A beta-beta achievability bound with applications

The MIT Faculty has made this article openly available. Please share how this access benefits you. Your story matters.

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>As Published</td>
<td><a href="http://dx.doi.org/10.1109/ISIT.2016.7541783">http://dx.doi.org/10.1109/ISIT.2016.7541783</a></td>
</tr>
<tr>
<td>Publisher</td>
<td>Institute of Electrical and Electronics Engineers (IEEE)</td>
</tr>
<tr>
<td>Version</td>
<td>Original manuscript</td>
</tr>
<tr>
<td>Accessed</td>
<td>Sun Nov 25 22:26:43 EST 2018</td>
</tr>
<tr>
<td>Citable Link</td>
<td><a href="http://hdl.handle.net/1721.1/113659">http://hdl.handle.net/1721.1/113659</a></td>
</tr>
<tr>
<td>Terms of Use</td>
<td>Creative Commons Attribution-Noncommercial-Share Alike</td>
</tr>
<tr>
<td>Detailed Terms</td>
<td><a href="http://creativecommons.org/licenses/by-nc-sa/4.0/">http://creativecommons.org/licenses/by-nc-sa/4.0/</a></td>
</tr>
</tbody>
</table>
A Beta-Beta Achievability Bound with Applications

Wei Yang 1, Austin Collins 2, Giuseppe Durisi 3, Yury Polyanskiy 2, and H. Vincent Poor 1

1Princeton University, Princeton, NJ, 08544 USA
2Massachusetts Institute of Technology, Cambridge, MA, 02139 USA
3Chalmers University of Technology, 41296 Gothenburg, Sweden

Abstract—A channel coding achievability bound expressed in terms of the ratio between two Neyman-Pearson \( \beta \) functions is proposed. This bound is the dual of a converse bound established earlier by Polyanskiy and Verdú (2014). The new bound turns out to simplify considerably the analysis in situations where the channel output distribution is not a product distribution, for example due to a cost constraint or a structural constraint (such as orthogonality or constant composition) on the channel inputs. Connections to existing bounds in the literature are discussed.

The bound is then used to derive 1) an achievability bound on the channel dispersion of additive non-Gaussian noise channels with random Gaussian codebooks, 2) the channel dispersion of an exponential-noise channel, 3) a second-order expansion for the minimum energy per bit of an AWGN channel, and 4) a lower bound on the maximum coding rate of a multiple-input multiple-output Rayleigh-fading channel with perfect channel state information at the receiver, which is the tightest known achievable result.

I. INTRODUCTION

We consider an abstract channel that consists of an input set \( \mathcal{A} \), an output set \( \mathcal{B} \), and a random transformation \( P_{Y|X} : \mathcal{A} \rightarrow \mathcal{B} \). An \( (M, \epsilon) \) code for the channel \( (\mathcal{A}, P_{Y|X}, \mathcal{B}) \) comprises a message set \( \mathcal{M} \triangleq \{1, \ldots, M\} \), an encoder \( f : \mathcal{M} \rightarrow \mathcal{A} \), and a decoder \( g : \mathcal{B} \rightarrow \mathcal{M} \cup \{\epsilon\} \) (\( \epsilon \) denotes an error event) that satisfies the average error probability constraint

\[
\frac{1}{M} \sum_{j=1}^{M} \left( 1 - P_{Y|X}(g^{-1}(j) \mid f(j)) \right) \leq \epsilon.
\]

(1)

Here, \( g^{-1}(j) \triangleq \{y \in \mathcal{Y} : g(y) = j\} \). For a fixed arbitrary \( \epsilon \in (0, 1) \), we are interested in finding a lower bound (i.e., an achievable bounds) on the largest number \( M^* \) of codewords for which an \( (M, \epsilon) \) code exists.

For stationary memoryless channels, Shannon’s channel coding theorem establishes that the rate of the best code converges to the channel capacity

\[
C = \max_{P_X} I(X; Y)
\]

as the blocklength grows to infinity. Here, \( I(X; Y) \) denotes the mutual information between the channel input and output. The mutual information can be expressed through an arbitrary output distribution \( Q_Y \) as follows [1, Eq. (8.7)]:

\[
I(X; Y) = D(P_{Y|X} \parallel Q_Y | P_X) - D(P_Y \parallel Q_Y).
\]

(3)

This work was supported in part by the US National Science Foundation (NSF) under Grants CCF-1420575 and ECCS-1343210, by the Swedish Research Council, under grant 322452, by the Center for Science of Information (CSoI), an NSF Science and Technology Center, under grant agreement CCF-09-39370, and by the NSF CAREER award CCF-12-53205.

This identity—also known as the golden formula—has found many applications in information theory. For example, it allows us to prove converse bounds on channel capacity (by dropping the term \( -D(P_Y \parallel Q_Y) \); see [2]). It is also used in the derivation of the capacity per unit cost [3], in the Blahut-Arimoto algorithm [4], [5], in Gallager’s formula for the minimax redundancy in universal source coding [6], and in characterizing properties of good channel codes [7], [8]. Therefore, it is of paramount interest to find a finite-blocklength analog of (3).

