all $x \in \mathcal{X}$ and $y \in \mathcal{Y}$, the transition probability $P(Y = y | X = x)$ is positive. Denoting the right-hand side of (13) by C_2, we can apply Lemma 1 (at the end of this section) to obtain:

$$\begin{aligned}
&\mathbb{E}[\tau_i | \theta = i] \\
&\leq \frac{\log \frac{1-\epsilon}{\epsilon} - \log \frac{\rho_i}{1-\rho_i}}{C_1} + \log \frac{\rho_i}{1-\rho_i} \mathbf{1}_{\{\rho_i < 0.5\}} \left(\frac{1}{C_1} - \frac{1}{C} \right) \\
&\quad + F(C, C_1, C_2) \\
&= \frac{\log \frac{1-\epsilon}{\epsilon}}{C_1} + \frac{\log \frac{1-\rho_i}{\rho_i}}{C_1} \mathbf{1}_{\{\rho_i \geq 0.5\}} + \frac{\log \frac{1-\rho_i}{\rho_i}}{C} \mathbf{1}_{\{\rho_i < 0.5\}} \\
&\quad + F(C, C_1, C_2) \\
&\leq \frac{\log \frac{1-\epsilon}{\epsilon}}{C_1} + \frac{\log \frac{1-\rho_i}{\rho_i}}{C} \mathbf{1}_{\{\rho_i < 0.5\}} + F(C, C_1, C_2) \\
&\leq \frac{\log \frac{1}{\epsilon}}{C_1} + \frac{\log \frac{1}{\rho_i}}{C} + K_i',
\end{aligned} \tag{14}$$

where K_i' is independent of ϵ and the size of the message set M. Combining (11) and (14) and defining $K' := \sum_i \rho_i K_i'$ proves the proposition. ∎

Lemma 1 (A slight modification of Lemma 1 in [12])**.** *Assume that the sequence $\{\xi_t\}$, $t = 0, 1, \ldots$ forms a submartingale with respect to a filtration $\{\mathcal{F}_t\}$. Furthermore, assume there exist positive constants K_1, K_2, K_3, $K_1 \leq K_2 \leq K_3$, such that*

$$\begin{aligned}
&\mathbb{E}[\xi_{t+1} | \mathcal{F}_t] \geq \xi_t + K_1 \quad \text{if} \quad \xi_t < 0, \\
&\mathbb{E}[\xi_{t+1} | \mathcal{F}_t] \geq \xi_t + K_2 \quad \text{if} \quad \xi_t \geq 0, \\
&|\xi_{t+1} - \xi_t| \leq K_3.
\end{aligned}$$

For the stopping time $\upsilon = \min\{t : \xi_t \geq B\}$, $B > 0$, we have:

$$\mathbb{E}[\upsilon] \leq \frac{B - \xi_0}{K_2} + \xi_0 \mathbf{1}_{\{\xi_0 < 0\}} \left(\frac{1}{K_2} - \frac{1}{K_1} \right) + F(K_1, K_2, K_3),$$

where the function F depends only on K_1, K_2, K_3.

IV. Discussion and Future Work

We proposed a deterministic one-phase coding scheme for a class of binary-input memoryless channels that achieves the optimal error exponent of the channel.

The proposed coding scheme requires finding a partitioning of the message set into $S_0(t-1)$ and $S_1(t-1)$ such that $\sum_{j \in S_0(t-1)} \rho_j(t-1) - \sum_{j \in S_1(t-1)} \rho_j(t-1)$ is positive and minimized. This is the optimization version of the partition problem and has a complexity of order $O(2^M)$. Our proof of optimality remains valid so long as the set of messages is partitioned such that $\sum_{j \in S_0(t-1)} \rho_j(t-1) - \sum_{j \in S_1(t-1)} \rho_j(t-1)$ is positive and less than $\rho_i(t-1)$ for every $i \in S_0(t-1)$. It is possible, fortunately, to construct an algorithm which partitions the message set with this less stringent condition via sorting the beliefs and then a maximum of M^2 rounds of operations, resulting in an encoding scheme with complexity $O(M^2)$.

Extending the result to general binary and k-ary symmetric channels is the topic of ongoing research.

References

[1] M. V. Burnashev, "Data Transmission Over a Discrete Channel with Feedback. Random Transmission Time," *Problemy Peredachi Informatsii*, vol. 12, no. 4, pp. 10–30, 1975.

[2] H. Yamamoto and K. Itoh, "Asymptotic Performance of a Modified Schalkwijk-Barron Scheme for Channels with Noiseless Feedback," *IEEE Transactions on Information Theory*, vol. 25, pp. 729–733, 1979.

[3] J. M. Ooi and G. W. Wornell, "Fast Iterative Coding Techniques for Feedback Channels," *IEEE Transactions on Information Theory*, vol. 44, no. 7, pp. 2960–2976, November 1998.

[4] G. Caire, S. Shamai, and S. Verdu, "Propagation, Feedback and Belief," *4th International Symposium on Turbo Codes & Related Topics; 6th International ITG-Conference on Source and Channel Coding (TURBOCODING)*, pp. 1–6, April 2006.

