Dispersion of the Gilbert-Elliott Channel

Yury Polyanskiy, H. Vincent Poor, and Sergio Verdú

Abstract

Channel dispersion plays a fundamental role in assessing the backoff from capacity due to finite blocklength. This paper analyzes the channel dispersion for a simple channel with memory: the Gilbert-Elliott communication model in which the crossover probability of a binary symmetric channel evolves as a binary symmetric Markov chain, with and without side information at the receiver about the channel state. With side information, dispersion is equal to the average of the dispersions of the individual binary symmetric channels plus a term that depends on the Markov chain dynamics, which do not affect the channel capacity. Without side information, dispersion is equal to the spectral density at zero of a certain stationary process, whose mean is the capacity. In addition, the finite blocklength behavior is analyzed in the non-ergodic case, in which the chain remains in the initial state forever.

Index Terms

Gilbert-Elliott channel, non-ergodic channels, finite blocklength regime, hidden Markov models, coding for noisy channels, Shannon theory, channel capacity.

The authors are with the Department of Electrical Engineering, Princeton University, Princeton, NJ, 08544 USA. e-mail: {ypolyans,poor,verdu}@princeton.edu.

The research was supported by the National Science Foundation under Grants CCF-06-35154 and CNS-09-05398.

I. Introduction

The fundamental performance limit for a channel in the finite blocklength regime is $M^*(n,\epsilon)$, the maximal cardinality of a codebook of blocklength n which can be decoded with block error probability no greater than ϵ. Denoting the channel capacity by C[1], the approximation

$$\frac{\log M^*(n,\epsilon)}{n} \approx C \tag{1}$$

is asymptotically tight for channels that satisfy the strong converse. However for many channels, error rates and blocklength ranges of practical interest, (1) is too optimistic. It has been shown in [1] that a much tighter approximation can be obtained by defining a second parameter referred to as the channel dispersion:

Definition 1: The dispersion V (measured in squared information units per channel use) of a channel with capacity C is equal to[2]

$$V = \lim_{\epsilon\to 0}\limsup_{n\to\infty}\frac{1}{n}\frac{(nC-\log M^*(n,\epsilon))^2}{2\ln\frac{1}{\epsilon}}\,. \tag{2}$$

In conjunction with the channel capacity C, channel dispersion emerges as a powerful analysis and design tool; for example in [1] we demonstrated how channel dispersion can be used to assess the efficiency of practical codes and optimize system design. One of the main advantages of knowing the channel dispersion lies in estimating the minimal blocklength required to achieve a given fraction η of capacity with a given error probability ϵ:[3]

$$n \gtrsim \left(\frac{Q^{-1}(\epsilon)}{1-\eta}\right)^2 \frac{V}{C^2}\,. \tag{3}$$

The rationale for Definition 1 and estimate (3) is the following expansion

$$\log M^*(n,\epsilon) = nC - \sqrt{nV}Q^{-1}(\epsilon) + O(\log n)\,. \tag{4}$$

As shown in [1], in the context of memoryless channels (4) gives an excellent approximation for blocklengths and error probabilities of practical interest.

Traditionally, the dependence of the optimal coding rate on blocklength has been associated with the question of computing the channel reliability function. Although channel dispersion is

[1] Capacity and all rates in this paper are measured in information units per channel use.

[2] All logarithms, $\log$, and exponents, $\exp$, in this paper are taken with respect to an arbitrary fixed base, which also determines the information units.

[3] As usual, $Q(x) = \int_x^\infty \frac{1}{\sqrt{2\pi}} e^{-t^2/2}\,dt\,.$

equal to the reciprocal of the second derivative of the reliability function at capacity, determining the reliability function is not necessary to obtain channel dispersion, which is in fact far easier. Moreover, for determining the blocklength required to achieve a given performance predictions obtained from error-exponents may be far inferior compared to those obtained from (3) (e.g. [1, Table I]).

In this paper, we initiate the study of the dispersion of channels subject to fading with memory. For coherent channels that behave ergodically, channel capacity is independent of the fading dynamics [2] since a sufficiently long codeword sees a channel realization whose empirical statistics have no randomness. In contrast, channel dispersion does depend on the extent of the fading memory since it determines the blocklength required to ride out not only the noise but the channel fluctuations due to fading. One of the simplest models that incorporates fading with memory is the Gilbert-Elliott channel (GEC): a binary symmetric channel where the crossover probability is a binary Markov chain [3], [4]. The results and required tools depend crucially on whether the channel state is known at the decoder.

In Section II we define the communication model. Section III reviews the known results for the Gilbert-Elliott channel. Then in Section IV we present our main results for the ergodic case: an asymptotic expansion (4) and a numerical comparison against tight upper and lower bounds on the maximal rate for fixed blocklength. After that, we move to analyzing the non-ergodic case in Section V thereby accomplishing the first analysis of the finite-blocklength maximal rate for a non-ergodic channel: we prove an expansion similar to (4), and compare it numerically with upper and lower bounds.

II. Channel model

Let $\{S_j\}_{j=1}^\infty$ be a homogeneous Markov process with states $\{1,2\}$ and transition probabilities

$$\mathbb{P}[S_2 = 1 | S_1 = 1] = \mathbb{P}[S_2 = 2 | S_1 = 2] = 1 - \tau\,, \tag{5}$$

$$\mathbb{P}[S_2 = 2 | S_1 = 1] = \mathbb{P}[S_2 = 1 | S_1 = 2] = \tau\,. \tag{6}$$

Now for $0 \le \delta_1, \delta_2 \le 1$ we define $\{Z_j\}_{j=1}^\infty$ as conditionally independent given $\{S_j\}_{j=1}^\infty$ and

$$\mathbb{P}[Z_j = 0 | S_j = s] \;=\; 1 - \delta_s\,, \tag{7}$$

$$\mathbb{P}[Z_j = 1 | S_j = s] \;=\; \delta_s\,. \tag{8}$$

The Gilbert-Elliott channel acts on an input binary vector X^n by adding (modulo 2) the vector Z^n:

$$Y^n = X^n + Z^n\,. \tag{9}$$

The description of the channel model is incomplete without specifying the distribution of S_1:

$$\begin{aligned} \mathbb{P}[S_1 = 1] &= p_1, \qquad (10)\\ \mathbb{P}[S_1 = 2] &= p_2 = 1 - p_1\,. \qquad (11) \end{aligned}$$

In this way the Gilbert-Elliott channel is completely specified by the parameters $(\tau, \delta_1, \delta_2, p_1)$.

There are two drastically different modes of operation of the Gilbert-Elliott channel[4]. When $\tau > 0$ the chain S_1 is ergodic and for this reason we consider only the stationary case $p_1 = 1/2$. On the other hand, when $\tau = 0$ we will consider the case of arbitrary p_1.

III. Previous results

A. Capacity of the Gilbert-Elliott Channel

The capacity C_1 of a Gilbert-Elliott channel $\tau > 0$ and state S^n known perfectly at the receiver depends only on the stationary distribution P_{S_1} and is given by

$$\begin{aligned} C_1 &= \log 2 - \mathbb{E}\left[h(\delta_{S_1})\right] \qquad (12)\\ &= \log 2 - \mathbb{P}[S_1 = 1]h(\delta_1) - \mathbb{P}[S_1 = 2]h(\delta_2)\,, \qquad (13) \end{aligned}$$

where $h(x) = -x \log x - (1-x)\log(1-x)$ is the binary entropy function. In the symmetric-chain special case considered in this paper, both states are equally likely and

$$C_1 = \log 2 - \frac{1}{2}h(\delta_1) - \frac{1}{2}h(\delta_2). \tag{14}$$

When $\tau > 0$ and state S^n is not known at the receiver, the capacity is given by [5]

$$\begin{aligned} C_0 &= \log 2 - \mathbb{E}\left[h(\mathbb{P}[Z_0 = 1|Z_{-\infty}^{-1}])\right] \qquad (15)\\ &= \log 2 - \lim_{n\to\infty} \mathbb{E}\left[h(\mathbb{P}[Z_0 = 1|Z_{-n}^{-1}])\right]\,. \qquad (16) \end{aligned}$$

Throughout the paper we use subscripts 1 and 0 for capacity and dispersion to denote the cases when the state S^n is known and is not known, respectively.

[4] We omit the case of $\tau = 1$ which is simply equivalent to two parallel binary symmetric channels.

Recall that for $0 < \epsilon < 1$ the ϵ-capacity of the channel is defined as

$$C_\epsilon = \liminf_{n\to\infty} \frac{1}{n} \log M^*(n,\epsilon)\,. \tag{17}$$

In the case $\tau = 0$ and regardless of the state knowledge at the transmitter or receiver, the ϵ-capacity is given by (assuming $h(\delta_1) > h(\delta_2)$)

$$C_\epsilon = \begin{cases} \log 2 - h(\delta_1)\,, & \epsilon < p_1\,, \\ \log 2 - h(\delta_2)\,, & \epsilon > p_1\,. \end{cases} \tag{18}$$

Other than the case of small $|\delta_2 - \delta_1|$, solved in [11], the value of the ϵ-capacity at the breakpoint $\epsilon = p_1$ is in general unknown (see also [12]).

B. Bounds

For our analysis of channel dispersion we need to invoke a few relevant results from [1]. These results apply to arbitrary blocklength but as in [1] we give them for an abstract random transformation $P_{Y|X}$ with input and output alphabets A and B, respectively. An (M,ϵ) code for an abstract channel consists of a codebook with M codewords $(c_1,\dots,c_M) \in \mathsf{A}^M$ and a (possibly randomized) decoder $P_{\hat{W}|Y} : \mathsf{B} \mapsto \{0,1,\dots M\}$ (where '0' indicates that the decoder chooses "error"), satisfying

$$1 - \frac{1}{M}\sum_{m=1}^{M} P_{\hat{W}|X}(m|c_m) \le \epsilon. \tag{19}$$

In this paper, both A and B correspond to $\{0,1\}^n$, where n is the blocklength.

Define the (extended) random variable[5]

$$i(X;Y) = \log \frac{P_{Y|X}(Y|X)}{P_Y(Y)}\,, \tag{20}$$

where $P_Y(y) = \sum_{x\in\mathsf{A}} P_X(x) P_{Y|X}(y|x)$ and P_X is an arbitrary input distribution over the input alphabet A.

Theorem 1 (DT bound [1]): For an arbitrary P_X there exists a code with M codewords and average probability of error ϵ satisfying

$$\epsilon \le \mathbb{E}\left[\exp\left\{-\left[i(X;Y) - \log\tfrac{M-1}{2}\right]^+\right\}\right]\,. \tag{21}$$

[5] In this paper we only consider the case of discrete alphabets, but [1] has more general results that apply to arbitrary alphabets.

Among the available achievability bounds, Gallager's random coding bound [6] does not yield the correct $\sqrt{n}$ term in (4) even for memoryless channels; Shannon's (or Feinstein's) bound is always weaker than Theorem 1 [1], and the RCU bound in [1] is harder than (21) to specialize to the channels considered in this paper.

The optimal performance of binary hypothesis testing plays an important role in our development. Consider a random variable W taking values in a set W, distributed according to either probability measure P or Q. A randomized test between those two distributions is defined by a random transformation $P_{Z|W} : \mathsf{W} \mapsto \{0,1\}$ where 0 indicates that the test chooses Q. The best performance achievable among those randomized tests is given by

$$\beta_\alpha(P,Q) = \min \sum_{w \in \mathsf{W}} Q(w) P_{Z|W}(1|w)\,, \tag{22}$$

where the minimum is taken over all $P_{Z|W}$ satisfying

$$\sum_{w \in \mathsf{W}} P(w) P_{Z|W}(1|w) \geq \alpha\,. \tag{23}$$

The minimum in (22) is guaranteed to be achieved by the Neyman-Pearson lemma. Thus, $\beta_\alpha(P,Q)$ gives the minimum probability of error under hypothesis Q if the probability of error under hypothesis P is not larger than $1-\alpha$. It is easy to show that (e.g. [7]) for any $\gamma > 0$

$$\alpha \leq P\left[\frac{P}{Q} \geq \gamma\right] + \gamma \beta_\alpha(P,Q). \tag{24}$$

On the other hand,

$$\beta_\alpha(P,Q) \leq \frac{1}{\gamma_0}\,, \tag{25}$$

for any γ_0 that satisfies

$$P\left[\frac{P}{Q} \geq \gamma_0\right] \geq \alpha\,. \tag{26}$$

Virtually all known converse results for channel coding (including Fano's inequality and various sphere-packing bounds) can be derived as corollaries to the next theorem by a judicious choice of $Q_{Y|X}$ and a lower bound on β, see [1]. In addition, this theorem gives the strongest bound non-asymptotically.

Theorem 2 (meta-converse): Consider $P_{Y|X}$ and $Q_{Y|X}$ defined on the same input and output spaces. For a given code (possibly randomized encoder and decoder pair), let

$$\begin{aligned} \epsilon &= \text{average error probability with } P_{Y|X}\,, \\ \epsilon' &= \text{average error probability with } Q_{Y|X}\,, \\ P_X = Q_X &= \text{encoder output distribution with} \\ &\quad\ \text{equiprobable codewords.} \end{aligned}$$

Then,

$$\beta_{1-\epsilon}(P_{XY}, Q_{XY}) \le 1 - \epsilon'\,, \tag{27}$$

where $P_{XY} = P_X P_{Y|X}$ and $Q_{XY} = Q_X Q_{Y|X}$.

IV. Ergodic case: $\tau > 0$

A. Main results

Before showing the asymptotic expansion (4) for the Gilbert-Elliott channel we recall the corresponding result for the binary symmetric channel (BSC) [1].

Theorem 3: The dispersion of the BSC with crossover probability δ is

$$V(\delta) = \delta(1-\delta)\log^2 \frac{1-\delta}{\delta}\,. \tag{28}$$

Furthermore, provided that $V(\delta) > 0$ and regardless of whether $0 < \epsilon < 1$ is a maximal or average probability of error we have

$$\begin{aligned} \log M^*(n,\epsilon) &= n(\log 2 - h(\delta)) - \sqrt{nV(\delta)}Q^{-1}(\epsilon) \\ &\quad + \frac{1}{2}\log n + O(1)\,. \end{aligned} \tag{29}$$

The first new result of this paper is:

Theorem 4: Suppose that the state sequence S^n is stationary, $\mathbb{P}[S_1 = 1] = 1/2$, and ergodic, $0 < \tau < 1$. Then the dispersion of the Gilbert-Elliott channel with state S^n known at the receiver is

$$V_1 = \frac{1}{2}(V(\delta_1) + V(\delta_2)) + \frac{1}{4}\left(h(\delta_1) - h(\delta_2)\right)^2 \left(\frac{1}{\tau} - 1\right)\,. \tag{30}$$

Furthermore, provided that $V_1 > 0$ and regardless of whether $0 < \epsilon < 1$ is a maximal or average probability of error we have

$$\log M^*(n,\epsilon) = nC_1 - \sqrt{nV_1}Q^{-1}(\epsilon) + O(\log n)\,, \tag{31}$$

where C_1 is given in (14). Moreover, (31) holds even if the transmitter knows the full state sequence S^n in advance (i.e., non-causally).

Note that the condition $V_1 > 0$ for (31) to hold excludes only some degenerate cases for which we have: $M^*(n,\epsilon) = 2^n$ (when both crossover probabilities are 0 or 1) or $M^*(n,\epsilon) = \lfloor \frac{1}{1-\epsilon} \rfloor$ (when $\delta_1 = \delta_2 = 1/2$).

The proof of Theorem 4 is given in Appendix A. It is interesting to notice that it is the generality of Theorem 2 that enables the extension to the case of state known at the transmitter.