As a first step, Polyanskiy and Verdú recently proved that every \( (M, \epsilon) \) code satisfies the following converse bound [8, Th. 15]

\[
M \leq \inf_{0 \leq \delta < 1 - \epsilon} \inf_{Q_Y} \frac{\beta_{1-\delta}(P_Y, Q_Y)}{\beta_{1-\epsilon-\delta}(P_{XY}, P_X, Q_Y)}.
\]

(4)

Here, \( P_X \) and \( P_Y \) denote the empirical input and output distributions induced by the code (for the case of uniformly distributed messages). The function \( \beta_\alpha(P, Q) \) in (4) measures the difficulty of distinguishing \( P \) from \( Q \) in terms of hypothesis testing, and is defined as

\[
\beta_\alpha(P, Q) \triangleq \min \int P_{Z|W}(1 \mid w)Q(dw)
\]

(5)

where the minimum is over all conditional probability distributions \( P_{Z|W} : W \rightarrow \{0, 1\} \) satisfying

\[
\int P_{Z|W}(1 \mid w)P(dw) \geq \alpha
\]

(6)

and \( W \) denotes the support of \( P \) and \( Q \). The analogy between (3) and (4) follows from Stein’s lemma:

\[
- \log \beta_\alpha(P^n, Q^n) = nD(P^n || Q^n) + o(n), \quad \forall \alpha \in (0, 1).
\]

(7)

Contributions: In this paper, we continue the program of establishing a finite-blocklength analog of the golden formula by proving the following achievability counterpart of (4).

Theorem 1 (\( \beta \beta \) achievability bound): For every \( 0 < \epsilon < 1 \) and every input distribution \( P_X \), there exists an \( (M, \epsilon) \) code for the channel \( (\mathcal{A}, P_{Y|X}, \mathcal{B}) \) satisfying

\[
\frac{M}{2} \geq \sup_{0 < r < \epsilon} \sup_{Q_Y} \frac{\beta_{r}(P_Y, Q_Y)}{\beta_{1-\epsilon-r}(P_{XY}, P_X, Q_Y)}.
\]

(8)

1By the Neyman-Pearson lemma [9], there exists an optimal \( P_{Z|W} \) that attains the minimum in (5). This test, which we shall refer to as the Neyman-Pearson test, involves thresholding the Radon-Nikodym derivative of \( P \) with respect to \( Q \).
where \( P_Y \equiv P_{Y|X} \circ P_X \).

The proof of this bound relies on Shannon’s random coding technique and on a suboptimal decoder that is based on the Neyman-Pearson test between \( P_{XY} \) and \( P_X Q_Y \). Hypothesis testing is used twice in the proof: to relate the decoding error probability to \( \beta_{1-\epsilon+\tau}(P_{XY}, P_X Q_Y) \), and to perform a change of measure from \( P_Y \) to \( Q_Y \).

The bound \( (8) \) is useful in situations where \( P_Y \) is not a product distribution (although the underlying channel law \( P_{Y|X} \) is stationary and memoryless), for example due to cost constraints, or structural constraints on the channel input, such as orthogonality or constant composition. In such cases, traditional achievability bounds such as Feinstein’s bound \([10]\) and the dependence-testing (DT) bound \([11, \text{Th. 18}]\), which are explicit in \( dP_{Y|X}/dP_Y \), become difficult to evaluate. In contrast, the \( \beta \beta \) bound \( (8) \) requires the evaluation of \( dP_{Y|X}/dP_Y \), which factorizes for product \( Q_Y \). This allows for an analytical computation of \( (8) \). Furthermore, the term \( \beta_{1-\epsilon+\tau}(P_{XY}, P_X Q_Y) \), which captures the cost of the change of measure from \( P_Y \) to \( Q_Y \), can be evaluated or bounded even when a closed-form expression for \( P_Y \) is not available. To illustrate these points, we present the following applications of Theorem 1:

- We derive an achievability bound on the channel dispersion \([11, \text{Def. 1}]\) of additive non-Gaussian noise channels, for the case in which the encoder uses a power-constrained random Gaussian codebook. We show that the power constraint introduces an additional term in the expression of the achievable dispersion, which depends on the minimum mean square error (MMSE) of estimating the channel input given the channel output.

- We characterize the channel dispersion of the additive exponential noise channel introduced in \([12]\). The channel dispersion of a discrete counterpart of the exponential-noise channel is studied in \([13]\).

- We prove a second-order expansion for the minimum energy per bit of an additive white Gaussian noise (AWGN) channel at finite blocklength, hence establishing a nonasymptotic counterpart of the “wideband slope” result of Verdú \([14]\). Even though this result can be obtained via other techniques (such as the \( \kappa \beta \) bound \([11, \text{Th. 25}]\)), the proof based on \( (8) \) is conceptually simpler and generalizes to other channel models.

- We evaluate \( (8) \) for a multiple-input multiple-output (MIMO) Rayleigh-fading channel with perfect channel state information at the receiver (CSIR). In this case, \( (8) \) yields the tightest known achievable result.

Notation: For an input distribution \( P_X \) and a channel \( P_{Y|X} \), we let \( P_{Y|X} \circ P_X \) denote the distribution of \( Y \) induced by \( P_X \) through \( P_{Y|X} \). The distribution of a circularly symmetric complex Gaussian random vector with covariance matrix \( A \) is denoted by \( CN(0, A) \). With \( \chi_k^2(\lambda) \) we denote the noncentral chi-squared distribution with \( k \) degrees of freedom and noncentrality parameter \( \lambda \). Finally, \( \text{Exp}(\mu) \) stands for the exponential distribution with mean \( \mu \).