[5] A. Tchamkerten and E. Telatar, "Variable Length Coding Over an Unknown Channel," *IEEE Transactions on Information Theory*, vol. 52, pp. 2126–2145, May 2006.

[6] M. Horstein, "Sequential Transmission Using Noiseless Feedback," *IEEE Transactions on Information Theory*, vol. 9, no. 3, pp. 136–143, July 1963.

[7] M. V. Burnashev and K. Sh. Zigangirov, "An Interval Estimation Problem for Controlled Observations," *Problemy Peredachi Informatsii*, vol. 10, no. 3, pp. 51–61, 1974.

[8] O. Shayevitz and M. Feder, "Optimal Feedback Communication via Posterior Matching," *IEEE Transactions on Information Theory*, vol. 57, no. 3, pp. 1186–1222, March 2011.

[9] P. Berlin, B. Nakiboglu, B. Rimoldi, and E. Telatar, "A Simple Converse of Burnashev's Reliability Function," *IEEE Transactions on Information Theory*, vol. 55, pp. 3074–3080, July 2009.

[10] Y. Polyanskiy, H. V. Poor, and S. Verdu, "Feedback in the Non-Asymptotic Regime," *IEEE Transactions on Information Theory*, vol. 57, no. 8, pp. 4903–4925, August 2011.

[11] M. Naghshvar and T. Javidi, "Active Sequential Hypothesis Testing," 2012, available on arXiv:1203.4626.

[12] M. V. Burnashev and K. Sh. Zigangirov, "On One Problem of Observation Control," *Problemy Peredachi Informatsii*, vol. 11, no. 3, pp. 44–52, 1975.

Appendix A
Proof of inequality (12)

We first state some definitions and lemmas.

A1. Auxiliary Lemmas and Definitions

For $t = 0, 1, \ldots, \tau - 1$, define

$$\delta(t) := \sum_{i \in S_0(t)} \rho_i(t) - \sum_{j \in S_1(t)} \rho_j(t). \tag{15}$$

Lemma 2. *For any $t = 0, 1, \ldots, \tau - 1$ and any $i \in S_0(t)$ (the "larger" of the two sets), $\rho_i(t) \geq \delta(t)$.*

Proof: Consider the sets

$$\hat{S}_0 = S_0(t) - \{i\} \quad \text{and} \quad \hat{S}_1 = S_1(t) \cup \{i\}.$$

If $\rho_i(t) < \delta(t)$, then the sets $\hat{S}_0$ and $\hat{S}_1$ are more balanced than the sets $S_0(t)$ and $S_1(t)$, i.e., assumption (9) is violated. ∎

Lemma 3. *Let $P(Y|X)$ be a binary-input channel of positive capacity $C > 0$. Let $P(X^*)$ be the capacity-achieving input distribution and $P(X)$ be an arbitrary input distribution for this channel. Also, let $P(Y^*)$ and $P(Y)$ be the output distributions induced by $P(X^*)$ and $P(X)$, respectively. Then, for any $x \in \mathcal{X}$ such that $P(X = x) \leq P(X^* = x)$:*

$$D(P(Y|X = x)||P(Y)) \geq D(P(Y|X = x)||P(Y^*)) = C.$$

Proof: Let $x \in \mathcal{X}$ satisfy $P(X = x) \leq P(X^* = x)$. Choose $\lambda \in [0, 1]$ such that

$$P(X^* = x') = \lambda P(X = x') + (1 - \lambda)\mathbf{1}_{\{x'=x\}}, \quad x' \in \mathcal{X},$$

and consequently $P(Y^*) = \lambda P(Y) + (1 - \lambda)P(Y|X = x)$. By the convexity of the KL divergence:

$$\begin{aligned} &D(P(Y|X = x)||P(Y^*)) \\ &\quad\leq \lambda D(P(Y|X = x)||P(Y)) \\ &\quad\quad + (1 - \lambda)D(P(Y|X = x)||P(Y|X = x)) \\ &\quad= \lambda D(P(Y|X = x)||P(Y)) \\ &\quad\leq D(P(Y|X = x)||P(Y)). \end{aligned} \tag{16}$$

Moreover, by the Karush–Kuhn–Tucker conditions and because $C > 0$ and $|\mathcal{X}| = 2$ imply that $P(X^* = x) > 0$:

$$D(P(Y|X = x)||P(Y^*)) = C. \tag{17}$$

Combining (16) and (17) establishes the lemma. ∎

Define the input probabilities

$$\pi_x(t + 1) := \sum_{j \in S_x(t)} \rho_j(t), \qquad x \in \mathcal{X}, \tag{18}$$

and for each $i \in \Omega$, the extrinsic probabilities

$$\tilde{\pi}_x^i(t + 1) := \begin{cases} \frac{\pi_x(t+1)}{1-\rho_i(t)}, & i \notin S_x(t) \\ \frac{\pi_x(t+1)-\rho_i(t)}{1-\rho_i(t)}, & i \in S_x(t) \end{cases} \qquad x \in \mathcal{X}. \tag{19}$$

A2. Inequality (12)