To formulate the result for the case of no state information at the receiver, we define the following stationary process:

$$F_j = -\log P_{Z_j|Z_{-\infty}^{j-1}}(Z_j|Z_{-\infty}^{j-1})\,. \tag{32}$$

Theorem 5: Suppose that $0 < \tau < 1$ and the state sequence S^n is started at the stationary distribution. Then the dispersion of the Gilbert-Elliott channel with no state information is

$$V_0 = \mathrm{Var}\,[F_0] + 2\sum_{i=1}^{\infty} \mathbb{E}\,\left[(F_i - \mathbb{E}\,[F_i])(F_0 - \mathbb{E}\,[F_0])\right]\,. \tag{33}$$

Furthermore, provided that $V_0 > 0$ and regardless of whether ϵ is a maximal or average probability of error, we have

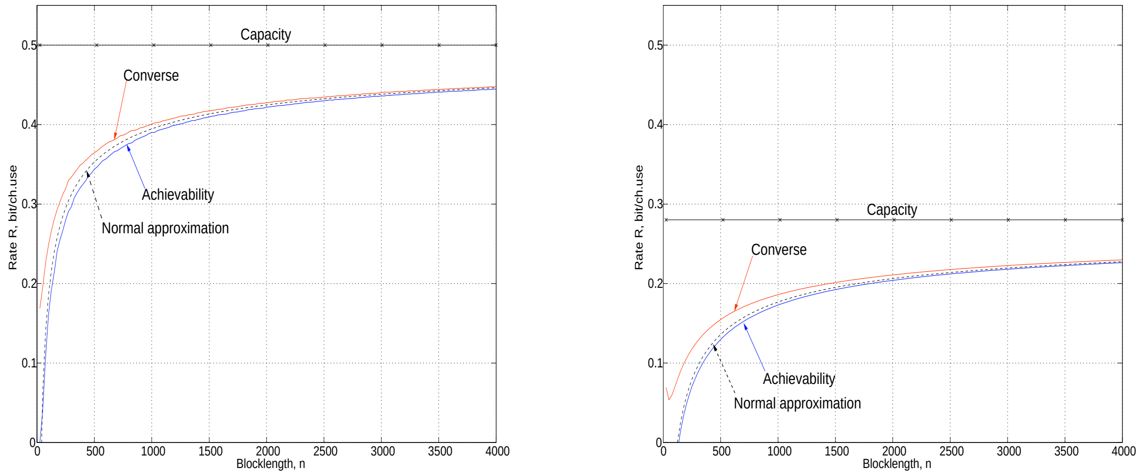
$$\log M^*(n,\epsilon) = nC_0 - \sqrt{nV_0}Q^{-1}(\epsilon) + o(\sqrt{n})\,, \tag{34}$$

where C_0 is given by (15).

It can be shown that the process F_j has a spectral density $S_F(f)$, and that [10]

$$V_0 = S_F(0)\,, \tag{35}$$

which provides a way of computing V_0 by Monte Carlo simulation paired with a spectral estimator. Alternatively, since the terms in the series (33) decay as $(1-2\tau)^j$, it is sufficient to compute only finitely many terms in (33) to achieve any prescribed approximation accuracy. In this regard note that each term in (33) can in turn be computed with arbitrary precision by noting that $P_{Z_j|Z_{-\infty}^{j-1}}[1|Z_{-\infty}^{j-1}]$ is a Markov process with a simple transition kernel.



(a) State S^n known at the receiver

(b) No state information

Fig. 1. Rate-blocklength tradeoff at block error rate $\epsilon = 10^{-2}$ for the Gilbert-Elliott channel with parameters $\delta_1 = 1/2$, $\delta_2 = 0$ and state transition probability $\tau = 0.1$.

Regarding the computation of C_0 it was shown in [5] that

$$\log 2 - \mathbb{E}\left[h(\mathbb{P}[Z_j = 1|Z^{j-1}])\right] \le C_0 \le \log 2 - \mathbb{E}\left[h(\mathbb{P}[Z_j = 1|Z^{j-1}, S_0])\right], \tag{36}$$

where the bounds are asymptotically tight as $j \to \infty$. The computation of the bounds in (36) is challenging because the distributions of $\mathbb{P}[Z_j = 1|Z_1^{j-1}]$ and $\mathbb{P}[Z_j = 1|Z_1^{j-1}, S_0]$ consist of 2^j atoms and therefore are impractical to store exactly. Rounding off the locations of the atoms to fixed quantization levels inside interval $[0, 1]$, as proposed in [5], leads in general to unspecified precision. However, for the special case of $\delta_1, \delta_2 \le 1/2$ the function $h(\cdot)$ is monotonically increasing in the range of values of its argument and it can be shown that rounding down (up) the locations of the atoms shifts the locations of all the atoms on subsequent iterations down (up). Therefore, if rounding is performed this way, the quantized versions of the bounds in (36) are also guaranteed to sandwich C_0.

The proof of Theorem 5 is given in Appendix B.

B. *Discussion and numerical comparisons*

The natural application of (4) is in approximating the maximal achievable rate. Unlike the BSC case (29), the coefficient of the $\log n$ term (or "prelog") for the GEC is unknown. However, the

TABLE I

CAPACITY AND DISPERSION FOR THE GILBERT-ELLIOTT CHANNELS IN FIG. 1

State information	Capacity	Dispersion
known	0.5 bit	2.25 bit^2
unknown	0.280 bit	2.173 bit^2

Parameters: $\delta_1 = 1/2, \delta_2 = 0, \tau = 0.1$.

fact that $\frac{1}{2}\log n$ in (29) is robust to variation in crossover probability, it is natural to conjecture that the unknown prelog for GEC is also $\frac{1}{2}$. With this choice, we arrive to the following approximation which will be used for numerical comparison:

$$\frac{1}{n}\log M^*(n,\epsilon) \approx C - \sqrt{\frac{V}{n}}Q^{-1}(\epsilon) + \frac{1}{2n}\log n\,, \tag{37}$$

with $(C, V) = (C_1, V_1)$, when the state is known at the receiver, and $(C, V) = (C_0, V_0)$, when the state is unknown.

The approximation in (37) is obtained through new non-asymptotic upper and lower bounds on the quantity $\frac{1}{n}\log M^*(n,\epsilon)$, which are given in Appendices A and B. The asymptotic analysis of those bounds led to the approximation (37). It is natural to compare those bounds with the analytical two-parameter approximation (37). Such comparison is shown in Fig. 1. For the case of state known at the receiver, Fig. 1(a), the achievability bound is (98) and the converse bound is (115). For the case of unknown state, Fig. 1(b), the achievability bound is (152) and the converse is (168). The achievability bounds are computed for the maximal probability of error criterion, whereas the converse bounds are for the average probability of error. The values of capacity and dispersion, needed to evaluate (37), are summarized in Table I.

Two main conclusions can be drawn from Fig. 1. First, we see that our bounds are tight enough to get an accurate estimate of $\frac{1}{n}\log M^*(n,\epsilon)$ even for moderate blocklengths n. Second, knowing only two parameters, capacity and dispersion, leads to approximation (37), which is precise enough for addressing the finite-blocklength fundamental limits even for rather short blocklengths. Both of these conclusions have already been observed in [1] for the case of memoryless channels.

Let us discuss two practical applications of (37). First, for the state-known case, the capacity C_1 is independent of the state transition probability τ. However, according to Theorem 4, the channel

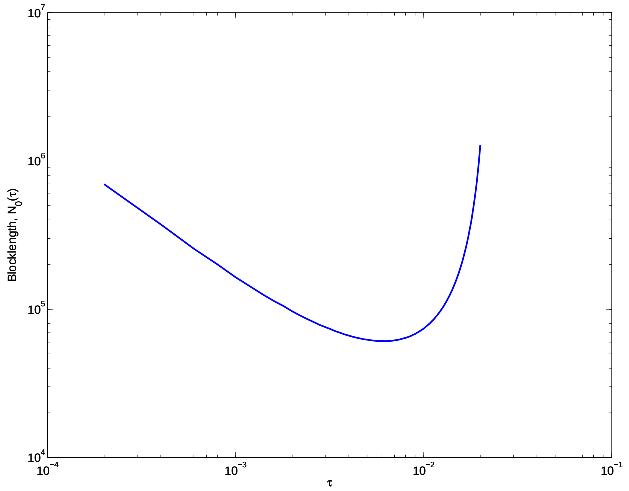


Fig. 2. Minimal blocklength needed to achieve $R = 0.4$ bit and $\epsilon = 0.01$ as a function of state transition probability τ. The channel is the Gilbert-Elliott with no state information at the receiver, $\delta_1 = 1/2, \delta_2 = 0$.

dispersion V_1 does indeed depend on τ. Therefore, according to (3), the minimal blocklength needed to achieve a fraction of capacity behaves as $O\left(\frac{1}{\tau}\right)$ when $\tau \to 0$; see (30). This has an intuitive explanation: to achieve the full capacity of a Gilbert-Elliott channel we need to wait until the influence of the random initial state “washes away”. Since transitions occur on average every $\frac{1}{\tau}$ channel uses, the blocklength should be $O\left(\frac{1}{\tau}\right)$ as $\tau \to 0$. Comparing (28) and (30) we can ascribe a meaning to each of the two terms in (30): the first one gives the dispersion due to the usual BSC noise, whereas the second one is due to memory in the channel.

Next, consider the case in which the state is not known at the decoder. As shown in [5], when the state transition probability τ decreases to 0 the capacity $C_0(\tau)$ increases to C_1. This is sometimes interpreted as implying that if the state is unknown at the receiver slower dynamics are advantageous. Our refined analysis, however, shows that this is true only up to a point.

Indeed, fix a rate $R < C_0(\tau)$ and an $\epsilon > 0$. In view of the tightness of (37), the minimal blocklength, as a function of state transition probability τ needed to achieve rate R is approximately given by

$$N_0(\tau) \approx V_0(\tau)\left(\frac{Q^{-1}(\epsilon)}{C_0(\tau) - R}\right)^2 . \tag{38}$$

When the state transition probability τ decreases we can predict the current state better; on the other hand, we also have to wait longer until the chain “forgets” the initial state. The trade-

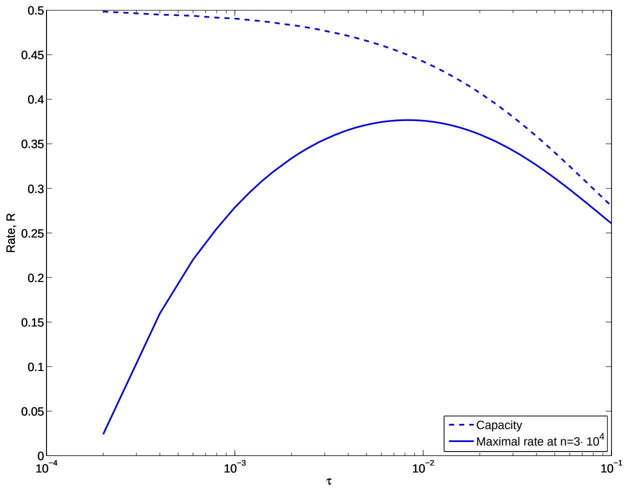


Fig. 3. Comparison of the capacity and the maximal achievable rate $\frac{1}{n}\log M^*(n,\epsilon)$ at blocklength $n = 3 \cdot 10^4$ as a function of the state transition probability τ for the Gilbert-Elliott channel with no state information at the receiver, $\delta_1 = 1/2, \delta_2 = 0$; probability of block error is $\epsilon = 0.01$.

off between these two effects is demonstrated in Fig. 2, where we plot $N_0(\tau)$ for the setup of Fig. 1(b).

The same effect can be demonstrated by analyzing the maximal achievable rate as a function of τ. In view of the tightness of the approximation in (37) for large n we may replace $\frac{1}{n}\log M^*(n,\epsilon)$ with (37). The result of such analysis for the setup in Fig. 1(b) and $n = 3 \cdot 10^4$ is shown as a solid line in Fig. 3, while a dashed line corresponds to the capacity $C_0(\tau)$. Note that at $n = 30000$ (37) is indistinguishable from the upper and lower bounds. We can see that once the blocklength n is fixed, the fact that capacity $C_0(\tau)$ grows when τ decreases does not imply that we can actually transmit at a higher rate. In fact we can see that once τ falls below some critical value, the maximal rate drops steeply with decreasing τ. This situation exemplifies the drawbacks of neglecting the second term in (4).

In general, as $\tau \to 0$ the state availability at the receiver does not affect neither the capacity nor the dispersion too much as the following result demonstrates.

Theorem 6: Assuming $0 < \delta_1, \delta_2 \le 1/2$ and $\tau \to 0$ we have

$$\begin{aligned} C_0(\tau) &\ge C_1 - O(\sqrt{-\tau \ln \tau})\,, && (39)\\ C_0(\tau) &\le C_1 - O(\tau)\,, && (40)\\ V_0(\tau) &= V_1(\tau) + O\left(\left[\frac{-\ln \tau}{\tau}\right]^{3/4}\right) && (41)\\ &= V_1(\tau) + o\left(1/\tau\right)\,. && (42) \end{aligned}$$

The proof is provided in Appendix B. Some observations on the import of Theorem 6 are in order. First, we have already demonstrated that the fact $V_0 = O\left(\frac{1}{\tau}\right)$ as $\tau \to 0$ is important since coupled with (3) it allows us to interpret the quantity $\frac{1}{\tau}$ as a natural "time constant" of the channel. Theorem 6 shows that the same conclusion holds when we do not have state knowledge at the decoder. Second, the evaluation of V_0 based on the Definition (33) is quite challenging[6], whereas in Appendix B we prove upper and lower bounds on V_1; see Lemma 11. Third, Theorem 6 shows that for small values of τ one can approximate the unknown value of V_0 with V_1 given by (30) in closed form. Table I illustrates that such approximation happens to be rather accurate even for moderate values of τ. Consequently, the value of $N_0(\tau)$ for small τ is approximated by replacing $V_0(\tau)$ with $V_1(\tau)$ in (38); in particular this helps quickly locate the extremum of $N_0(\tau)$, cf. Fig. 2.

V. Non-ergodic case: $\tau = 0$

When the range of blocklengths of interest are much smaller than $\frac{1}{\tau}$, we cannot expect (31) or (34) to give a good approximation of $\log M^*(n, \epsilon)$. In fact, in this case, a model with $\tau = 0$ is intuitively much more suitable. In the limit $\tau = 0$ the channel model becomes non-ergodic and a different analysis is needed.

A. Main result

Recall that the main idea behind the asymptotic expansion (4) is in approximating the distribution of an information density by a Gaussian distribution. For non-ergodic channels, it is

[6] Observe that even analyzing $\mathbb{E}\left[F_j\right]$, the entropy rate of the hidden Markov process Z_j, is nontrivial; whereas V_0 requires the knowledge of the spectrum of the process F for zero frequency.

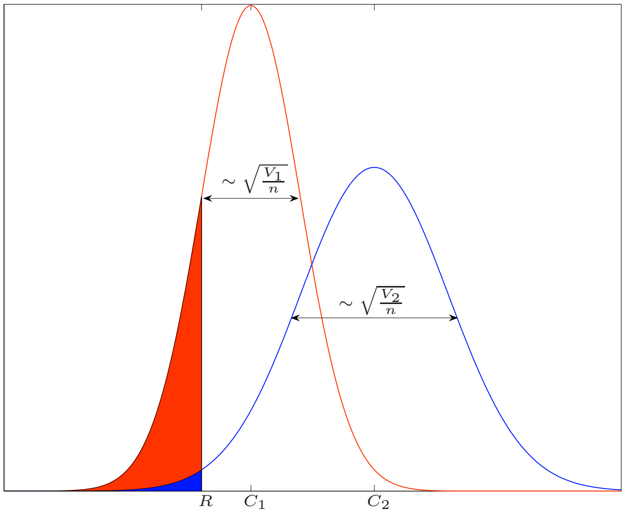


Fig. 4. Illustration to the Definition 2: $R_{na}(n,\epsilon)$ is found as the unique point R at which the weighted sum of two shaded areas equals ϵ.

natural to use an approximation via a mixture of Gaussian distributions. This motivates the next definition.