II. Proof of Theorem 1

Fix \( \epsilon \in (0, 1), \tau \in (0, \epsilon) \), and let \( P_X \) and \( Q_Y \) be two arbitrary probability measures on \( A \) and \( B \), respectively. Furthermore, let

\[
M = \left[ \frac{2\beta_{1-\epsilon+\tau}(P_Y, Q_Y)}{\beta_{1-\epsilon+\tau}(P_{XY}, P_X Q_Y)} \right].
\]

Finally, let \( P_{Z|X,Y} : A \times B \to \{0, 1\} \) be the Neyman-Pearson test that satisfies

\[
P_{XY}[Z(X,Y) = 1] \geq 1 - \epsilon + \tau \quad (10)
\]

\[
P_{XQY}[Z(X,Y) = 1] = \beta_{1-\epsilon+\tau}(P_{XY}, P_X Q_Y). \quad (11)
\]

For a given codebook \( \{c_1, \ldots, c_M\} \) and a received signal \( y \), the decoder computes the values of \( Z(c_j, y) \) and returns the smallest index \( j \) for which \( Z(c_j, y) = 1 \). If no such index is found, the decoder declares an error. The average probability of error of the given codebook \( \{c_1, \ldots, c_M\} \), under the assumption of uniformly distributed messages, is given by

\[
P_e(c_1, \ldots, c_M) = P \left[ \bigcup \left\{ Z(c_m, Y) = 0 \right\} \right.
\]

\[
\left. \exists m < W \text{ s.t. } Z(c_m, Y) = 1 \right] \quad (12)
\]

where \( W \) is equiprobable on \( \{1, \ldots, M\} \) and \( Y \sim P_{Y|W} \). Following Shannon’s random coding idea, we next average \( (12) \) over all codebooks \( \{C_1, \ldots, C_M\} \) whose codewords are generated as pairwise independent random variables with distribution \( P_X \). This yields

\[
E[P_e(C_1, \ldots, C_M)]
\]

\[
\leq P \left[ Z(X,Y) = 0 \right] + P \left[ \max_{m < W} Z(C_m, Y) = 1 \right] \quad (13)
\]

\[
\leq \epsilon - \tau + P \left[ \max_{m < W} Z(C_m, Y) = 1 \right]. \quad (14)
\]

Here, \( (13) \) follows from the union bound and \( (14) \) follows from \( (10) \).

To conclude the proof of \( (8) \), it suffices to show that

\[
P \left[ \max_{m < W} Z(C_m, Y) = 1 \right] \leq \tau. \quad (15)
\]

Consider the randomized test \( P_{\tilde{Z}|Y} : Y \to \{0, 1\} : \)

\[
\tilde{Z}(y) \equiv \max_{m < W} Z(C_m, y). \quad (16)
\]

It follows that

\[
\beta_{P_Y|\tilde{Z}=1}(P_Y, Q_Y) \leq Q_Y[\tilde{Z}(Y) = 1]
\]

\[
\leq \frac{1}{M} \sum_{j=1}^M (j-1) P_X Q_Y[Z(X,Y) = 1] \quad (17)
\]

\[
= \frac{M-1}{2} P_X Q_Y[Z(X,Y) = 1] \quad (18)
\]

\[
= \frac{M-1}{2} \beta_{1-\epsilon+\tau}(P_{XY}, P_X Q_Y) \quad (19)
\]

\[
\leq \beta_{1-\epsilon+\tau}(P_Y, Q_Y). \quad (20)
\]

\[
\leq \beta_{1-\epsilon+\tau}(P_{XY}, P_X Q_Y). \quad (21)
\]
Here, (17) follows from (5); (18) follows from (16) and from the union bound; (20) follows from (11); and (21) follows from (9). Since \( \alpha \mapsto \beta_{\alpha}(P_Y, Q_Y) \) is nondecreasing, we conclude that

\[
P_Y[\bar{Z} = 1] \leq \tau \tag{22}
\]

which is equivalent to (15).

### III. CONNECTION TO EXISTING BOUNDS

We next illustrate the connection between Theorem 1 and other achievability bounds.

1) The \( \kappa \beta \) bound: The \( \kappa \beta \) bound in [11, Th. 25] is based on Feinstein’s maximal coding and on a suboptimal decoder similar to the one used in Theorem 1. By further lower-bounding the \( \kappa \) term in the \( \kappa \beta \) bound using [15, Lemma 4], we can relax it to the following bound:

\[
M \geq \sup_{\tau \in [0, \epsilon)} \sup_{x \in F} \beta_{\tau}(P_{Y|X} \circ P_X, Q_Y) \tag{23}
\]

which holds under a maximal error probability constraint. Here, \( F \subset A \) denotes the permissible set of codewords, and \( P_X \) is an arbitrary distribution on \( F \). The similarity between (23) and (8) allows us to interpret the \( \beta \) bound as the average-error-probability counterpart of the \( \kappa \beta \) bound. For the case in which \( \beta_{\alpha}(P_{Y|X=x}, Q_Y) \) does not depend on \( x \in F \), by relaxing \( M/2 \) to \( M \) in (8) and by using [11, Lemma 29] we obtain a weaker version of (23) that holds under the average error probability constraint. However, for the case in which \( \beta_{\alpha}(P_{Y|X=x}, Q_Y) \) does depend on \( x \in F \), (8) can be both easier to analyze and numerically tighter than (23) (see Section V-D for an example).