We fix $i \in \Omega$. If $Y_{t+1} = y_{t+1}$, the belief state evolves as

$$\rho_i(t + 1) = \frac{\rho_i(t)P(Y = y_{t+1}|X = e_{t+1}(i, Y^t))}{\sum_{j=1}^{M} \rho_j(t)P(Y = y_{t+1}|X = e_{t+1}(j, Y^t))}.$$

Moreover, if $\theta = i$ and $i \in S_{x_i}(t)$, then Y_{t+1} is distributed according to the law $P(Y|X = x_i)$. Combining these two observations, we have

$$\begin{aligned} &\mathbb{E}\left[U_i(t + 1) - U_i(t)|\mathcal{F}_t, \theta = i\right] \\ &= \mathbb{E}\left[\log \frac{\rho_i(t + 1)}{1 - \rho_i(t + 1)} - \log \frac{\rho_i(t)}{1 - \rho_i(t)} \middle| \mathcal{F}_t, \theta = i\right] \\ &= \sum_{y \in \mathcal{Y}} P(Y = y|X = x_i) \\ &\quad \cdot \left(\log \frac{\frac{\rho_i(t)P(Y=y|X=x_i)}{\sum_{x\in\mathcal{X}} \pi_x(t+1)P(Y=y|X=x)}}{1 - \frac{\rho_i(t)P(Y=y|X=x_i)}{\sum_{x\in\mathcal{X}} \pi_x(t+1)P(Y=y|X=x)}} - \log \frac{\rho_i(t)}{1 - \rho_i(t)}\right) \\ &= \sum_{y \in \mathcal{Y}} P(Y = y|X = x_i) \\ &\quad \cdot \log \frac{P(Y = y|X = x_i)}{\sum_{x\in\mathcal{X}} \tilde{\pi}_x^i(t + 1)P(Y = y|X = x)} \\ &= D(P(Y|X = x_i)||P(\tilde{Y})), \end{aligned} \tag{20}$$

where $\tilde{Y}$ is the output induced by the channel $P(Y|X)$ for the input $\tilde{X} \sim P(\tilde{X} = x) = \tilde{\pi}_x^i(t + 1)$.

When $U_i(t) < 0$, we distinguish two cases. If $i \in S_1(t)$ and $x_i = 1$:

$$\tilde{\pi}_1^i(t + 1) < 0.5 = P(X^* = 1),$$

because, by definition, $\pi_1(t + 1) \leq 0.5$ and $\tilde{\pi}_1^i(t + 1) < \pi_1(t + 1)$. Thus, by (20) and Lemma 3:

$$\mathbb{E}\left[U_i(t + 1) - U_i(t)|\mathcal{F}_t, \theta = i\right] \geq C. \tag{21}$$

If $i \in S_0(t)$ and $x_i = 0$:

$$\tilde{\pi}_0^i(t + 1) \leq 0.5 = P(X^* = 0),$$

because by Lemma 2, $\rho_i(t) \geq \delta(t)$, and thus $\tilde{\pi}_0^i(t + 1) \leq \tilde{\pi}_1^i(t + 1)$. By (20) and Lemma 3, we again conclude (21).

When $U_i(t) \geq 0$, then $\rho_i(t) \geq 0.5$ and in our coding scheme $S_0(t) = \{i\}$. Thus, $x_i = 0$, $\tilde{\pi}_0^i(t + 1) = 0$, and $\tilde{Y} \sim P(Y|X = 1)$, and by (20):

$$\begin{aligned} &\mathbb{E}\left[U_i(t + 1) - U_i(t)|\mathcal{F}_t, \theta = i\right] \\ &\quad = D(P(Y|X = 0)||P(Y|X = 1)) = C_1. \end{aligned} \tag{22}$$

Appendix B
Proof of Inequality (13)

To prove (13), we note that when $Y_{t+1} = y$:

$$\begin{aligned} &|U_i(t + 1) - U_i(t)| \\ &= \left|\log \frac{\rho_i(t + 1)}{1 - \rho_i(t + 1)} - \log \frac{\rho_i(t)}{1 - \rho_i(t)}\right| \\ &= \left|\log \frac{\rho_i(t)P(Y = y|X = e_{t+1}(i, Y^t))}{\sum_{j\neq i} \rho_j(t)P(Y = y|X = e_{t+1}(j, Y^t))} \cdot \frac{1 - \rho_i(t)}{\rho_i(t)}\right| \\ &= \left|\log \frac{P(Y = y|X = e_{t+1}(i, Y^t))}{\sum_{j\neq i} \frac{\rho_j(t)}{1-\rho_i(t)}P(Y = y|X = e_{t+1}(j, Y^t))}\right| \\ &\leq \log \frac{\max_{x\in\mathcal{X}} P(Y = y|X = x)}{\min_{x\in\mathcal{X}} P(Y = y|X = x)}. \end{aligned}$$

Thus, we have

$$|U_i(t + 1) - U_i(t)| \leq \max_{y\in\mathcal{Y}} \log \frac{\max_{x\in\mathcal{X}} P(Y = y|X = x)}{\min_{x\in\mathcal{X}} P(Y = y|X = x)}.$$