Definition 2: For a pair of channels with capacities C_1, C_2 and channel dispersions $V_1, V_2 > 0$ we define a *normal approximation* $R_{na}(n,\epsilon)$ of their non-ergodic sum with respective probabilities p_1, p_2 ($p_2 = 1 - p_1$) as the solution to

$$p_1 Q\left((C_1 - R)\sqrt{\frac{n}{V_1}}\right) + p_2 Q\left((C_2 - R)\sqrt{\frac{n}{V_2}}\right) = \epsilon\,. \tag{43}$$

Note that for any $n \ge 1$ and $0 < \epsilon < 1$ the solution exists and is unique, see Fig. 4 for an illustration. To understand better the behavior of $R_{na}(n,\epsilon)$ with n we assume $C_1 < C_2$ and then it can be shown easily that[7]

$$R_{na}(n,\epsilon) = \begin{cases} C_1 - \sqrt{\frac{V_1}{n}} Q^{-1}\left(\frac{\epsilon}{p_1}\right) + O(1/n)\,, & \epsilon < p_1 \\ C_2 - \sqrt{\frac{V_2}{n}} Q^{-1}\left(\frac{\epsilon - p_1}{1-p_1}\right) + O(1/n)\,, & \epsilon > p_1\,. \end{cases} \tag{44}$$

We now state our main result in this section.

Theorem 7: Consider a non-ergodic BSC whose transition probability is $0 < \delta_1 < 1/2$ with probability p_1 and $0 < \delta_2 < 1/2$ with probability $1 - p_1$. Take $C_j = \log 2 - h(\delta_j)$, $V_j = V(\delta_j)$

[7] See the proof of Lemma 15 in Appendix C.

and define $R_{na}(n, \epsilon)$ as the solution to (43). Then for $\epsilon \not\in \{0, p_1, 1\}$ we have

$$\log M^*(n, \epsilon) = nR_{na}(n, \epsilon) + \frac{1}{2} \log n + O(1) \tag{45}$$

regardless of whether ϵ is a maximal or average probability of error, and regardless of whether the state S is known at the transmitter, receiver or both.

The proof of Theorem 7 appears in Appendix C.

B. *Discussion and numerical comparison*

Comparing (45) and (44) we see that, on one hand, there is the usual $\frac{1}{\sqrt{n}}$ type of convergence to capacity. On the other hand, because the capacity in this case depends on ϵ, the argument of Q^{-1} has also changed accordingly. Moreover, we see that for $p_1/2 < \epsilon < p_1$ we have that capacity is equal to $1 - h(\delta_1)$ but the maximal rate approaches it *from above*. In other words, we see that in non-ergodic cases it is possible to communicate at rates above the ϵ-capacity at finite blocklength.

In view of (45) it is natural to choose the following expression as the normal approximation for the $\tau = 0$ case:

$$R_{na}(n, \epsilon) + \frac{1}{2n} \log n\,. \tag{46}$$

We compare converse and achievability bounds against the normal approximation (46) in Fig. 5 and Fig. 6. On the latter we also demonstrate numerically the phenomenon of the possibility of transmitting above capacity. The achievability bounds are computed for the maximal probability of error criterion using (313) from Appendix C with $i(X^n; Y^n)$ given by expression (311), also from Appendix C, in the case of no state knowledge at the receiver; and using (317) with $i(X^n; Y^n S_1)$ given by the (314) from Appendix C in the case when S_1 is available at the receiver. The converse bounds are computed using (334) from Appendix C, that is for the average probability of error criterion and with the assumption of state availability at both the transmitter and the receiver. Note that the "jaggedness" of the curves is a property of the respective bounds, and not of the computational precision.

On comparing the converse bound and the achievability bound in Fig. 6, we conclude that the maximal rate, $\frac{1}{n} \log M^*(n, \epsilon)$ cannot be monotonically increasing with blocklength. In fact, the bounds and approximation hint that it achieves a global maximum at around $n = 200$. We have already observed [1] that for certain ergodic channels and values of ϵ, the supremum of $\frac{1}{n}\log M^*(n,\epsilon)$ need not be its asymptotic value. Although this conflicts with the principal teaching of the error exponent asymptotic analysis (the lower the required error probability, the higher the required blocklength), it does not contradict the fact that for a memoryless channel and any positive integer ℓ

$$\frac{1}{n\ell}\log M^*(n\ell, 1-(1-\epsilon)^\ell) \geq \frac{1}{n}\log M^*(n,\epsilon)\,, \tag{47}$$

since a system with blocklength $n\ell$ can be constructed by ℓ independent encoder/decoders with blocklength n.

The "typical sequence" approach fails to explain the behavior in Fig. 6, as it neglects the possibility that the two BSCs may be affected by an atypical number of errors. Indeed, typicality only holds asymptotically (and the maximal rate converges to the ϵ-capacity, which is equal to the capacity of the bad channel). In the short-run the stochastic variability of the channel is nonneglible, and in fact we see in Fig. 6 that atypically low numbers of errors for the bad channel (even in conjunction with atypically high numbers of errors for the good channel) allow a 20% decrease from the error probability (slightly more than 0.1) that would ensue from transmitting at a rate strictly between the capacities of the bad and good channels.

Before closing this section, we also point out that Fano's inequality is very uninformative in the non-ergodic case. For example, for the setup of Fig. 5 we have

$$\begin{aligned}\limsup_{n\to\infty}\frac{\log M^*(n,\epsilon)}{n} &\leq \limsup_{n\to\infty}\sup_{X^n}\frac{1}{n}\frac{I(X^nS_1;Y^nS_1)+\log 2}{1-\epsilon} &(48)\\ &= \frac{\log 2 - p_1 h(\delta_1) - p_2 h(\delta_2)}{1-\epsilon} &(49)\\ &= 0.71 \text{ bit} &(50)\end{aligned}$$

which is a very loose bound.

VI. Conclusion

As we have found previously in [1], asymptotic expansions such as (4) have practical importance by providing tight approximations of the speed of convergence to (ϵ-) capacity, and by allowing for estimation of the blocklength needed to achieve a given fraction of capacity, as given by (3).

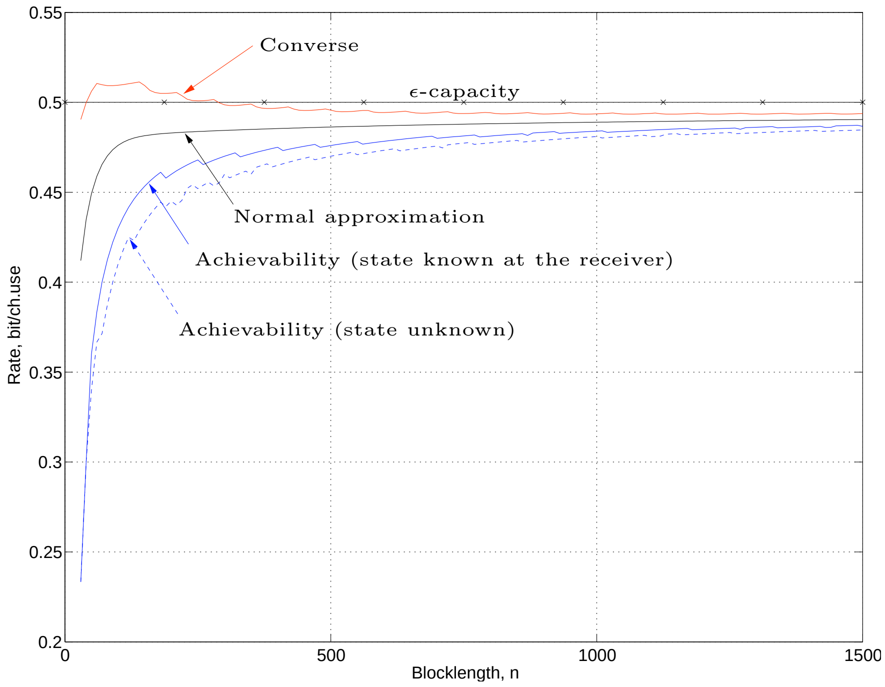


Fig. 5. Rate-blocklength tradeoff at block error rate $\epsilon = 0.03$ for the non-ergodic BSC whose transition probability is $\delta_1 = 0.11$ with probability $p_1 = 0.1$ and $\delta_2 = 0.05$ with probability $p_2 = 0.9$.

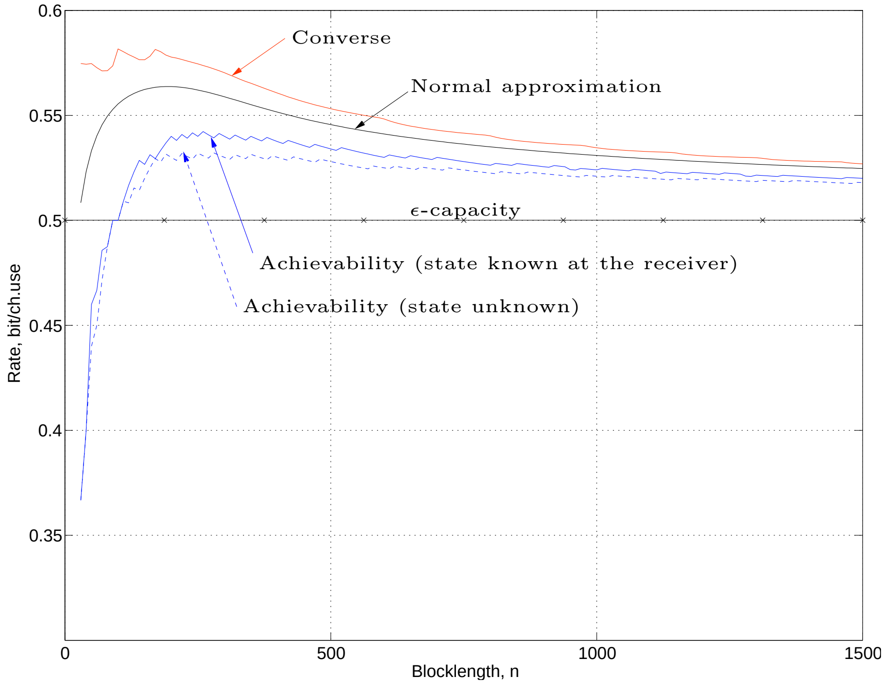


Fig. 6. Rate-blocklength tradeoff at block error rate $\epsilon = 0.08$ for the non-ergodic BSC whose transition probability is $\delta_1 = 0.11$ with probability $p_1 = 0.1$ and $\delta_2 = 0.05$ with probability $p_2 = 0.9$.

In this paper, similar conclusions have been established for two channels with memory. We have proved approximations of the form (4) for the Gilbert-Elliott channel with and without state knowledge at the receiver. In Fig. 1, we have illustrated the relevance of this approximation by comparing it numerically with upper and lower bounds. In addition, we have also investigated the non-ergodic limit case when the influence of the initial state does not dissipate. This non-ergodic model is frequently used to estimate the fundamental limits of shorter blocklength codes. For this regime, we have also proved an expansion similar to (4) and demonstrated its tightness numerically (see Fig. 5 and Fig. 6).

Going beyond quantitative questions, in this paper we have shown that the effect of the dispersion term in (4) can dramatically change our understanding of the fundamental limits of communication. For example, in Fig. 3 we observe that channel capacity fails to predict the qualitative effect of the state transition probability τ on maximal achievable rate even for a rather large blocklength $n = 30000$. Thus, channel capacity alone may offer scant guidance for system design in the finite-blocklength regime. Similarly, in the non-ergodic situation, communicating at rates above the ϵ-capacity of the channel at finite blocklength is possible, as predicted from a dispersion analysis; see Fig. 6.

In conclusion, knowledge of channel dispersion in addition to channel capacity offers fresh insights into the ability of the channel to communicate at blocklengths of practical interest.

REFERENCES

[1] Y. Polyanskiy, H. V. Poor and S. Verdú, "Channel coding rate in the finite blocklength regime," *IEEE Trans. Inform. Theory*, vol. 56, no. 5, May 2010.

[2] E. Biglieri, J. Proakis, and S. Shamai (Shitz), "Fading channels: Information-theoretic and communication aspects," *IEEE Trans. Inform. Theory*, 50th Anniversary Issue, Vol. 44, No. 6, pp. 2619-2692, October 1998.

[3] E. N. Gilbert, "Capacity of burst-noise channels," *Bell Syst. Tech. J.*, Vol. 39, pp. 1253-1265, Sept. 1960.

[4] E. O. Elliott, "Estimates of error rates for codes on burst-noise channels," *Bell Syst. Tech. J.*, Vol. 42, pp. 1977-1997, Sept. 1963

[5] M. Mushkin and I. Bar-David, "Capacity and coding for the Gilbert- Elliott channels," *IEEE Trans. Inform. Theory*, Vol. 35, No. 6, pp. 1277-1290, 1989.

[6] R. G. Gallager, "A simple derivation of the coding theorem and some applications", *IEEE Trans. Inform. Theory*, vol. 11, no. 1, pp. 3-18, 1965.

[7] S. Verdú, *EE528–Information Theory, Lecture Notes,* Princeton University, Princeton, NJ, 2007.

[8] A. N. Tikhomirov, "On the convergence rate in the central limit theorem for weakly dependent random variables," *Theory of Probability and Its Applications*, Vol. XXV, No. 4, 1980.

[9] Y. Polyanskiy, H. V. Poor and S. Verdú, "Dispersion of Gaussian channels," *Proc. IEEE Int. Symp. Information Theory (ISIT)*, Seoul, Korea, 2009.

[10] I. A. Ibragimov, "Some limit theorems for stationary processes," *Theor. Prob. Appl.*, Vol. 7, No. 4, 1962.

[11] J.C. Kieffer, "Epsilon-capacity of binary symmetric averaged channels," *IEEE Trans. Inform. Theory,* Vol 53, No. 1, pp. 288–303, 2007.

[12] S. Verdú and T. S. Han, "A general formula for channel capacity," *IEEE Trans. Inform. Theory*, vol. 40, no. 4, pp. 1147-1157, 1994.

[13] W. Feller, *An Introduction to Probability Theory and Its Applications, Volume II*, Second edition, John Wiley & Sons, Inc., New York, 1971.

[14] G. Birkhoff, "Extensions of Jentzsch's theorem.", *Trans. of AMS*, 85:219-227, 1957.

[15] T. Holliday, A. Goldsmith, and P. Glynn, "Capacity of finite state channels based on Lyapunov exponents of random matrices," *IEEE Trans. Inform. Theory*, vol. 52, no. 8, pp. 3509-3532, Aug 2006.

[16] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems,* Academic, New York, 1981.

APPENDIX A
PROOF OF THEOREM 4

Proof: Achievability: We choose P_{X^n} – equiprobable. To model the availability of the state information at the receiver, we assume that the output of the channel is (Y^n, S^n). Thus we need to write down the expression for $i(X^n; Y^n S^n)$. To do that we define an operation on $\mathbb{R} \times \{0, 1\}$:

$$a^{\{b\}} = \begin{cases} 1 - a\,, & b = 0\,, \\ a\,, & b = 1 \end{cases} . \tag{51}$$

Then we obtain

$$\begin{aligned} i(X^n; Y^n S^n) &= \log \frac{P_{Y^n|X^n S^n}(Y^n|X^n, S^n)}{P_{Y^n|S^n}(Y^n|S^n)} & (52) \\ &= n \log 2 + \sum_{j=1}^{n} \log \delta_{S_j}^{\{Z_j\}}\,, & (53) \end{aligned}$$

where (52) follows since $P_{S^n|X^n}(s^n|x^n) = P_{S^n}(s^n)$ by independence of X^n and S^n, (53) is because under equiprobable X^n we have that $P_{Y^n|S^n}$ is also equiprobable, while $P_{Y_j|X_j S_j}(Y_j|X_j, S_j)$ is equal to $\delta_{S_j}^{\{Z_j\}}$ with Z_j defined in (7). Using (53) we find

$$\mathbb{E}\left[i(X^n; Y^n S^n)\right] = nC_1\,. \tag{54}$$

The next step is to compute $\mathrm{Var}[i(X^n; Y^n S^n)]$. For convenience we write

$$h_a = \frac{1}{2}[h(\delta_1) + h(\delta_2)] \tag{55}$$

and

$$\Theta_j \quad = \quad \log \delta_{S_j}^{\{Z_j\}} \,. \tag{56}$$

Therefore

$$\begin{aligned}
\sigma_n^2 &\overset{\triangle}{=} \mathrm{Var}[i(X^n; Y^n S^n)] & (57)\\
&= \mathbb{E}\left[\left(\sum_{j=1}^n \Theta_j\right)^2\right] - n^2 h_a^2 & (58)\\
&= \sum_{j=1}^n \mathbb{E}\left[\Theta_j^2\right] + 2\sum_{i<j} \mathbb{E}\left[\Theta_i \Theta_j\right] - n^2 h_a^2 & (59)\\
&= n\mathbb{E}\left[\Theta_1^2\right] + 2\sum_{k=1}^n (n-k)\mathbb{E}\left[\Theta_1 \Theta_{1+k}\right] - n^2 h_a^2 & (60)\\
&= n(\mathbb{E}\left[\Theta_1^2\right] - h_a^2) \\
&\quad +2\sum_{k=1}^n (n-k)\mathbb{E}\left[h\left(\delta_{S_1}\right) h\left(\delta_{S_{1+k}}\right) - h_a^2\right] \,, & (61)
\end{aligned}$$

where (60) follows by stationarity and (61) by conditioning on S^n and regrouping terms.