2) The dependence-testing (DT) bound: Setting \( Q_Y = P_Y \) in (8), using \( \beta_{\tau}(P_Y, P_Y) = \tau \), and rearranging terms, we obtain

\[
\epsilon \leq \inf_{\alpha \in [0, 1]} \left\{ 1 - \alpha + \frac{M}{2} \beta_{\alpha}(P_{X|Y} \circ P_Y P_Y) \right\} \tag{24}
\]

Setting \( \alpha = P_{X|Y} \log dP_{X|Y} / dP_X P_Y \geq \log(M/2) \) and using the Neyman-Pearson lemma, we conclude that (24) is equivalent to a slightly weakened version of the DT bound [11, Th. 18] with \((M-1)/2 \) replaced by \( M/2 \). Since this weakened version of the DT bound implies Shannon’s bound [16] and the bound in [17, Th. 2], our bound implies these two bounds as well.

### IV. PROPERTIES OF \( \beta_{\alpha}(P, Q) \)

In this section, we collect properties of \( \beta_{\alpha}(P, Q) \), that are useful for evaluating (8).

Lemma 2: For every \( \alpha \in [0, 1] \) the following hold:

1) Data-processing inequality [18]: for every stochastic kernel \( P_{Y|X} : \mathcal{X} \to \mathcal{Y} \), every \( P_X \), and every \( Q_X \)

\[
\beta_{\alpha}(P_X, Q_X) \leq \beta_{\alpha}(P_{Y|X} \circ P_X, P_Y \circ Q_X) \tag{25}
\]

2) Action on mixtures of distributions [19, Lemma 25]: let \( P_X = \sum_j \lambda_j P_{X,j} \) be a convex combination of \( P_{X,j} \). Then for all \( Q_Y \) and \( j \) we have

\[
\beta_{\alpha}(P_{X,Y} \circ P_{X,Y} Q_Y) \geq \lambda_j \beta_{1-(1-\alpha)\lambda_j^{-1}}(P_{X,Y} \circ P_{X,Y} Q_Y) \tag{26}
\]

If the supports of \( P_{X,Y} \) are pairwise disjoint then

\[
\beta_{\alpha}(P_{X,Y} \circ P_{X,Y} Q_Y) = \inf \sum_{j} \lambda_j \beta_{\alpha}(P_{X,Y} \circ P_{X,Y} Q_Y) \tag{27}
\]

3) Action on product distributions: for every \( P_1, P_2, Q_1, Q_2 \)

\[
\beta_{\alpha}(P_1 P_2, Q_1 Q_2) \geq \beta_{\alpha}(P_1, Q_1) \beta_{\alpha}(P_2, Q_2) \tag{28}
\]

4) Bounds: for every \( \delta_1 \in (0, 1-\alpha) \) and every \( \delta_2 \in (0, \alpha) \)

\[
\frac{\beta_{\alpha+\delta_1}(P_{X,Y} \circ P_{X,Y} Q_Y)}{\beta_{\delta_1}(P_{X,Y} \circ P_{X,Y} Q_Y)} \geq \frac{\beta_{\alpha}(P_{X,Y} \circ P_{X,Y} Q_Y)}{\gamma} \tag{29}
\]

where \( \gamma \) satisfies \( P_Y[dP_Y/dQ_Y \geq \gamma] \geq 1 - \delta_2 \).

5) Bounds via Rényi divergence: for every \( \lambda > 1 \)

\[
\beta_{\alpha}(P, Q) \geq \alpha^{\lambda/(\lambda-1)} \left( (\lambda-1) D_{\lambda}(P || Q) - (1-\lambda)^{\lambda/(\lambda-1)} \right) \tag{30}
\]

where \( D_{\lambda}(\cdot || \cdot) \) denotes the Rényi divergence [20].

Proof: See Appendix A.

### V. APPLICATIONS

We shall take \( A \) and \( B \) to be \( n \)-fold Cartesian products of alphabets \( \mathcal{X} \) and \( \mathcal{Y} \). A channel is a sequence of conditional probabilities \( P_{Y^n|X^n} : \mathcal{X}^n \to \mathcal{Y}^n \). We shall refer to an \((M, \epsilon)\) code for the channel \( \{ \mathcal{X}^n, P_{Y^n|X^n}, \mathcal{Y}^n \} \) as an \((n, M, \epsilon)\) code. Furthermore, the maximum coding rate \( R^*(n, \epsilon) \) is defined as

\[
R^*(n, \epsilon) \triangleq \sup \left\{ \log \frac{M}{n} : \exists(n, M, \epsilon) \text{ code} \right\} \tag{32}
\]

#### A. Additive non-Gaussian noise channels

We consider the additive-noise channel

\[
Y_i = X_i + Z_i, \quad i = 1, \ldots, n \tag{33}
\]

where \( \{Z_i\} \) are independent and identically distributed (i.i.d.) \( P_Z \)-distributed (not necessarily Gaussian) and \( X_i, Y_i, Z_i \in \mathbb{R} \). Each codeword \( x^n \) must satisfy the constraint

\[
||x^n||^2 = \sum_{i=1}^{n} x_i^2 \leq nP \tag{34}
\]

Let \( Q_{X^n} = N(0, P_{L^n}) \), and let \( P_{X^n} \) denote the conditional distribution of \( X^n \sim Q_{X^n} \) conditioned on

\[
X^n \in A_n \triangleq \left\{ x^n \in \mathbb{R}^n : nP - \log n \leq ||x^n||^2 \leq nP \right\} \tag{35}
\]

\( ^2 \)Unless otherwise indicated, the \( \log \) and \( \exp \) functions in this paper are taken with respect to an arbitrary fixed basis.
In other words, $P_{X^n}$ is a truncated Gaussian distribution that is supported on the spherical shell $A_n$. We shall consider an ensemble of codes in which the codewords are generated independently from the distribution $P_{X^n}$. This ensemble of codes is used by Gallager to derive the random coding error exponent for channels with cost constraint [21, p. 326]. In the following theorem we present a second-order asymptotic expansion on the maximum rate achievable with this code over the channel (33).

**Theorem 3:** Let $Q_X = \mathcal{N}(0, P)$, let $Q_Y = P_{Y|X} \circ Q_X$, and let

$$i(x; y) \equiv \frac{dP_{Y|x}}{dQ_Y}(x; y)$$

be the information density of the joint distribution $Q_X P_{Y|X}$. Furthermore, let

$$I(P) \equiv \mathbb{E}_{Q_X P_{Y|X}}[i(X; Y)].$$

Assume that the noise $Z$ satisfies the following conditions:

1. $P_Z$ is absolutely continuous with respect to the Lebesgue measure on $\mathbb{R}$;
2. $\mathbb{E}_{Q_X P_Z}[i(X; X + Z) - I(P)] < \infty$; and
3. $\mathbb{E}[|Z|^6] < \infty$.

Then, for every $0 < \epsilon < 1$, we have

$$R^*(n, \epsilon) \geq I(P) - \sqrt{\frac{V(P)}{n}} Q^{-1}(\epsilon) + O\left(\frac{\log n}{n}\right).$$

Here, $Q^{-1}(\cdot)$ denotes the inverse of the Gaussian $Q$-function.

**Proof:** See Appendix B.

**Remark 1:** For $P_Z = \mathcal{N}(0, 1)$, (39) recovers the dispersion $V(P) = \frac{P(2+P)}{2(1+P^2)} \log^2 e$ of the AWGN channel [11, Th. 54].

**B. The exponential-noise channel**

We next consider the exponential-noise case, i.e., $P_Z = \text{Exp}(1)$. As in [12], we assume that each codeword $x^n \in \mathbb{R}^n$ must satisfy

$$x_i \geq 0 \quad \text{and} \sum_{i=1}^n x_i \leq n \sigma.$$  \hspace{1cm} (42)

The practical relevance of such a channel is discussed in [12], [22]. The capacity of the exponential-noise channel with constraint (42) is given by [12, Th. 3]

$$C(\sigma) = \log(1 + \sigma) \hspace{1cm} (43)$$

and is achieved by the input distribution $P_{X^n}$, according to which $X$ takes the value zero with probability $1/(1 + \sigma)$ and follows an $\text{Exp}(1 + \sigma)$ distribution conditioned on it being positive. Furthermore, the capacity-achieving output distribution is $\text{Exp}(1 + \sigma)$.

**Theorem 4:** For the additive-exponential noise channel subject to the constraint (42) and for $0 < \epsilon < 1$,

$$R^*(n, \epsilon) = \log(1 + \sigma) - \sqrt{\frac{V(\sigma)}{n}} Q^{-1}(\epsilon) + O\left(\frac{\log n}{n}\right)$$

where

$$V(\sigma) = \frac{\sigma^2}{(1 + \sigma)^2} \log^2 e. \hspace{1cm} (45)$$

**Proof:** See Appendix C.

**C. Minimum energy per bit over AWGN channels**

For a complex-valued AWGN channel, we set $\mathcal{A} = \mathbb{C}^n$, $\mathcal{B} = \mathbb{C}^n$, and $P_{Y^n|X^n = x^n} = \mathcal{CN}(x^n, L_n)$. We assume that every codeword $x^n$ satisfies the equal power constraint

$$\|x^n\|^2 = nP. \hspace{1cm} (46)$$

Let $R_e^*(n, \epsilon, P)$ denote the maximum coding rate $R^*(n, \epsilon)$ under the constraint (46). In Theorem 5 below, we provide expressions for $\beta$ functions in (4) and (8) for the AWGN case.

**Theorem 5:** Consider the complex-valued AWGN channel $P_{Y^n|X^n}$. Let $S_n \sim \chi^2_{2n}(2nP)$ and $L_n \sim \chi^2_{2n}(0)$. Let $Q_{Y^n} = \mathcal{CN}(0, I_n)$. Furthermore, let $S_n \triangleq \{x^n \in \mathbb{C}^n : \|x^n\|^2 = nP\}$. Then, for every distribution $P_{X^n}$ supported on $S_n$

$$\beta_o(P_{X^n|Y^n}, P_{X^n}, Q_{Y^n}) = Q\left(\sqrt{2nP} + Q^{-1}(\alpha)\right) \hspace{1cm} (47)$$

and

$$\beta_o(P_{X^n|Y^n} \circ P_{X^n}, Q_{Y^n}) \leq \mathbb{P}[L_n \geq \gamma] \hspace{1cm} (48)$$

where $\gamma$ satisfies

$$\mathbb{P}[S_n \geq \gamma] = a. \hspace{1cm} (49)$$

Furthermore, (48) holds with equality if $P_{X^n}$ is the uniform distribution over $S_n$.

**Proof:** See Appendix D.

By evaluating (47) and (48) in the asymptotic regime $P \to 0$ and $nP^2 \to \infty$ as $n \to \infty$ and by substituting the resulting expressions in Theorem 1 and in (4), we obtain the following result.