Before proceeding further we define an α-mixing coefficient of the process (S_j, Z_j) as

$$\alpha(n) \quad = \quad \sup \left|\mathbb{P}[A,B] - \mathbb{P}[A]\mathbb{P}[B]\right| \,, \tag{62}$$

where the supremum is over $A \in \sigma\{S_{-\infty}^0, Z_{-\infty}^0\}$ and $B \in \sigma\{S_n^\infty, Z_n^\infty\}$; by $\sigma\{\cdots\}$ we denote a σ-algebra generated by a collection of random variables. Because S_j is such a simple Markov process it is easy to show that for any $a, b \in \{1, 2\}$ we have

$$\frac{1}{2} - \frac{1}{2}|1-2\tau|^n \leq \mathbb{P}[S_n = a | S_0 = b] \leq \frac{1}{2} + \frac{1}{2}|1-2\tau|^n \,, \tag{63}$$

and, hence,

$$\alpha(n) \leq |1-2\tau|^n \,. \tag{64}$$

By Lemma 1.2 of [10] for any pair of bounded random variables U and V measurable with respect to $\sigma\{S_j, j \leq m\}$ and $\sigma\{S_j, j \geq m+n\}$, respectively, we have

$$\left|\mathbb{E}\left[UV\right] - \mathbb{E}\left[U\right]\mathbb{E}\left[V\right]\right| \leq 16\alpha(n) \cdot \text{ess sup } |U| \cdot \text{ess sup } |V| \,. \tag{65}$$

Then we can conclude that since $\left|h\left(\delta_{S_1}\right)\right| \leq \log 2$ we have for some constant B_3

$$\begin{aligned}
&\left|\sum_{k=1}^{n} k\mathbb{E}\left[h\left(\delta_{S_1}\right)h\left(\delta_{S_{1+k}}\right)-h_a^2\right]\right| \\
&\quad\leq \sum_{k=1}^{n} k\mathbb{E}\left[\left|h\left(\delta_{S_1}\right)h\left(\delta_{S_{1+k}}\right)-h_a^2\right|\right] && (66)\\
&\quad\leq \sum_{k=1}^{n} 16k\alpha(k)\log^2 2 && (67)\\
&\quad\leq B_3\sum_{k=1}^{\infty} k(1-2\tau)^k && (68)\\
&\quad= O(1)\,, && (69)
\end{aligned}$$

where (67) is by (65) and (68) is by (80). On the other hand,

$$\begin{aligned}
&n\left|\sum_{k=n+1}^{\infty}\mathbb{E}\left[h\left(\delta_{S_1}\right)h\left(\delta_{S_{1+k}}\right)-h_a^2\right]\right| && (70)\\
&\quad\leq 16n\sum_{k=n+1}^{\infty}\alpha(k)\log^2 2 && (71)\\
&\quad\leq 16Kn\sum_{k=n+1}^{\infty}(1-2\tau)^k\log^2 2 && (72)\\
&\quad= O(1)\,. && (73)
\end{aligned}$$

Therefore, we have proved that

$$\begin{aligned}
&\sum_{k=1}^{n}(n-k)\mathbb{E}\left[h\left(\delta_{S_1}\right)h\left(\delta_{S_{1+k}}\right)-h_a^2\right] && (74)\\
&\quad= n\sum_{k=1}^{n}\mathbb{E}\left[h\left(\delta_{S_1}\right)h\left(\delta_{S_{1+k}}\right)-h_a^2\right]+O(1) && (75)\\
&\quad= n\sum_{k=1}^{\infty}\mathbb{E}\left[h\left(\delta_{S_1}\right)h\left(\delta_{S_{1+k}}\right)-h_a^2\right]+O(1)\,, && (76)
\end{aligned}$$

A straightforward calculation reveals that

$$\begin{aligned}
&\sum_{k=1}^{\infty}\mathbb{E}\left[h\left(\delta_{S_1}\right)h\left(\delta_{S_{1+k}}\right)-h_a^2\right] && (77)\\
&\quad= \frac{1}{4}\left(h\left(\delta_1\right)-h\left(\delta_2\right)\right)^2\left[\frac{1}{2\tau}-1\right]\,. && (78)
\end{aligned}$$

Therefore, using (76) and (78) in (61), we obtain after some algebra that

$$\sigma_n^2 = \mathrm{Var}[i(X^n;Y^nS^n)] = nV_1 + O(1)\,. \tag{79}$$

By (53) we see that $i(X^n;Y^nS^n)$ is a sum over an α-mixing process. For such sums the following theorem of Tikhomirov [8] serves the same purpose in this paper as the Berry-Esseen inequality does in [1] and [9].

Theorem 8: Suppose that a stationary zero-mean process $X_1, X_2, \ldots$ is α-mixing and for some positive K, β and γ we have

$$\begin{aligned} \alpha(k) &\leq Ke^{-\beta k}\,, & (80)\\ \mathbb{E}\left[|X_1|^{4+\gamma}\right] &< \infty & (81)\\ \sigma_n^2 &\to \infty\,, & (82) \end{aligned}$$

where

$$\sigma_n^2 = \mathbb{E}\left[\left(\sum_1^n X_j\right)^2\right]\,. \tag{83}$$

Then, there is a constant B, depending on K, β and γ, such that

$$\sup_{x\in\mathbb{R}}\left|\mathbb{P}\left[\sum_1^n X_j \geq x\sqrt{\sigma_n^2}\right] - Q(x)\right| \leq \frac{B\log n}{\sqrt{n}}\,. \tag{84}$$

Application of Theorem 8 to $i(X^n;Y^nS^n)$ proves that

$$\left|\mathbb{P}\left[i(X^n;Y^nS^n) \geq nC_1 + \sqrt{\sigma_n^2}x\right] - Q(x)\right| \leq \frac{B\log n}{\sqrt{n}}\,. \tag{85}$$

But then for arbitrary λ there exists some constant $B_2 > B$ such that we have

$$\begin{aligned} &\left|\mathbb{P}\left[i(X^n;Y^nS^n) \geq nC_1 + \sqrt{nV_1}\lambda\right] - Q(\lambda)\right| & (86)\\ &= \left|\mathbb{P}\left[i(X^n;Y^nS^n) \geq nC_1 + \sqrt{\sigma_n^2}\sqrt{\frac{nV_1}{\sigma_n^2}}\lambda\right] - Q(\lambda)\right| & (87)\\ &\leq \frac{B\log n}{\sqrt{n}} + \left|Q(\lambda) - Q\left(\lambda\sqrt{\frac{nV_1}{\sigma_n^2}}\right)\right| & (88)\\ &= \frac{B\log n}{\sqrt{n}} + \left|Q(\lambda) - Q\left(\lambda + O(1/n)\right)\right| & (89)\\ &\leq \frac{B\log n}{\sqrt{n}} + O(1/n) & (90)\\ &\leq \frac{B_2\log n}{\sqrt{n}}\,, & (91) \end{aligned}$$

where (88) is by (85), (89) is by (79) and (90) is by Taylor's theorem.

Now, we state an auxiliary lemma to be proved later.

Lemma 9: Let $X_1, X_2, \ldots$ be a process satisfying the conditions of Theorem 8; then for any constant A

$$\mathbb{E}\left[\exp\left\{-\sum_{j=1}^{n} X_j\right\} \cdot 1\left\{\sum_{j=1}^{n} X_j > A\right\}\right] \le 2\left(\frac{\log 2}{\sqrt{2\pi\sigma_n^2}} + \frac{2B\log n}{\sqrt{n}}\right)\exp\{-A\}\,, \tag{92}$$

where B is the constant in (84).

Observe that there exists some $B_1 > 0$ such that

$$\begin{aligned} 2\left(\frac{\log 2}{\sqrt{2\pi\sigma_n^2}} + \frac{2B\log n}{\sqrt{n}}\right) &= 2\left(\frac{\log 2}{\sqrt{2\pi(nV + O(1))}} + \frac{2B\log n}{\sqrt{n}}\right) &(93)\\ &\le \frac{B_1\log n}{\sqrt{n}}\,, &(94)\end{aligned}$$

where σ_n^2 is defined in (57) and (93) follows from (79). Therefore, from (94) we conclude that there exists a constant B_1 such that for any A

$$\mathbb{E}\left[\exp\{-i(X^n;Y^nS^n) + A\} \cdot 1\{i(X^n;Y^nS^n) \ge A\}\right] \le \frac{B_1\log n}{\sqrt{n}}\,, \tag{95}$$

Finally, we set

$$\log\tfrac{M-1}{2} = nC - \sqrt{nV}Q^{-1}(\epsilon_n)\,, \tag{96}$$

where

$$\epsilon_n = \epsilon - \frac{(B_1 + B_2)\log n}{\sqrt{n}}\,. \tag{97}$$

Then, by Theorem 1 we know that there exists a code with M codewords and average probability of error p_e bounded by

$$\begin{aligned} p_e &\le \mathbb{E}\left[\exp\left\{-\left[i(X^n;Y^nS^n) - \log\tfrac{M-1}{2}\right]^+\right\}\right] &(98)\\ &\le \mathbb{P}\left[i(X^n;Y^nS^n) \le \log\tfrac{M-1}{2}\right] + \frac{B_1}{\sqrt{n}} &(99)\\ &\le \epsilon_n + \frac{(B_1 + B_2)\log n}{\sqrt{n}} &(100)\\ &\le \epsilon\,, &(101)\end{aligned}$$

where (99) is by (95) with $A = \log\frac{M-1}{2}$, (100) is by (91) and (96), and (101) is by (97). Therefore, invoking Taylor's expansion of Q^{-1} in (96) we have

$$\log M^*(n,\epsilon) \ge \log M \ge nC - \sqrt{nV}Q^{-1}(\epsilon) + O(\log n)\,. \tag{102}$$

This proves the achievability bound with the average probability of error criterion.

However, as explained in [1], the proof of Theorem 1 relies only on pairwise independence of the codewords in the ensemble of codes. Therefore, if $M = 2^k$ for an integer k, a fully random ensemble of M equiprobable binary strings may be replaced with an ensemble of 2^k codewords of a random linear $[k, n]$ code. But a maximum likelihood decoder for such a code can be constructed so that the maximal probability of error coincides with the average probability of error; see Appendix A of [1] for complete details. In this way, the above argument actually applies to both average and maximal error criteria after replacing $\log M$ by $\lfloor \log M \rfloor$, which is asymptotically immaterial.

Converse: In the converse part we will assume that the transmitter has access to the full state sequence S^n and then generates X^n based on both the input message and S^n. Take the best such code with $M^*(n, \epsilon)$ codewords and average probability of error no greater than ϵ. We now propose to treat the pair (X^n, S^n) as a combined input to the channel (but the S^n part is independent of the message) and the pair (Y^n, S^n) as a combined output, available to the decoder. Note that in this situation, the encoder induces a distribution $P_{X^n S^n}$ and is necessarily randomized because the distribution of S^n is not controlled by the input message and is given by the output of the Markov chain.

To apply Theorem 2 we choose the auxiliary channel which passes S^n unchanged and generates Y^n equiprobably:

$$Q_{Y^n|X^n S^n}(y^n, s^n|x^n) = 2^{-n} \quad \text{for all } x^n, y^n, s^n\,. \tag{103}$$

Note that by the constraint on the encoder, S^n is independent of the message W. Moreover, under Q-channel the Y^n is also independent of W and we clearly have

$$\epsilon' \geq 1 - \frac{1}{M^*}\,. \tag{104}$$

Therefore by Theorem 2 we obtain

$$\beta_{1-\epsilon}\left(P_{X^n Y^n S^n}, Q_{X^n Y^n S^n}\right) \leq \frac{1}{M^*}\,. \tag{105}$$

To lower bound $\beta_{1-\epsilon}\left(P_{X^nY^nS^n}, Q_{X^nY^nS^n}\right)$ via (24) we notice that

$$\begin{aligned}\log\frac{P_{X^nY^nS^n}(x^n,y^n,s^n)}{Q_{X^nY^nS^n}(x^n,y^n,s^n)} &= \log\frac{P_{Y^n|X^nS^n}(y^n|x^n,s^n)P_{X^nS^n}(x^n,s^n)}{Q_{Y^n|X^nS^n}(y^n|x^n,s^n)Q_{X^nS^n}(x^n,s^n)} &(106)\\ &= \log\frac{P_{Y^n|X^nS^n}(y^n|x^n,s^n)}{Q_{Y^n|X^nS^n}(y^n|x^n,s^n)} &(107)\\ &= i(x^n;y^ns^n)\,, &(108)\end{aligned}$$

where (107) is because $P_{X^nS^n} = Q_{X^nS^n}$ and (108) is simply by noting that $P_{Y^n|S^n}$ in the definition (52) of $i(X^n;Y^nS^n)$ is also equiprobable and, hence, is equal to $Q_{Y^n|X^nS^n}$. Now set

$$\log\gamma = nC - \sqrt{nV}Q^{-1}(\epsilon_n)\,, \tag{109}$$

where this time

$$\epsilon_n = \epsilon + \frac{B_2\log n}{\sqrt{n}} + \frac{1}{\sqrt{n}}\,. \tag{110}$$

By (24) we have for $\alpha = 1-\epsilon$ that

$$\begin{aligned}\beta_{1-\epsilon} &\geq \frac{1}{\gamma}\left(1-\epsilon-\mathbb{P}\left[\log\frac{P_{X^nY^nS^n}(X^n,Y^n,S^n)}{Q_{X^nY^nS^n}(X^n,Y^n,S^n)}\geq\log\gamma\right]\right) &(111)\\ &= \frac{1}{\gamma}\left(1-\epsilon-\mathbb{P}\left[i(X^n;Y^nS^n)\geq\log\gamma\right]\right) &(112)\\ &\geq \frac{1}{\gamma}\left(1-\epsilon-(1-\epsilon_n)-\frac{B_2\log n}{\sqrt{n}}\right) &(113)\\ &= \frac{1}{\sqrt{n}\gamma}\,, &(114)\end{aligned}$$

where (112) is by (108), (113) is by (91) and (114) is by (110).

Finally,

$$\begin{aligned}\log M^*(n,\epsilon) &\leq \log\frac{1}{\beta_{1-\epsilon}} &(115)\\ &\leq \log\gamma + \frac{1}{2}\log n &(116)\\ &= nC - \sqrt{nV}Q^{-1}(\epsilon_n) + \frac{1}{2}\log n &(117)\\ &= nC - \sqrt{nV}Q^{-1}(\epsilon) + O(\log n)\,, &(118)\end{aligned}$$

where (115) is just (105), (116) is by (114), (117) is by (109) and (118) is by Taylor's formula applied to Q^{-1} using (110) for ϵ_n.

■

Proof of Lemma 9: By Theorem 8 for any z we have that

$$\begin{aligned} & \mathbb{P}\left[z \le \sum_{j=1}^{n} X_j < z + \log 2\right] \\ \le & \int_{z/\sigma_n}^{(z+\log 2)/\sigma_n} \frac{1}{\sqrt{2\pi}} e^{-t^2/2} dt + \frac{2B \log n}{\sqrt{n}} \,. & (119) \\ \le & \frac{\log 2}{\sigma_n \sqrt{2\pi}} + \frac{2B \log n}{\sqrt{n}} \,. & (120) \end{aligned}$$

On the other hand,

$$\begin{aligned} & \mathbb{E}\left[\exp\left\{-\sum_{j=1}^{n} X_j\right\} \cdot 1\left\{\sum_{j=1}^{n} X_j > A\right\}\right] \\ \le & \sum_{l=0}^{\infty} \exp\{-A - l \log 2\} \, \mathbb{P}\left[A + l \log 2 \le \sum_{j=1}^{n} X_j < A + (l+1) \log 2\right] \,. & (121) \end{aligned}$$

Using (120) we get (92) after noting that

$$\sum_{l=0}^{\infty} 2^{-l} = 2 \,. \tag{122}$$

■

Appendix B
Proofs of Theorems 5 and 6

For convenience, we begin by summarizing the definitions and some of the well-known properties of the processes used in this appendix:

$$\begin{aligned} R_j &= \mathbb{P}[S_{j+1} = 1 | Z_1^j] \,, & (123) \\ Q_j &= \mathbb{P}[Z_{j+1} = 1 | Z_1^j] = \delta_1 R_j + \delta_2 (1 - R_j) \,, & (124) \\ R_j^* &= \mathbb{P}[S_{j+1} = 1 | Z_1^j, S_0] \,, & (125) \\ G_j &= -\log P_{Z_j | Z_1^{j-1}}(Z_j | Z_1^{j-1}) = -\log Q_{j-1}^{\{Z_j\}} \,, & (126) \\ \Psi_j &= \mathbb{P}[S_{j+1} = 1 | Z_{-\infty}^j] \,, & (127) \\ U_j &= \mathbb{P}[Z_{j+1} = 1 | Z_{-\infty}^j] = \delta_1 \Psi_j + \delta_2 (1 - \Psi_j) \,, & (128) \\ F_j &= -\log P_{Z_j | Z_{-\infty}^{j-1}}(Z_j | Z_{-\infty}^{j-1}) = -\log U_{j-1}^{\{Z_j\}} \,, & (129) \\ \Theta_j &= \log P_{Z_j | S_j}(Z_j | S_j) = \log \delta_{S_j}^{\{Z_j\}} \,, & (130) \\ \Xi_j &= F_j + \Theta_j \,. & (131) \end{aligned}$$

With this notation, the entropy rate of the process Z_j is given by

$$\begin{aligned}\mathcal{H} &= \lim_{n\to\infty}\frac{1}{n}H(Z^n) && (132)\\ &= \mathbb{E}\left[F_0\right] && (133)\\ &= \mathbb{E}\left[h(U_0)\right]\,. && (134)\end{aligned}$$

Define two functions $T_{0,1}:[0,1]\mapsto[\tau,1-\tau]$:

$$\begin{aligned}T_0(x) &= \frac{x(1-\tau)(1-\delta_1)+(1-x)\tau(1-\delta_2)}{x(1-\delta_1)+(1-x)(1-\delta_2)}\,, && (135)\\ T_1(x) &= \frac{x(1-\tau)\delta_1+(1-x)\tau\delta_2}{x\delta_1+(1-x)\delta_2}\,. && (136)\end{aligned}$$

Applying Bayes formula to the conditional probabilities in (123), (125) and (127) yields[8]

$$\begin{aligned}R_{j+1} &= T_{Z_{j+1}}(R_j)\,, j\geq 0\,,\ \text{a.s.} && (137)\\ R^*_{j+1} &= T_{Z_{j+1}}(R^*_j)\,, j\geq -1\,,\ \text{a.s.} && (138)\\ \Psi_{j+1} &= T_{Z_{j+1}}(\Psi_j)\,, j\in\mathbb{Z}\,,\ \text{a.s.} && (139)\end{aligned}$$

where we start R_j and R^*_j as follows:

$$\begin{aligned}R_0 &= 1/2\,, && (140)\\ R^*_0 &= (1-\tau)1\{S_0=1\}+\tau 1\{S_0=2\}\,. && (141)\end{aligned}$$

In particular, R_j, R^*_j, Q_j, Ψ_j and U_j are Markov processes.

Because of (139) we have

$$\min(\tau,1-\tau)\leq\Psi_j\leq\max(\tau,1-\tau)\,. \qquad (142)$$

For any pair of points $0<x,y<1$ denote their projective distance (as defined in [14]) by

$$d_P(x,y)=\left|\ln\frac{x}{1-x}-\ln\frac{y}{1-y}\right|\,. \qquad (143)$$

As shown in [14] operators T_0 and T_1 are contracting in this distance (see also Section V.A of [15]):

$$d_P(T_a(x),T_a(y))\leq|1-2\tau|d_P(x,y)\,. \qquad (144)$$

[8] Since all conditional expectations are defined only up to almost sure equivalence, the qualifier “a.s.” will be omitted below when dealing with such quantities.

Since the derivative of $\ln \frac{x}{1-x}$ is lower-bounded by 4 we also have

$$|x-y| \le \frac{1}{4} d_P(x,y)\,, \tag{145}$$

which implies for all $a \in \{0,1\}$ that

$$|T_a(x) - T_a(y)| \le \frac{1}{4}|1-2\tau| d_P(x,y)\,. \tag{146}$$

Applying (146) to (137)-(139) and in the view of (140) and (142) we obtain

$$\begin{aligned} |R_j - \Psi_j| &\le \frac{1}{4}\left|\ln\frac{\tau}{1-\tau}\right| |1-2\tau|^{j-1} \qquad j \ge 1\,, &(147)\\ |Q_j - U_j| &\le \frac{|\delta_1-\delta_2|}{4}\left|\ln\frac{\tau}{1-\tau}\right| |1-2\tau|^{j-1} \qquad j \ge 1\,. &(148)\end{aligned}$$

Proof of Theorem 5: Achievability: In this proof we demonstrate how a central-limit theorem (CLT) result for the information density implies the $o(\sqrt{n})$ expansion. Otherwise, the proof is a repetition of the proof of Theorem 4. In particular, with equiprobable P_{X^n}, the expression for the information density $i(X^n;Y^n)$ becomes

$$\begin{aligned} i(X^n;Y^n) &= n\log 2 + \log P_{Z^n}(Z^n)\,, &(149)\\ &= n\log 2 + \sum_{j=1}^n G_j\,. &(150)\end{aligned}$$

One of the main differences with the proof of Theorem 4 is that the process G_j need not be α-mixing. In fact, for a range of values of δ_1, δ_2 and τ it can be shown that all (Z_j, G_j), $j = 1 \ldots n$ can be reconstructed by knowing G_n. Consequently, α-mixing coefficients of G_j are all equal to $1/4$, hence G_j is not α-mixing and Theorem 8 is not applicable. At the same time G_j is mixing and ergodic (and Markov) because the underlying time-shift operator is Bernoulli.

Nevertheless, Theorem 2.6 in [10] provides a CLT extension of the classic Shannon-MacMillan-Breiman theorem. Namely it proves that the process $\frac{1}{\sqrt{n}}\log P_{Z^n}(Z^n)$ is asymptotically normal with variance V_0. Or, in other words, for any $\lambda \in \mathbb{R}$ we can write

$$\mathbb{P}\left[i(X^n;Y^n) > nC_0 + \sqrt{nV_0}\lambda\right] \to Q(\lambda)\,. \tag{151}$$

Conditions of Theorem 2.6 in [10] are fulfilled because of (64) and (148). Note that Appendix I.A of [15] also establishes (151) but with an additional assumption $\delta_1, \delta_2 > 0$.

By Theorem 1 we know that there exists a code with M codewords and average probability of error p_e bounded as

$$\begin{aligned} p_e &\leq \mathbb{E}\left[\exp\left\{-\left[i(X^n;Y^n) - \log\tfrac{M-1}{2}\right]^+\right\}\right] && (152)\\ &\leq \mathbb{E}\left[\exp\left\{-\left[i(X^n;Y^n) - \log M\right]^+\right\}\right] && (153)\end{aligned}$$

where (153) is by monotonicity of $\exp\{-[i(X^n;Y^n)-a]^+\}$ with respect to a. Furthermore, notice that for any random variable U and $a, b \in \mathbb{R}$ we have[9]

$$\mathbb{E}\left[\exp\left\{-\left[U-a\right]^+\right\}\right] \leq \mathbb{P}[U \leq b] + \exp\{a-b\}\,. \tag{154}$$

Fix some $\epsilon' > 0$ and set

$$\log\gamma_n = nC_0 - \sqrt{nV_0}Q^{-1}(\epsilon-\epsilon')\,. \tag{155}$$

Then continuing from (153) we obtain

$$\begin{aligned} p_e &\leq \mathbb{P}[i(X^n;Y^n) \leq \log\gamma_n] + \exp\{\log M - \log\gamma_n\} && (156)\\ &= \epsilon - \epsilon' + o(1) + \frac{M}{\gamma_n}\,, && (157)\end{aligned}$$

where (156) follows by applying (154) and (157) is by (151). If we set $\log M = \log\gamma_n - \log n$ then the right-hand side of (157) for sufficiently large n falls below ϵ. Hence we conclude that for n large enough we have

$$\begin{aligned} \log M^*(n,\epsilon) &\geq \log\gamma_n - \log n && (158)\\ &\geq nC_0 - \sqrt{nV_0}Q^{-1}(\epsilon-\epsilon') - \log n\,, && (159)\end{aligned}$$

but since ϵ' is arbitrary,

$$\log M^*(n,\epsilon) \geq nC_0 - \sqrt{nV_0}Q^{-1}(\epsilon) + o(\sqrt{n})\,. \tag{160}$$

Converse: To apply Theorem 2 we choose the auxiliary channel $Q_{Y^n|X^n}$ which simply outputs an equiprobable Y^n independent of the input X^n:

$$Q_{Y^n|X^n}(y^n|x^n) = 2^{-n}\,. \tag{161}$$

[9] This upper-bound reduces (152) to the usual Feinstein Lemma.

Similar to the proof of Theorem 4 we get

$$\beta_{1-\epsilon}\left(P_{X^nY^n}, Q_{X^nY^n}\right) \le \frac{1}{M^*}\,, \tag{162}$$

and also

$$\begin{aligned}\log\frac{P_{X^nY^n}(X^n,Y^n)}{Q_{X^nY^n}(X^n,Y^n)} &= n\log 2 + \log P_{Z^n}(Z^n) && (163)\\ &= i(X^n;Y^n)\,. && (164)\end{aligned}$$

We choose $\epsilon' > 0$ and set

$$\log\gamma_n = nC_0 - \sqrt{nV_0}Q^{-1}(\epsilon+\epsilon')\,. \tag{165}$$

By (24) we have, for $\alpha = 1-\epsilon$,

$$\begin{aligned}\beta_{1-\epsilon} &\ge \frac{1}{\gamma_n}\left(1-\epsilon-\mathbb{P}\left[i(X^n;Y^n)\ge\log\gamma_n\right]\right) && (166)\\ &= \frac{1}{\gamma_n}(\epsilon'+o(1))\,, && (167)\end{aligned}$$

where (167) is from (151). Finally, from (162) we obtain

$$\begin{aligned}\log M^*(n,\epsilon) &\le \log\frac{1}{\beta_{1-\epsilon}} && (168)\\ &= \log\gamma_n - \log(\epsilon'+o(1)) && (169)\\ &= nC_0 - \sqrt{nV_0}Q^{-1}(\epsilon+\epsilon') + O(1) && (170)\\ &= nC_0 - \sqrt{nV_0}Q^{-1}(\epsilon) + o(\sqrt{n})\,. && (171)\end{aligned}$$

■

Proof of Theorem 6: Without loss of generality, we assume everywhere throughout the remainder of the appendix

$$0 < \delta_2 \le \delta_1 \le 1/2\,. \tag{172}$$

The bound (39) follows from Lemma 10: (40) follows from (176) after observing that when $\delta_2 > 0$ the right-hand side of (176) is $O(\tau)$ when $\tau\to 0$. Finally, by (177) we have

$$B_0 = O\left(\sqrt{-\tau\ln\tau}\right) \tag{173}$$

which implies that

$$\frac{B_1}{B_0} = O\left(\frac{-\ln^{3/4}\tau}{\tau^{1/4}}\right)\,. \tag{174}$$

Substituting these into the definition of Δ in Lemma 11, see (199), we obtain

$$\Delta = O\left(\sqrt{\frac{-\ln^3\tau}{\tau}}\right) \tag{175}$$

as $\tau \to 0$. Then (41) follows from Lemma 11 and (30). ■

Lemma 10: For any $0 < \tau < 1$ the difference $C_1 - C_0$ is lower bounded as

$$C_1 - C_0 \geq h(\delta_1\tau_{max} + \delta_2\tau_{min}) - \tau_{max}h(\delta_1) - \tau_{min}h(\delta_2)\,, \tag{176}$$

where $\tau_{max} = \max(\tau, 1-\tau)$ and $\tau_{min} = \min(\tau,1-\tau)$. Furthermore, when $\tau \to 0$ we have

$$C_1 - C_0 \leq O\left(\sqrt{-\tau\ln\tau}\right)\,. \tag{177}$$

Proof: First, notice that

$$C_1 - C_0 = \mathcal{H} - H(Z_1|S_1) = \mathbb{E}\left[\Xi_1\right], \tag{178}$$

where $\mathcal{H}$ and Ξ_j were defined in (132) and (131), respectively. On the other hand we can see that

$$\mathbb{E}\left[\Xi_1|Z_{-\infty}^0\right] \;=\; f(\Psi_0)\,, \tag{179}$$

where f is a non-negative, concave function on $[0,1]$, which attains 0 at the endpoints; explicitly,

$$f(x) = h(\delta_1 x + \delta_2(1-x)) - xh(\delta_1) - (1-x)h(\delta_2)\,. \tag{180}$$

Since we know that Ψ_0 almost surely belongs to the interval between τ and $1-\tau$ we obtain after trivial algebra

$$f(x) \geq \min_{t\in[\tau_{min},\tau_{max}]} f(t) = f(\tau_{max})\,, \quad \forall x \in [\tau_{min},\tau_{max}]\,. \tag{181}$$

Taking expectation in (179) and using (181) we prove (176).

On the other hand,

$$\begin{aligned} C_1 - C_0 &= \mathcal{H} - H(Z_1|S_1) && (182)\\ &= \mathbb{E}\left[h(\delta_1\Psi_0 + \delta_2(1-\Psi_0)) - h(\delta_1 1\{S_1 = 1\} + \delta_2 1\{S_1 = 2\})\right]. && (183) \end{aligned}$$

Because $\delta_2 > 0$ we have

$$B = \max_{x\in[0,1]}\left|\frac{d}{dx}h(\delta_1 x + \delta_2(1-x))\right| < \infty\,. \tag{184}$$

So we have

$$\begin{aligned}\mathbb{E}\left[\Xi_1\right] &\leq B\mathbb{E}\left[\left|\Psi_0 - 1\{S_1 = 1\}\right|\right] &(185)\\ &\leq B\sqrt{\mathbb{E}\left[(\Psi_0 - 1\{S_1 = 1\})^2\right]}\,, &(186)\end{aligned}$$

where (186) follows from the Lyapunov inequality. Notice that for any estimator $\hat{A}$ of $1\{S_1 = 1\}$ based on $Z_{-\infty}^0$ we have

$$\mathbb{E}\left[(\Psi_0 - 1\{S_1 = 1\})^2\right] \leq \mathbb{E}\left[(\hat{A} - 1\{S_1 = 1\})^2\right], \tag{187}$$

because $\Psi_0 = \mathbb{E}\left[1\{S_1 = 1\}|Z_{-\infty}^0\right]$ is a minimal mean square error estimate.