**Theorem 6:** For an AWGN channel with SNR $P_n$ satisfying $P_n \to 0$ and $nP^2 \to \infty$ as $n \to \infty$, the maximum coding rate $R^*(n, \epsilon, P_n)$ behaves as

$$\frac{R^*(n, \epsilon, P_n)}{\log e} \to P_n - \sqrt{\frac{2P_n}{n}} Q^{-1}(\epsilon) - \frac{1}{2} P_n^2 \hspace{1cm} + o\left(\sqrt{\frac{P_n}{n}}\right) + o\left(P_n^2\right), \hspace{1cm} n \to \infty. \hspace{1cm} (50)$$

**Proof:** See Appendix E.

\footnote{As we shall see, this regime is of interest for the characterization of the minimum energy per bit.}
We now relate (50) to the minimum energy per bit \( E_b'(k,\epsilon,R) \) to transmit \( k \) information bits at rate \( R \) and error probability \( \epsilon \). Specifically, Theorem 6 implies that
\[
10\log_{10} E_b'(k,\epsilon,R) = 10\log_{10} \frac{R_c(n,\epsilon,P_n)}{P_n}
\]
\[
= 10\log_{10} \left( \log_e 2 + \frac{2\log_e 2}{k} Q^{-1}(\epsilon) + \frac{\log^2 2}{2} \frac{R}{k} \right) + o(R) + o(1/\sqrt{k})
\]
\[
= 10\log_{10} E_b'(k,\epsilon,0) + 10\log_{10} \frac{R}{k} + o(R) + o\left(\frac{1}{\sqrt{k}}\right).
\]  

The last step follows from [23, Th. 3]. Note that (53) is the finite-blocklength counterpart of Verdú’s wideband-slope result [14, Eqs. (172)]. In Fig. 1, we present a comparison between the approximation (53) (with the \( o(\cdot) \) term omitted), the converse bound [11, Th. 28], and the achievability bound (8). In both cases \( Q_Y \) is chosen to be the capacity-achieving output distribution. For the parameters considered in Fig. 1, the approximation (53) is accurate.

D. MIMO block-fading channel with perfect CSIR

Consider an \( m_t \times m_r \) Rayleigh MIMO block-fading channel that stays constant for \( n_c \) channel uses. The input-output relation within the \( k \)th coherence interval is given by
\[
Y_k = X_k H_k + W_k.
\]  

Here, \( X_k \in \mathbb{C}^{m_t \times 1} \) and \( Y_k \in \mathbb{C}^{m_r \times 1} \) are the transmitted and received matrices, respectively; the entries of the fading matrix \( H_k \in \mathbb{C}^{m_t \times m_r} \) and the noise \( W_k \in \mathbb{C}^{m_r \times 1} \) are i.i.d. \( \mathcal{CN}(0,1) \). We assume that \( \{H_k\} \) and \( \{W_k\} \) take on independent realizations over successive coherence intervals. The channel matrices \( \{H_k\} \) are assumed to be known to the receiver but not to the transmitter. We shall also assume that each codeword spans \( l \in \mathbb{N} \) coherence intervals, i.e., the blocklength of the code is \( n = ln_c \). Finally, each codeword \( X^l \) is constrained to satisfy
\[
||X^l||_F \leq \sqrt{nP}.
\]  

To obtain an achievable bound on \( R^*(n,\epsilon) \), we apply Theorem 1 with \( P_{Y^l} \) chosen as the uniform distribution on \( S_n^c \triangleq \{X^l : ||X^l||_F^2 = nP\} \) and \( Q_{Y^l|X^l} \) chosen as the capacity-achieving output distribution. With these choices, we have
\[
R^*(n,\epsilon) \geq \frac{1}{n} \max_{\beta} \beta c \ln P_{Y^l|X^l} \left( P_{Y^l|X^l}, P_{Q_{Y^l|X^l}}, P_{Q_{Y^l|X^l}}\right).
\]  

The denominator \( \beta_1 - \epsilon + \tau (P_{Y^l|X^l}, P_{Q_{Y^l|X^l}}) \) using the data-processing inequality for \( \beta_1 \) as follows. Let \( X^l \) be a sequence of \( n_c \times m_t \) complex matrices with i.i.d. \( \mathcal{CN}(0,P/m_t) \) entries. Then, \( P_{Y^l} \) can be obtained via \( X^l \) through \( X^l = \sqrt{nP}\mathbb{F}^{1/2}/||X^l||_F^{1/2} \). Furthermore, \( Q_{Y^l|X^l} = P_{Y^l|X^l} \circ P_{X^l} \). Let \( P^{(s)}_{Y^l|X^l} \triangleq P_{Y^l|X^l}^{(s)} \), where \( P^{(s)}_{Y^l|X^l} \) denotes the channel law defined by
\[
Y_k = X_k H_k \frac{\sqrt{nP}}{||X^l||_F} + W_k, \quad k = 1, \ldots, l.
\]  

We have that \( P_{Y^l|X^l} = P_{Y^l|X^l}^{(s)} \circ P_{X^l} = P_{X^l}^{(s)} P_{Y^l|X^l} \circ P_{X^l} \). Now, by the data-processing inequality,
\[
\beta_1 - \epsilon + \tau (P_{Y^l|X^l}^{(s)}, P_{Q_{Y^l|X^l}}^{(s)}) \geq \beta_1 - \epsilon + \tau (P_{X^l}^{(s)}, P_{Q_{Y^l|X^l}}^{(s)}) \circ P_{X^l}.
\]  

Since the Radon-Nikodym derivative \( dP_{X^l}^{(s)} / dP_{X^l} \) can be computed in closed form, the right-hand side of (58) can be computed via Monte Carlo techniques. The resulting bound is compared with the normal approximation of \( R^*(n,\epsilon) \) in Fig. 2. In contrast, the \( n_c \) bound [11, Th. 25] with \( F = S_n^c \) is much more difficult to compute due to the maximization over
codewords $X^l \in S'_n$. Furthermore, for blocklength values of practical interest, we expect that

$$\max_{X^l \in S'_n} \beta_\alpha(P_{X^n|X^l=x^l}, Q_{X^n|X^l=x^l}) \gg \beta_\alpha(P_{X^n|X^l=x^l}, P_{X^n}, Q_{X^n|X^l=x^l}) \tag{59}$$

which means that the resulting bound is much looser than (56).

**APPENDIX**

**A. Proof of Lemma 2**

To prove (28), we assume without loss of generality that $P_1 P_2$ is supported on $X \times Y$ and so is $Q_1 Q_2$. Let $Z : X \times Y \to \{0, 1\}$ denote the Neyman-Pearson test between $P_1 P_2$ and $Q_1 Q_2$, i.e.,

$$P_1 P_2[Z(X, Y) = 1] = \alpha \tag{60}$$

$$Q_1 Q_2[Z(X, Y) = 1] = \beta_\alpha(P_1 P_2, Q_1 Q_2). \tag{61}$$

Interpreting $Z(\cdot, \cdot)$ as a randomized test between $P_1$ and $Q_1$ and $Z(X, \cdot)$ between $P_2$ and $Q_2$, we obtain

$$Q_1 Q_2[Z(X, Y) = 1] \geq \beta_{\beta_\alpha(P_1 P_2, Q_1 Q_2)}(P_2, Q_2). \tag{62}$$

The last step follows by the monotonicity of $\alpha \mapsto \beta_\alpha(P_1, Q_1)$. Combining (61) and (62), we conclude (28).

We next prove the first inequality in (29). Let $Z_1 : X \times Y \to \{0, 1\}$ be the Neyman-Pearson test that achieves $\beta_{\alpha - \delta_1}(P_{XY}, P_{X} Q_Y)$, and let $Z_2 : Y \to \{0, 1\}$ be the Neyman-Pearson test that achieves $\beta_{\delta_1}(P_Y, Q_Y)$. Consider the following test $Z : X \times Y \to \{0, 1\}:

$$Z(x, y) \equiv Z_1(x, y) \cdot (1 - Z_2(y)). \tag{64}$$

We have:

$$P_{XY}[Z = 1] = P_{XY}[Z_1 = 1, Z_2 = 0] \tag{65}$$

$$\geq P_{XY}[Z_2 = 0] - P_{XY}[Z_1 = 0] = \alpha. \tag{66}$$

Let

$$\tilde{\gamma} \equiv \sup\{\gamma : P_Y[dP_Y / dQ_Y \geq \gamma] \geq \delta_1\}. \tag{67}$$

By the Neyman-Pearson lemma, we have $dP_Y / dQ_Y \geq \tilde{\gamma}$ for every $y$ such that $Z_2(y) = 1$. Hence,

$$\beta_\alpha(P_{XY}, P_X P_Y) \leq \beta_{\tilde{\gamma}}(P_{XY}|Z_1 = 1)(P_{XY}, P_X P_Y) \leq P_{XY}[Z = 1] \tag{68}$$

$$\leq P_{XY}[Z_1 = 1] \tag{69}$$

$$\leq \tilde{\gamma} P_X Q_Y[Z_1 = 1] \tag{70}$$

$$= \tilde{\gamma} \beta_{\alpha - \delta_1}(P_{XY}, P_X Q_Y) \tag{71}$$

$$\leq \beta_{\alpha - \delta_1}(P_{XY}, P_X Q_Y) / \beta_{\delta_1}(P_X Q_Y). \tag{72}$$

Here, (68) follows from (66) and because $\alpha \mapsto \beta_\alpha(\cdot, \cdot)$ is monotonically nondecreasing; (71) follows from the definition of the test $Z_1$; finally, (72) follows from (67) and [11, Eq. (103)]. The proof of the second inequality in (30) follows from similar steps and is omitted.

Finally, to prove (31), we use the data-processing inequality for Rényi divergence [20] and view the Neyman-Pearson test between $P$ and $Q$ as a map from the support of $P$ and $Q$ to $\{0, 1\}$. This yields

$$D_\lambda(P||Q) \geq d_\lambda(\alpha || \beta_\alpha) \tag{73}$$

$$= \frac{1}{\lambda - 1} \log((\alpha^\lambda \beta_\alpha^{1-\lambda} + (1 - \alpha)^\lambda (1 - \beta_\alpha)^{1-\lambda}) \tag{74}$$

where $d_\lambda(\cdot || \cdot)$ denote the binary Rényi divergence [18, Eq. (23)], and where $\beta_\alpha \equiv \beta_\alpha(P, Q)$. By further lower-bounding $(1 - \beta_\alpha)^{1-\lambda}$ by 1 (recall that $\lambda > 1$), and solving the resulting inequality for $\beta_\alpha$, we obtain (31).

**B. Proof of Theorem 3**

Let $P_{Y^n} \triangleq P_{Y^n|X^n} \circ P_{X^n}$ and let $Q_{Y^n} \triangleq P_{Y^n|X^n} \circ Q_{X^n}$. We will apply Theorem 1 to the channel (33) with $\tau = 1/\sqrt{n}$ and with $P_{X^n}$ and $Q_{Y^n}$ chosen as above. For the term $\beta_{\tau}(P_{Y^n}, Q_{Y^n})$, we have

$$\log \beta_{\tau}(P_{Y^n}, Q_{Y^n}) \geq \log \beta_{\tau}(P_{X^n}, Q_{X^n}) \tag{75}$$

$$= \log Q_{X^n} \left[ nP - \log n \leq \sum_{i=1}^n X_i^2 \leq nP \right] + \log \tau \tag{76}$$

$$= \log \left( Q \left( \frac{-\log n}{\sqrt{2nP^2}} \right) - Q \left( 0 \right) - O \left( \frac{1}{\sqrt{n}} \right) \right) + \log \tau \tag{77}$$

$$= O(\log n). \tag{78}$$

Here, (75) follows from the data-processing inequality (25); (76) follows by using the Neyman-Pearson lemma and by observing that $dP_{X^n} / dQ_{X^n}$ is a binary random variable; (77) follows from the Berry-Esseen theorem [24, Sec. XVI.5].