We now take the following estimator:

$$\hat{A}_n = 1\left\{\sum_{j=-n+1}^{0} Z_j \geq n\delta_a\right\}\,, \tag{188}$$

where n is to be specified later and $\delta_a = \frac{\delta_1 + \delta_2}{2}$. We then have the following upper bound on its mean square error:

$$\begin{aligned}\mathbb{E}\left[(\hat{A}_n - 1\{S_1 = 1\})^2\right] &= \mathbb{P}[1\{S_1 = 1\} \neq \hat{A}_n] &(189)\\ &\leq \mathbb{P}[\hat{A}_n \neq 1\{S_1 = 1\}, S_1 = \cdots = S_{-n+1}]\\ &\qquad + 1 - \mathbb{P}[S_1 = \cdots = S_{-n+1}] &(190)\\ &= \frac{1}{2}(1-\tau)^n\left(\mathbb{P}[B(n,\delta_1) < n\delta_a] + \mathbb{P}[B(n,\delta_2) \geq n\delta_a]\right)\\ &\qquad + 1 - (1-\tau)^n\,, &(191)\end{aligned}$$

where $B(n, \delta)$ denotes the binomially distributed random variable. Using Chernoff bounds we can find that for some E_1 we have

$$\mathbb{P}[B(n,\delta_1) < n\delta_a] + \mathbb{P}[B(n,\delta_2) \geq n\delta_a] \leq 2e^{-nE_1}\,. \tag{192}$$

Then we have

$$\mathbb{E}\left[(\hat{A}_n - 1\{S_1 = 1\})^2\right] \leq 1 - (1-\tau)^n(1 - e^{-nE_1})\,. \tag{193}$$

If we denote

$$\beta = -\ln(1-\tau)\,. \tag{194}$$

and choose

$$n = \left\lceil -\frac{1}{E_1}\ln\frac{\beta}{E_1}\right\rceil\,, \tag{195}$$

we obtain that

$$\mathbb{E}\left[(\hat{A}_n - 1\{S_1 = 1\})^2\right] \le 1 - (1-\tau)\cdot e^{-\frac{\beta}{E_1}\ln\frac{\beta}{E_1}}\left(1 - \frac{\beta}{E_1}\right). \tag{196}$$

When $\tau \to 0$ we have $\beta = \tau + o(\tau)$ and then it is not hard to show that

$$\mathbb{E}\left[(\hat{A}_n - 1\{S_1 = 1\})^2\right] \le \frac{\tau}{E_1}\ln\frac{\tau}{E_1} + o(\tau\ln\tau). \tag{197}$$

From (186), (187), and (197) we obtain (177). ■

Lemma 11: For any $0 < \tau < 1$ we have

$$|V_0 - V_1| \le 2\sqrt{V_1\Delta} + \Delta, \tag{198}$$

where Δ satisfies

$$\begin{aligned} \Delta &\le B_0 + \frac{B_0}{2(1-\sqrt{|1-2\tau|})}\ln\frac{eB_1}{B_0}, && (199)\\ B_0 &= \frac{d_2(\delta_1||\delta_2)}{d(\delta_1||\delta_2)}|C_0 - C_1|, && (200)\\ B_1 &= \sqrt{\frac{B_0}{|1-2\tau|}}\left(d(\delta_1||\delta_2)\left|\ln\frac{\tau}{1-\tau}\right| + \frac{h(\delta_1)-h(\delta_2)}{2|1-2\tau|}\right), && (201)\\ d_2(a||b) &= a\log^2\frac{a}{b} + (1-a)\log^2\frac{1-a}{1-b} && (202) \end{aligned}$$

and $d(a||b) = a\log\frac{a}{b} + (1-a)\log\frac{1-a}{1-b}$ is the binary divergence.

Proof: First denote

$$\Delta = \lim_{n\to\infty}\frac{1}{n}\mathrm{Var}\left[\sum_{j=1}^{n}\Xi_j\right], \tag{203}$$

where Ξ_j was defined in (131); the finiteness of Δ is to be proved below.

By (131) we have

$$F_j = -\Theta_j + \Xi_j. \tag{204}$$

In Appendix A we have shown that

$$\begin{aligned} \mathbb{E}[\Theta_j] &= C_1 - \log 2, && (205)\\ \mathrm{Var}\left[\sum_{j=1}^{n}\Theta_j\right] &= nV_1 + O(1). && (206) \end{aligned}$$

Essentially, Ξ_j is a correction term, compared to the case of state known at the receiver, which we expect to vanish as $\tau \to 0$. By definition of V_0 we have

$$\begin{aligned} V_0 &= \lim_{n\to\infty} \frac{1}{n} \mathrm{Var}\left[\sum_{j=1}^n F_j\right] && (207) \\ &= \lim_{n\to\infty} \mathrm{Var}\left[-\frac{1}{\sqrt{n}}\sum_{j=1}^n \Theta_j + \frac{1}{\sqrt{n}}\sum_{j=1}^n \Xi_j\right]. && (208) \end{aligned}$$

Now (198) follows from (203), (206) and by an application of the Cauchy-Schwartz inequality to (208).

We are left to prove (199). First, notice that

$$\Delta = \mathrm{Var}[\Xi_0] + 2\sum_{j=1}^{\infty} \mathrm{cov}(\Xi_0, \Xi_j)\,. \tag{209}$$

The first term is bounded by Lemma 12

$$\mathrm{Var}[\Xi_j] \le \mathbb{E}\,[\Xi_j^2] \le B_0\,. \tag{210}$$

Next, set

$$N = \left\lceil \frac{2\ln\frac{B_0}{B_1}}{\ln|1-2\tau|} \right\rceil\,. \tag{211}$$

We have then

$$\begin{aligned} \sum_{j=1}^{\infty} \mathrm{cov}[\Xi_0, \Xi_j] &\le (N-1)B_0 + B_1 \sum_{j\ge N} |1-2\tau|^{j/2} && (212) \\ &\le \frac{\ln\frac{B_0}{B_1}}{\ln\sqrt{|1-2\tau|}} B_0 + \frac{B_0}{1-\sqrt{|1-2\tau|}} && (213) \\ &\le \frac{B_0}{1-\sqrt{|1-2\tau|}} \ln\frac{eB_1}{B_0}\,, && (214) \end{aligned}$$

where in (212) for $j < N$ we used Cauchy-Schwarz inequality and (210), for $j \ge N$ we used Lemma 13; (213) follows by definition of N and (214) follows by $\ln x \le x - 1$. Finally, (199) follows now by applying (210) and (214) to (209). ■

Lemma 12: Under the conditions of Lemma 11, we have

$$\mathrm{Var}[\Xi_j] \le \mathbb{E}\,[\Xi_j^2] \le B_0\,. \tag{215}$$

Proof: First notice that

$$\begin{aligned}\mathbb{E}\left[\Xi_1|Z_{-\infty}^0\right] &= \Psi_0 d(\delta_1||\delta_1\Psi_0+\delta_2(1-\Psi_0)) \\ &\quad +(1-\Psi_0)d(\delta_2||\delta_1\Psi_0+\delta_2(1-\Psi_0))\,, \qquad (216)\\ \mathbb{E}\left[\Xi_1^2|Z_{-\infty}^0\right] &= \Psi_0 d_2(\delta_1||\delta_1\Psi_0+\delta_2(1-\Psi_0)) \\ &\quad +(1-\Psi_0)d_2(\delta_2||\delta_1\Psi_0+\delta_2(1-\Psi_0))\,. \qquad (217)\end{aligned}$$

Below we adopt the following notation

$$\bar{x} = 1-x\,. \tag{218}$$

Applying Lemma 14 twice (with $a=\delta_1\,, b=\delta_1 x+\delta_2\bar{x}$ and with $a=\delta_2\,, b=\delta_1 x+\delta_2\bar{x}$) we obtain

$$\begin{aligned}& x d_2(\delta_1||\delta_1 x+\delta_2\bar{x})+\bar{x}d_2(\delta_2||\delta_1 x+\delta_2\bar{x}) \\ &\quad \le \frac{d_2(\delta_1||\delta_2)}{d(\delta_1||\delta_2)}\left(x d(\delta_1||\delta_1 x+\delta_2\bar{x})+\bar{x}d(\delta_2||\delta_1 x+\delta_2\bar{x})\right)\,. \qquad (219)\end{aligned}$$

If we substitute $x=\Psi_0$ here, then by comparing (216) and (217) we obtain that

$$\mathbb{E}\left[\Xi_1^2|Z_{-\infty}^0\right] \le \frac{d_2(\delta_1||\delta_2)}{d(\delta_1||\delta_2)}\mathbb{E}\left[\Xi_1|Z_{-\infty}^0\right]. \tag{220}$$

Averaging this we obtain[10]

$$\mathbb{E}\left[\Xi_1^2\right] \le \frac{d_2(\delta_1||\delta_2)}{d(\delta_1||\delta_2)}(C_1-C_0)\,. \tag{222}$$

■

Lemma 13: Under the conditions of Lemma 11, we have

$$\mathrm{cov}[\Xi_0,\Xi_j] \le B_1|1-2\tau|^{j/2}\,. \tag{223}$$

Proof: From the definition of Ξ_j we have that

$$\mathbb{E}\left[\Xi_j|S_{-\infty}^0, Z_{-\infty}^{j-1}\right] = f(\Psi_{j-1}, R_{j-1}^*)\,, \tag{224}$$

where

$$f(x,y) = y d(\delta_1||\delta_1 x+\delta_2(1-x))+(1-y)d(\delta_2||\delta_1 x+\delta_2(1-x))\,. \tag{225}$$

[10] Note that it can also be shown that

$$\mathbb{E}\left[\Xi_1^2\right] \ge \frac{d_2(\delta_2||\delta_1)}{d(\delta_2||\delta_1)}(C_1-C_0)\,, \tag{221}$$

and therefore (222) cannot be improved significantly.

Notice the following relationship:

$$\frac{d}{d\lambda}H(\bar{\lambda}Q+\lambda P)=D(P||\bar{\lambda}Q+\lambda P)-D(Q||\bar{\lambda}Q+\lambda P)+H(P)-H(Q)\,. \tag{226}$$

This has two consequences. First it shows that the function

$$D(P||\bar{\lambda}Q+\lambda P)-D(Q||\bar{\lambda}Q+\lambda P) \tag{227}$$

is monotonically decreasing with λ (since it is a derivative of a concave function). Second, we have the following general relation for the excess of the entropy above its affine approximation:

$$\left.\frac{d}{d\lambda}\right|_{\lambda=0}[H((1-\lambda)Q+\lambda P)-(1-\lambda)H(Q)-\lambda H(P)] \;=\; D(P||Q)\,, \tag{228}$$

$$\left.\frac{d}{d\lambda}\right|_{\lambda=1}[H((1-\lambda)Q+\lambda P)-(1-\lambda)H(Q)-\lambda H(P)] \;=\; -D(Q||P)\,. \tag{229}$$

Also it is clear that for all other λ's the derivative is in between these two extreme values.

Applying this to the binary case we have

$$\begin{aligned}\max_{x,y\in[0,1]}\left|\frac{df(x,y)}{dy}\right| &= \max_{x\in[0,1]}|d(\delta_1||\delta_1x+\delta_2(1-x))-d(\delta_2||\delta_1x+\delta_2(1-x))| && (230)\\ &= \max(d(\delta_1||\delta_2),d(\delta_2||\delta_1)) && (231)\\ &= d(\delta_1||\delta_2)\,, && (232)\end{aligned}$$

where (231) follows because the function in the right side of (230) is decreasing and (232) is because we are restricted to $\delta_2\le\delta_1\le\frac{1}{2}$. On the other hand, we see that

$$f(x,x)=h(\delta_1x+\delta_2(1-x))-xh(\delta_1)-(1-x)h(\delta_2)\ge 0\,. \tag{233}$$

Comparing with (228) and (229), we have

$$\begin{aligned}\max_{x\in[0,1]}\left|\frac{df(x,x)}{dx}\right| &= \max(d(\delta_1||\delta_2),d(\delta_2||\delta_1)) && (234)\\ &= d(\delta_1||\delta_2)\,. && (235)\end{aligned}$$

By the properties of f we have

$$\begin{aligned}\left|f(\Psi_{j-1},R^*_{j-1})-f(\Psi_{j-1},\Psi_{j-1})\right| &\le d(\delta_1||\delta_2)|R^*_{j-1}-\Psi_{j-1}| && (236)\\ &\le B_2|1-2\tau|^{j-1}\,, && (237)\end{aligned}$$

where for convenience we denote

$$B_2=\frac{1}{2}d(\delta_1||\delta_2)\left|\ln\frac{\tau}{1-\tau}\right|\,. \tag{238}$$

Indeed, (236) is by (232) and (237) follows by observing that

$$\Psi_{j-1} = T_{Z_{j-1}} \circ \cdots \circ T_{Z_1}(\Psi_0)\,, \tag{239}$$

$$R^*_{j-1} = T_{Z_{j-1}} \circ \cdots \circ T_{Z_1}(R^*_0) \tag{240}$$

and applying (146). Consequently, we have shown

$$\left|\mathbb{E}\left[\Xi_j | S^0_{-\infty}, Z^{j-1}_{-\infty}\right] - f(\Psi_{j-1}, \Psi_{j-1})\right| \le B_2 |1-2\tau|^{j-1}\,, \tag{241}$$

or, after a trivial generalization,

$$\left|\mathbb{E}\left[\Xi_j | S^k_{-\infty}, Z^{j-1}_{-\infty}\right] - f(\Psi_{j-1}, \Psi_{j-1})\right| \le B_2 |1-2\tau|^{j-1-k}\,. \tag{242}$$

Notice that by comparing (233) with (216) we have

$$\mathbb{E}\left[f(\Psi_{j-1}, \Psi_{j-1})\right] = \mathbb{E}\left[\Xi_j\right]. \tag{243}$$

Next we show that

$$\left|\mathbb{E}\left[\Xi_j | S^0_{-\infty}, Z^0_{-\infty}\right] - \mathbb{E}\left[\Xi_j\right]\right| \le |1-2\tau|^{\frac{j-1}{2}}\left[2B_2 + B_3\right]\,, \tag{244}$$

where

$$B_3 = \frac{h(\delta_1) - h(\delta_2)}{2|1-2\tau|}\,. \tag{245}$$

Denote

$$t(\Psi_k, S_k) \triangleq \mathbb{E}\left[f(\Psi_{j-1}, \Psi_{j-1}) | S^k_{-\infty} Z^k_{-\infty}\right]. \tag{246}$$

Then because of (235) and since Ψ_k affects only the initial condition for Ψ_{j-1} when written as (239), we have for arbitrary $x_0 \in [\tau, 1-\tau]$,

$$|t(\Psi_k, S_k) - t(x_0, S_k)| \le B_2 |1-2\tau|^{j-k-1}\,. \tag{247}$$

On the other hand, as an average of $f(x,x)$ the function $t(x_0, s)$ satisfies

$$0 \le t(x_0, S_k) \le \max_{x\in[0,1]} f(x,x) \le h(\delta_1) - h(\delta_2)\,. \tag{248}$$

From here and (63) we have

$$\left|\mathbb{E}\left[t(x_0, S_k) | S^0_{-\infty} Z^0_{-\infty}\right] - \mathbb{E}\left[t(x_0, S_k)\right]\right| \le \frac{h(\delta_1) - h(\delta_2)}{2} |1-2\tau|^k\,, \tag{249}$$

or, together with (247),

$$\left|\mathbb{E}\left[t(\Psi_k, S_k) | S^0_{-\infty} Z^0_{-\infty}\right] - \mathbb{E}\left[t(x_0, S_k)\right]\right| \le \frac{h(\delta_1) - h(\delta_2)}{2} |1-2\tau|^k + B_2 |1-2\tau|^{j-k-1}\,. \tag{250}$$

This argument remains valid if we replace x_0 with a random variable $\tilde{\Psi}_k$, which depends on S_k but conditioned on S_k is independent of $(S^0_{-\infty}, Z^0_{-\infty})$. Having made this replacement and assuming $P_{\tilde{\Psi}_k|S_k} = P_{\Psi_k|S_k}$ we obtain

$$\left|\mathbb{E}\left[t(\Psi_k, S_k)|S^0_{-\infty}Z^0_{-\infty}\right] - \mathbb{E}\left[t(\Psi_k, S_k)\right]\right| \le \frac{h(\delta_1) - h(\delta_2)}{2}|1-2\tau|^k + B_2|1-2\tau|^{j-k-1}\ . \tag{251}$$

Summing together (242), (243), (246), (247) and (251) we obtain that for arbitrary $0 \le k \le j-1$ we have

$$\left|\mathbb{E}\left[\Xi_j|S^0_{-\infty}Z^0_{-\infty}\right] - \mathbb{E}\left[\Xi_j\right]\right| \le \frac{h(\delta_1) - h(\delta_2)}{2}|1-2\tau|^k + 2B_2|1-2\tau|^{j-k-1}\ . \tag{252}$$

Setting here $k = \lfloor j - 1/2 \rfloor$ we obtain (244).

Finally, we have

$$\begin{aligned}
\mathrm{cov}[\Xi_0, \Xi_j] &= \mathbb{E}\left[\Xi_0\Xi_j\right] - \mathbb{E}^2[\Xi_0] && (253)\\
&= \mathbb{E}\left[\Xi_0\mathbb{E}\left[\Xi_j|S^0_{-\infty}, Z^0_{-\infty}\right]\right] - \mathbb{E}^2[\Xi_0] && (254)\\
&\le \mathbb{E}\left[\Xi_0\mathbb{E}\left[\Xi_j\right]\right] + \mathbb{E}\left[|\Xi_0|(2B_2+B_3)|1-2\tau|^{\frac{j-1}{2}}\right] - \mathbb{E}^2[\Xi_0] && (255)\\
&= \mathbb{E}\left[|\Xi_0|\right](2B_2+B_3)|1-2\tau|^{\frac{j-1}{2}} && (256)\\
&\le \sqrt{\mathbb{E}\left[\Xi_0^2\right]}(2B_2+B_3)|1-2\tau|^{\frac{j-1}{2}} && (257)\\
&= \sqrt{B_0}(2B_2+B_3)|1-2\tau|^{\frac{j-1}{2}}\,, && (258)
\end{aligned}$$

where (255) is by (244), (257) is a Lyapunov's inequality and (258) is Lemma 12. ■

Lemma 14: Assume that $\delta_1 \ge \delta_2 > 0$ and $\delta_2 \le a, b \le \delta_1$; then

$$\frac{d(a||b)}{d_2(a||b)} \ge \frac{d(\delta_1||\delta_2)}{d_2(\delta_1||\delta_2)}\,. \tag{259}$$

Proof: While inequality (259) can be easily checked numerically, its rigorous proof is somewhat lengthy. Since the base of the logarithm cancels in (259), we replace $\log$ by $\ln$ below. Observe that the lemma is trivially implied by the following two statements:

$$\forall\delta \in [0, 1/2]: \quad \frac{d(a||\delta)}{d_2(a||\delta)} \quad \text{is a non-increasing function of } a \in [0, 1/2]\,; \tag{260}$$

and

$$\frac{d(\delta_1||b)}{d_2(\delta_1||b)} \quad \text{is a non-decreasing function of } b \in [0, \delta_1]\,. \tag{261}$$

To prove (260) we show that the derivative of $\frac{d_2(a||\delta)}{d(a||\delta)}$ is non-negative. This is equivalent to showing that

$$\begin{cases} f_a(\delta) \le 0\,, & \text{if } a \le \delta\,, \\ f_a(\delta) \ge 0\,, & \text{if } a \ge \delta\,, \end{cases} \tag{262}$$

where

$$f_a(\delta) = 2d(a||\delta) + \ln \frac{a}{\delta} \cdot \ln \frac{1-a}{1-\delta}\,. \tag{263}$$

It is easy to check that

$$f_a(a) = 0\,, f'_a(a) = 0\,. \tag{264}$$

So it is sufficient to prove that

$$f_a(\delta) = \begin{cases} \text{convex}\,, & 0 \le \delta \le a\,, \\ \text{concave}\,, & a \le \delta \le 1/2\,. \end{cases} \tag{265}$$

Indeed, if (265) holds then an affine function $g(\delta) = 0\delta + 0$ will be a lower bound for $f_a(\delta)$ on $[0, a]$ and an upper bound on $[a, 1/2]$, which is exactly (262). To prove (265) we analyze the second derivative of f_a:

$$f''_a(\delta) = \frac{2a}{\delta^2} + \frac{2\bar{a}}{\bar{\delta}^2} - \frac{1}{\delta^2} \ln \frac{\bar{\delta}}{\bar{a}} - \frac{2}{\delta\bar{\delta}} - \frac{1}{\bar{\delta}^2} \ln \frac{\delta}{a}\,. \tag{266}$$

In the case $\delta \ge a$ an application of the bound $\ln x \le x - 1$ yields

$$\begin{aligned} f''_a(\delta) &\le \frac{2a}{\delta^2} + \frac{2\bar{a}}{\bar{\delta}^2} - \frac{1}{\delta^2} \left(\frac{\bar{\delta}}{\bar{a}} - 1 \right) - \frac{2}{\delta\bar{\delta}} - \frac{1}{\bar{\delta}^2} \left(\frac{\delta}{a} - 1 \right) && (267) \\ &\le 0\,. && (268) \end{aligned}$$

Similarly, in the case $\delta \le a$ an application of the bound $\ln x \ge 1 - \frac{1}{x}$ yields

$$\begin{aligned} f''_a(\delta) &\ge \frac{2a}{\delta^2} + \frac{2\bar{a}}{\bar{\delta}^2} - \frac{1}{\delta^2} \left(1 - \frac{\bar{a}}{\bar{\delta}} \right) - \frac{2}{\delta\bar{\delta}} - \frac{1}{\bar{\delta}^2} \left(1 - \frac{a}{\delta} \right) && (269) \\ &\ge 0\,. && (270) \end{aligned}$$

This proves (265) and, therefore, (260).

To prove (261) we take the derivative of $\frac{d(\delta_1||b)}{d_2(\delta_1||b)}$ with respect to b; requiring it to be non-negative is equivalent to

$$2(1-2b) \left(\delta \ln \frac{\delta}{b} \right) \left(\bar{\delta} \ln \frac{\bar{\delta}}{\bar{b}} \right) + (\delta\bar{b} + \bar{\delta}b) \left(\delta \ln^2 \frac{\delta}{b} - \bar{\delta} \ln^2 \frac{\bar{\delta}}{\bar{b}} \right) \ge 0\,. \tag{271}$$

It is convenient to introduce $x = b/\delta \in [0,1]$ and then we define

$$f_\delta(x) = 2(1-2\delta x)\delta\bar{\delta}\ln x \cdot \ln\frac{1-\delta x}{\bar{\delta}} + \delta(1+x(1-2\delta))\left(\delta\ln^2 x - \bar{\delta}\ln^2\frac{1-\delta x}{\bar{\delta}}\right)\,, \tag{272}$$

for which we must show

$$f_\delta(x) \geq 0\,. \tag{273}$$

If we think of $A = \ln x$ and $B = \ln\frac{1-\delta x}{\bar{\delta}}$ as independent variables, then (271) is equivalent to solving

$$2\gamma AB + \alpha A^2 - \beta B^2 \geq 0\,, \tag{274}$$

which after some manipulation (and observation that we naturally have a requirement $A < 0 < B$) reduces to

$$\frac{A}{B} \leq -\frac{\gamma}{\alpha} - \frac{1}{\alpha}\sqrt{\gamma^2 + \alpha\beta}\,. \tag{275}$$

After substituting the values for A, B, α, β and γ we get that (271) will be shown if we can show for all $0 < x < 1$ that

$$\frac{\ln\frac{1}{x}}{\ln\frac{1-\delta x}{\bar{\delta}}} \geq \frac{1-2\delta x}{1+x(1-2\delta)}\frac{\bar{\delta}}{\delta} + \left(\left(\frac{1-2\delta x}{1-2\delta x+x}\right)^2\left(\frac{\bar{\delta}}{\delta}\right)^2 + \frac{\bar{\delta}}{\delta}\right)^{1/2}\,. \tag{276}$$

To show (276) we are allowed to upper-bound $\ln x$ and $\ln\frac{1-\delta x}{\bar{\delta}}$. We use the following upper bounds for $\ln x$ and $\ln\frac{1-\delta x}{\bar{\delta}}$, correspondingly:

$$\ln x \quad \leq \quad (x-1) - (x-1)^2/2 + (x-1)^3/3 - (x-1)^4/4 + (x-1)^5/5\,, \tag{277}$$

$$\ln y \quad \leq \quad (y-1) - (y-1)^2/2 + (y-1)^3/3\,, \tag{278}$$

particularized to $y = 1 - \frac{\delta x}{\bar{\delta}}$; both bounds follow from the fact that the derivative of $\ln x$ of the corresponding order is always negative. Applying (277) and (278) to the left side of (276) and after some tedious algebra, we find that (276) is implied by the

$$\frac{\delta^2(1-x)^3}{(1-\delta)^5}P_\delta(1-x) \geq 0\,, \tag{279}$$

where

$$\begin{aligned} P_\delta(x) \quad = \quad & -(4\delta^2-1)(1-\delta)^2/12 \\ & + (1-\delta)(4 - 5\delta + 4\delta^2 - 24\delta^3 + 24\delta^4)x/24 \\ & + (8 - 20\delta + 15\delta^2 + 20\delta^3 - 100\delta^4 + 72\delta^5)x^2/60 \\ & - (1-\delta)^3(11 - 28\delta + 12\delta^2)x^3/20 \\ & + (1-\delta)^3(1-2\delta)^2x^4/5\,. \end{aligned} \tag{280}$$

Assume that $P_\delta(x_0) < 0$ for some x_0. For all $0 < \delta \le 1/2$ we can easily check that $P_\delta(0) > 0$ and $P_\delta(1) > 0$. Therefore, there must be a root x_1 of P_δ in $(0, x_0)$ and a root x_2 in $(x_0, 1)$ by continuity. It is also easily checked that $P'_\delta(0) > 0$ for all δ. But then we must have at least one root of P'_δ in $[0, x_1)$ and at least one root of P'_δ in $(x_2, 1]$.

Now, $P'_\delta(x)$ is a cubic polynomial such that $P'_\delta(0) > 0$. So it must have at least one root on the negative real axis and two roots on $[0, 1]$. But since $P''_\delta(0) > 0$, it must be that $P''_\delta(x)$ also has two roots on $[0, 1]$. But $P''_\delta(x)$ is a quadratic polynomial, so its roots are algebraic functions of δ, for which we can easily check that one of them is always larger than 1. So, $P'_\delta(x)$ has at most one root on $[0, 1]$. And therefore we arrive at a contradiction and $P_\delta \ge 0$ on $[0, 1]$, which proves (279). ■

APPENDIX C
PROOF OF THEOREM 7

We need the following auxiliary result:

Lemma 15: Define $R_{na}(n, \epsilon)$ as in (43). Assume $C_1 < C_2$ and $\epsilon \not\in \{0, p_1, 1\}$. Then the following holds:

$$R_{na}\left(n, \epsilon + O(1/\sqrt{n})\right) = R_{na}(n, \epsilon) + O(1/n)\,. \tag{281}$$

Proof: Denote

$$f_n(R) \triangleq p_1 Q\left((C_1 - R)\sqrt{\frac{n}{V_1}}\right) + p_2 Q\left((C_2 - R)\sqrt{\frac{n}{V_2}}\right) \tag{282}$$

$$R_n \triangleq R_{na}(n, \epsilon) = f_n^{-1}(\epsilon)\,. \tag{283}$$

It is clear that $f_n(R)$ is a monotonically increasing function, and that our goal is to show that

$$f_n^{-1}(\epsilon + O(1/\sqrt{n})) = R_n + O(1/n)\,. \tag{284}$$

Assume $\epsilon < p_1$; then for any $0 < \delta < (C_2 - C_1)$ we have $f_n(C_1 + \delta) \to p_1$ and $f_n(C_1 - \delta) \to 0$. Therefore,

$$R_n = C_1 + o(1)\,. \tag{285}$$

This implies, in particular, that for large enough n we have

$$0 \le p_2 Q\left((C_2 - R_n)\sqrt{\frac{n}{V_2}}\right) \le \frac{1}{\sqrt{n}}\,. \tag{286}$$

Then, from the definition of R_n we conclude that

$$\epsilon - \frac{1}{\sqrt{n}} \le p_1 Q\left((C_2 - R_n)\sqrt{\frac{n}{V_2}}\right) \le \epsilon\,. \tag{287}$$

After applying Q^{-1} to this inequality we get

$$Q^{-1}\left(\frac{\epsilon}{p_1}\right) \le (C_2 - R_n)\sqrt{\frac{n}{V_2}} \le Q^{-1}\left(\frac{\epsilon - 1/\sqrt{n}}{p_1}\right)\,. \tag{288}$$

By Taylor's formula we conclude

$$R_n = C_1 - \sqrt{\frac{V_1}{n}} Q^{-1}\left(\frac{\epsilon}{p_1}\right) + O(1/n)\,. \tag{289}$$

Note that the same argument works for ϵ that depends on n, provided that $\epsilon_n < p_1$ for all sufficiently large n. This is indeed the case when $\epsilon_n = \epsilon + O(1/\sqrt{n})$. Therefore, similarly to (289), we can show

$$\begin{aligned} f_n^{-1}(\epsilon + O(1/\sqrt{n})) &= C_1 - \sqrt{\frac{V_1}{n}} Q^{-1}\left(\frac{\epsilon + O(1/\sqrt{n})}{p_1}\right) + O(1/n)\,, & (290)\\ &= C_1 - \sqrt{\frac{V_1}{n}} Q^{-1}\left(\frac{\epsilon}{p_1}\right) + O(1/n)\,, & (291)\\ &= R_n + O(1/n)\,, & (292) \end{aligned}$$

where (291) follows by applying Taylor's expansion and (292) follows from (289). The case $\epsilon > p_1$ is treated similarly. ■

We also quote the Berry-Esseen theorem in the following form:

Theorem 16 (Berry-Esseen): (e.g. Theorem 2, Chapter XVI.5 in [13]) Let X_k, $k = 1, \ldots, n$ be independent with

$$\begin{aligned} \mu_k &= \mathbb{E}\left[X_k\right], & (293)\\ \sigma_k^2 &= \mathrm{Var}[X_k]\,, & (294)\\ t_k &= \mathbb{E}\left[|X_k - \mu_k|^3\right], & (295)\\ \sigma^2 &= \sum_{k=1}^{n} \sigma_k^2\,, & (296)\\ T &= \sum_{k=1}^{n} t_k & (297) \end{aligned}$$

Then for all $-\infty < \lambda < \infty$

$$\left|\mathbb{P}\left[\sum_{k=1}^{n}(X_k - \mu_k) \ge \lambda\sigma\right] - Q(\lambda)\right| \le \frac{6T}{\sigma^3}\,. \tag{298}$$

Proof of Theorem 7: First of all, notice that $p_1 = 0$ and $p_1 = 1$ are treated by Theorem 3. So, everywhere below we assume $0 < p_1 < 1$.

Achievability: The proof of the achievability part closely follows the steps of the proof of Theorem 3 [1, Theorem 52]. It is therefore convenient to adopt the notation and the results of [1, Appendix K]. In particular, for all n and M there exists an (n, M, p_e) code with

$$p_e \le \sum_{k=0}^{n} \binom{n}{k} \left(p_1 \delta_1^k (1-\delta_1)^{n-k} + p_2 \delta_2^k (1-\delta_2)^{n-k}\right) \min\left\{1, M S_n^k\right\}\,, \tag{299}$$

where S_n^k is

$$S_n^k \triangleq 2^{-n} \sum_{l=0}^{k} \binom{n}{l} \tag{300}$$

(cf. [1, (580)]).

Fix $\epsilon \notin \{0, p_1, 1\}$ and for each n select K as a solution to

$$p_1 Q\left(\frac{K - n\delta_1}{\sqrt{n\delta_1(1-\delta_1)}}\right) + p_2 Q\left(\frac{K - n\delta_2}{\sqrt{n\delta_2(1-\delta_2)}}\right) = \epsilon - \frac{G}{\sqrt{n}}\,, \tag{301}$$

where $G > 0$ is some constant. Application of the Berry-Esseen theorem shows that there exists a choice of G such that for all sufficiently large n we have

$$\mathbb{P}[W > K] \le \epsilon\,, \tag{302}$$

where

$$W = \sum_{j=1}^{n} 1\{Z_j = 1\}\,. \tag{303}$$

The distribution of W is a mixture of two Bernoulli distributions:

$$\mathbb{P}[W = w] = \binom{n}{w} \left(p_1 \delta_1^w (1-\delta_1)^{n-w} + p_2 \delta_2^w (1-\delta_2)^{n-w}\right)\,. \tag{304}$$

Repeating the steps [1, (580)-(603)] we can now prove that as $n \to \infty$ we have

$$\begin{aligned} \log M^*(n,\epsilon) &\ge -\log S_n^K & (305)\\ &\ge n - nh\left(\frac{K}{n}\right) + \frac{1}{2}\log n + O(1)\,, & (306) \end{aligned}$$

where h is the binary entropy function. Thus we only need to analyze the asymptotics of $h\left(\frac{K}{n}\right)$. First, notice that the definition of K as the solution to (301) is entirely analogous to the definition of $nR_{na}(n,\epsilon)$. Assuming without loss of generality $\delta_2 < \delta_1$ (the case of $\delta_2 = \delta_1$ is treated in Theorem 3), in parallel to (44) we have as $n \to \infty$

$$K = \begin{cases} n\delta_1 + \sqrt{n\delta_1(1-\delta_1)}Q^{-1}\left(\frac{\epsilon}{p_1}\right) + O(1)\,, & \epsilon < p_1 \\ n\delta_2 + \sqrt{n\delta_2(1-\delta_2)}Q^{-1}\left(\frac{\epsilon-p_1}{p_2}\right) + O(1)\,. & \epsilon > p_1\,. \end{cases} \tag{307}$$

From Taylor's expansion applied to $h\left(\frac{K}{n}\right)$ as $n \to \infty$ we get

$$nh\left(\frac{K}{n}\right) = \begin{cases} nh(\delta_1) + \sqrt{nV(\delta_1)}Q^{-1}\left(\frac{\epsilon}{p_1}\right) + O(1)\,, & \epsilon < p_1 \\ nh(\delta_2) + \sqrt{nV(\delta_2)}Q^{-1}\left(\frac{\epsilon-p_1}{p_2}\right) + O(1)\,, & \epsilon > p_1\,. \end{cases} \tag{308}$$

Comparing (308) with (44) we notice that for $\epsilon \neq p_1$ we have

$$n - nh\left(\frac{K}{n}\right) = nR_{na}(n,\epsilon) + O(1)\,. \tag{309}$$

Finally, after substituting (309) in (306) we obtain the required lower-bound of the expansion:

$$\log M^*(n,\epsilon) \geq nR_{na}(n,\epsilon) + \frac{1}{2}\log n + O(1)\,. \tag{310}$$

Before proceeding to the converse part we also need to specify the non-asymptotic bounds that have been used to numerically compute the achievability curves in Fig. 5 and 6. For this purpose we use Theorem 1 with equiprobable P_{X^n}. Without state knowledge at the receiver we have

$$i(X^n;Y^n) = g_n(W)\,, \tag{311}$$

$$g_n(w) = n\log 2 + \log\left(p_1\delta_1^w(1-\delta_1)^{n-w} + p_2\delta_2^w(1-\delta_2)^{n-w}\right)\,, \tag{312}$$

where W is defined in (303). Theorem 1 guarantees that for every M there exists a code with (average) probability of error p_e satisfying

$$p_e \leq \mathbb{E}\left[\exp\left\{-\left[g_n(W) - \log\frac{M-1}{2}\right]^+\right\}\right]\,. \tag{313}$$

In addition, by application of the random linear code method, the same can be seen to be true for maximal probability of error, provided that $\log_2 M$ is an integer (see Appendix A in [1]). Therefore, the numerical computation of the achievability bounds in Fig. 5 and 6 amounts to finding the largest integer k such that right-hand side of (313) with $M = 2^k$ is still smaller than a prescribed ϵ.

With state knowledge at the receiver we can assume that the output of the channel is (Y^n, S_1) instead of Y^n. Thus, $i(X^n; Y^n)$ needs to be replaced by $i(X^n; Y^n, S_1)$ and then expressions (311), (312) and (304) become

$$\begin{aligned} i(X^n; Y^n S_1) &= g_n(W, S_1)\,, && (314)\\ g_n(w,s) &= n \log 2 + \log\left(\delta_s^w (1-\delta_s)^{n-w}\right)\,, && (315)\\ \mathbb{P}[W=w, S_1=s] &= p_s \binom{n}{w} \delta_s^w (1-\delta_s)^{n-w}\,. && (316)\end{aligned}$$

Again, in parallel to (313) Theorem 1 constructs a code with M codewords and probability of error p_e satisfying

$$p_e \le \mathbb{E}\left[\exp\left\{-\left[g_n(W,S_1) - \log\tfrac{M-1}{2}\right]^+\right\}\right]\,. \qquad (317)$$

Converse: In the converse part we will assume that the transmitter has access to the state realization S_1 and then generates X^n based on both the input message and S_1. Take the best such code with $M^*(n,\epsilon)$ codewords and average probability of error no greater than ϵ. We now propose to treat the pair (X^n, S_1) as a combined input to the channel (but the S_1 part is independent of the input message) and the pair (Y^n, S_1) as a combined output, available to the decoder. Note that in this situation, the encoder induces a distribution $P_{X^n S_1}$ and is necessarily randomized, because the distribution of S_1 is not controlled by the input message and is given by

$$\mathbb{P}[S_1 = 1] = p_1\,. \qquad (318)$$

To apply Theorem 2 we select the auxiliary Q-channel as follows:

$$Q_{Y^n S_1|X^n}(y^n, s|x^n) = \mathbb{P}[S_1 = s]2^{-n} \quad \text{for all } y^n, s, x^n\,. \qquad (319)$$

Then it is easy to see that under this channel, the output (Y^n, S_1) is independent of X^n. Hence, we have

$$1 - \epsilon' \le \frac{1}{M^*(n,\epsilon)}\,. \qquad (320)$$

To compute $\beta_{1-\epsilon}(P_{X^nY^nS_1}, Q_{X^nY^nS_1})$ we need to find the likelihood ratio:

$$
\begin{aligned}
r(X^n;Y^nS_1) &\triangleq \log\frac{P_{X^nY^nS_1}(X^n,Y^n,S_1)}{Q_{X^nY^nS_1}(X^n,Y^n,S_1)} && (321)\\
&= \log\frac{P_{Y^n|X^nS_1}P_{X^nS_1}}{Q_{Y^n|X^nS_1}Q_{X^nS_1}} && (322)\\
&= n\log 2+\log P_{Y^n|X^nS_1}(Y^n|X^nS_1) && (323)\\
&= n\log 2(1-\delta_{S_1})-W\log\frac{1-\delta_{S_1}}{\delta_{S_1}}\,, && (324)
\end{aligned}
$$

where (322) is because $P_{X^nS_1}=Q_{X^nS_1}$ (we omitted the obvious arguments for simplicity), (323) is by (319) and in (324) random variable W is defined in (303) and its distribution is given by (304).

Now, choose

$$
\begin{aligned}
R_n &= R_{na}\left(n,\epsilon+\frac{p_1B_1+p_2B_2+1}{\sqrt{n}}\right)\,, && (325)\\
\gamma_n &= nR_n\,, && (326)
\end{aligned}
$$

where B_1 and B_2 are the Berry-Esseen constants for the sum of independent Bernoulli(δ_j) random variables. Then, we have

$$
\begin{aligned}
&\mathbb{P}[r(X^n;Y^nS_1)\le\gamma_n|S_1=1]\\
&= \mathbb{P}\left[n\log 2(1-\delta_1)-W\log\frac{(1-\delta_1)}{\delta_1}\le\gamma_n\,\middle|\,S_1=1\right] && (327)\\
&\ge Q\left(-\frac{\gamma_n-nC_1}{\sqrt{nV_1}}\right)-\frac{B_1}{\sqrt{n}} && (328)\\
&= Q\left((C_1-R_n)\sqrt{\frac{n}{V_1}}\right)-\frac{B_1}{\sqrt{n}}\,, && (329)
\end{aligned}
$$

where (328) is by the Berry-Esseen theorem and (329) is just the definition of γ_n. Analogously, we have

$$\mathbb{P}[r(X^n;Y^nS_1)\le\gamma_n|S_1=2]\ge Q\left((C_2-R_n)\sqrt{\frac{n}{V_2}}\right)-\frac{B_2}{\sqrt{n}}\,. \qquad (330)$$

Together (329) and (330) imply

$$
\begin{aligned}
&\mathbb{P}[r(X^n;Y^nS)\le\gamma_n]\\
&\ge p_1Q\left((C_1-R_n)\sqrt{\frac{n}{V_1}}\right)+p_2Q\left((C_2-R_n)\sqrt{\frac{n}{V_2}}\right)-\frac{p_1B_1+p_2B_2}{\sqrt{n}} && (331)\\
&= \epsilon+\frac{1}{\sqrt{n}}\,, && (332)
\end{aligned}
$$

where (332) follows from (325). Then by using the bound (24) we obtain

$$\beta_{1-\epsilon}(P_{X^nY^nS_1}, Q_{X^nY^nS_1}) \geq \frac{1}{\sqrt{n}} \exp\{-\gamma_n\} \,. \tag{333}$$

Finally, by Theorem 2 and (320) we obtain

$$\begin{aligned} \log M^*(n,\epsilon) &\leq \log \frac{1}{\beta_{1-\epsilon}} && (334)\\ &\leq \gamma_n + \frac{1}{2}\log n && (335)\\ &= nR_{na}\left(n, \epsilon + \frac{p_1B_1 + p_2B_2 + 1}{\sqrt{n}}\right) + \frac{1}{2}\log n && (336)\\ &= nR_{na}(n,\epsilon) + \frac{1}{2}\log n + O(1)\,, && (337) \end{aligned}$$

where (337) is by Lemma 15. ■

As noted before, for $\epsilon = p_1$ even the capacity term is unknown. However, application of Theorem 2 with $Q_{Y|X} = BSC(\delta_{max})$ where $\delta_{max} = \max(\delta_1, \delta_2)$, yields the following upper bound:

$$C_{p_1} \leq 1 - h(s^*)\,, \tag{338}$$

where s^* is found as the solution of

$$d(s^*||\delta_2) = d(s^*||\delta_1)\,. \tag{339}$$

To get (338), take any rate $R > 1 - h(\delta_{max})$ and apply a well-known above-the-capacity error estimate for the Q-channel [16]:

$$1 - \epsilon' \lesssim \exp\left(-nd(s||\delta_{max})\right)\,, \tag{340}$$

where $s < \delta_1$ satisfies $R = 1 - h(s)$. Then it is not hard to obtain that

$$\beta_{1-p_1}(P_{Y|X}, Q_{Y|X}) \sim \exp\left(-nd(s^*||\delta_{max})\right)\,. \tag{341}$$

The upper bound (338) then follows from Theorem 2 immediately. Note that the same upper-bound was derived in [11] (and there it was also shown to be tight in the special case of $|\delta_1 - \delta_2|$ being small enough), but the proof we have outlined above is more general since it also applies to the average probability of error criterion and various state-availability scenarios.

Yury Polyanskiy (S'08) received the B.S. and M.S. degrees (both with honors) in applied mathematics and physics from the Moscow Institute of Physics and Technology in 2003 and 2005, respectively. He is currently pursuing a Ph.D. degree in electrical engineering at Princeton University, Princteon, NJ.

In 2000-2005, he was with the Department of Surface Oilfield Equipment, Borets Company LLC, where he rose to the position of Chief Software Designer. His research interests include information theory, coding theory and the theory of random processes.

Mr. Polyanskiy won a silver medal at the 30th International Physics Olympiad (IPhO), held in Padova, Italy. He was a recipient of the Best Student Paper Award at the 2008 IEEE International Symposium on Information Theory (ISIT), Toronto, ON, Canada.

H. Vincent Poor (S'72-M'77-SM'82-F'87) received the Ph.D. degree in electrical engineering and computer science from Princeton University in 1977. From 1977 until 1990, he was on the faculty of the University of Illinois at Urbana-Champaign. Since 1990 he has been on the faculty at Princeton, where he is the Dean of Engineering and Applied Science, and the Michael Henry Strater University Professor of Electrical Engineering. Dr. Poor's research interests are in the areas of stochastic analysis, statistical signal processing and information theory, and their applications in wireless networks and related fields. Among his publications in these areas are *Quickest Detection* (Cambridge University Press, 2009), co-authored with Olympia Hadjiliadis, and *Information Theoretic Security* (Now Publishers, 2009), co-authored with Yingbin Liang and Shlomo Shamai.

Dr. Poor is a member of the National Academy of Engineering, a Fellow of the American Academy of Arts and Sciences, and an International Fellow of the Royal Academy of Engineering (U. K.). He is also a Fellow of the Institute of Mathematical Statistics, the Optical Society of America, and other organizations. In 1990, he served as President of the IEEE Information Theory Society, in 2004-07 as the Editor-in-Chief of these TRANSACTIONS, and recently as General Co-chair of the 2009 IEEE International Symposium on Information Theory, held in Seoul, South Korea. He is the recipient of the 2005 IEEE Education Medal. Recent recognition of his work includes the 2007 Technical Achievement Award of the IEEE Signal Processing Society, the 2008 Aaron D. Wyner Distinguished Service Award of the IEEE Information Theory Society, and the 2009 Edwin Howard Armstrong Achievement Award of the IEEE Communications Society.

Sergio Verdú (S'80-M'84-SM'88-F'93) received the Telecommunications Engineering degree from the Universitat Politècnica de Barcelona, Barcelona, Spain, in 1980 and the Ph.D. degree in Electrical Engineering from the University of Illinois at Urbana-Champaign, Urbana, in 1984.

Since 1984, he has been a member of the faculty of Princeton University, Princeton, NJ, where he is the Eugene Higgins Professor of Electrical Engineering.

Dr. Verdú is the recipient of the 2007 Claude E. Shannon Award and the 2008 IEEE Richard W. Hamming Medal. He is a member of the National Academy of Engineering and was awarded a Doctorate Honoris Causa from the Universitat Politècnica de Catalunya in 2005. He is a recipient of several paper awards from the IEEE: the 1992 Donald Fink Paper Award, the 1998 Information Theory Outstanding Paper Award, an Information Theory Golden Jubilee Paper Award, the 2002 Leonard Abraham Prize Award, the 2006 Joint Communications/ Information Theory Paper Award, and the 2009 Stephen O. Rice Prize from IEEE Communications Society. He has also received paper awards from the Japanese Telecommunications Advancement Foundation and from Eurasip. He received the 2000 Frederick E. Terman Award from the American Society for Engineering Education for his book Multiuser Detection (Cambridge, U.K.: Cambridge Univ. Press, 1998). He served as President of the IEEE Information Theory Society in 1997. He is currently Editor-in-Chief of Foundations and Trends in Communications and Information Theory.