Let $p_Z$ and $q_Y$ be the probability density function (pdf) corresponding to the distributions $P_Z$ and $Q_Y$, respectively. Since $Q_X$ is a Gaussian distribution, it follows that $q_Y$ is smooth. To evaluate $\beta_{1+\epsilon}(P_{Y^n|Y^n}, P_{X^n} Q_{Y^n})$, we shall prove that, under $P_{X^n|Y^n}$, the random variable

$$\log \frac{dP_{Y^n|X^n}}{dQ_{Y^n}}(X^n, Y^n) \sim \sum_{i=1}^n \left( \log p_Z(Z_i) - \log q_Y(X_i + Z_i) \right) \tag{79}$$

is asymptotically normal as $n \to \infty$. The main difficulty in establishing this result is that, under $P_{X^n|Y^n}$, the $\{X_i\}$ are not independent, which prevents us from using the Berry-Esseen theorem. To circumvent this difficulty, we introduce a joint probability distribution $P_{X^n, \tilde{X}^n}$ with marginals $X^n \sim P_{X^n}$ and $\tilde{X}^n \sim Q_{X^n}$, under which $E \left[ \|X^n - \tilde{X}^n\|^2 \right]$ is small, and we approximate $\log q_Y(X_i + Z_i)$ by $\log q_Y(X_i + Z_i)$. Specifically, let $P_{X^n, \tilde{X}^n}$ be the joint distribution for which $X^n / \|X^n\| = \tilde{X}^n / \|\tilde{X}^n\|$ and for which $\|X^n\|$ is independent of $\|\tilde{X}^n\|$. Writing $\Delta_i \equiv X_i - X_i$ and $f(y) \equiv \log q_Y(y)$, we next relate $f(X_i + Z_i)$ to $f(X_i + Z_i)$ as follows:

$$f(\tilde{X}_i + Z_i) - f(X_i + Z_i)$$

$$= \int_0^1 \Delta_i f'(Z_i + X_i + \Delta_i t) dt \tag{80}$$

4In this appendix, statements involving “=”, “≥”, and “≤” hold with probability one, whenever random variables are involved.
\[
\Delta_i f'(\hat{X}_i + Z_i) - \Delta_i^2 \int_0^1 tf''(X_i + Z_i + t\Delta_i)dt \tag{81}
\]
where in the last step we used integration by parts. The second-order derivative \(f''(y)\) can be computed as follows (see [25, Eq. (131)])
\[
f''(y) = \frac{d^2 \log q_{Y}(y)}{dy^2} = -\frac{\log e}{P} + \frac{\log e}{P^2} \Var[X|Y = y] \tag{82}
\]
\[
\leq -\frac{\log e}{P} + \frac{2 \log e}{P^2} (y^2 + \Var[Z]) \tag{83}
\]
where the conditional variance on the right-hand side (RHS) of (82) is computed with respect to \((X,Y) \sim Q_X P_{Y|X}\). Here, (83) follows from steps similar to the ones leading to [25, Eq. (169)]. Substituting (83) into (81) and upper-bounding \(t\) by 1, we obtain
\[
f(X_i + Z_i) \leq f(\hat{X}_i + Z_i) - \Delta_i f'(\hat{X}_i + Z_i) + \frac{\log e}{P} \Delta_i^2 \left(c_0 + \frac{2}{P} \int_0^1 (X_i + Z_i + t\Delta_i)^2 dt \right) \tag{84}
\]
where \(c_0 \triangleq \frac{2 \Var[Z]}{P} - 1\). Furthermore,
\[
\Delta_i = \hat{X}_i - X_i = \frac{\hat{X}_i}{\|X^n\|} \left(\|\hat{X}^n\| - \sqrt{nP}\right) + \frac{X_i}{\|X^n\|} \left(\sqrt{nP} - \|X^n\|\right) \tag{85}
\]
where in the last step we used that \(\hat{X}^n/\|\hat{X}^n\| = X^n/\|X^n\|\), and that both \(X^n/\|X^n\|\) and \(X^n/\|X^n\|\) are independent of \(\|X^n\|^P\). Letting
\[
A_{1,i} \triangleq \log p_Z(Z_i) - f(\hat{X}_i + Z_i) = i(\hat{X}_i, \hat{X}_i + Z_i) \tag{87}
\]
\[
T_{2,i} \triangleq f'(\hat{X}_i + Z_i) \frac{\hat{X}_i}{\|X^n\|} \left(\sqrt{nP} - \|X^n\|^P\right) \tag{88}
\]
and substituting (84) and (86) into (79), we obtain
\[
\sum_{i=1}^n \left(\log p_Z(Z_i) - \log q_Y(X_i + Z_i)\right) \leq \sum_{i=1}^n \left(A_{1,i} + f'(\hat{X}_i + Z_i)\frac{\hat{X}_i}{\|X^n\|} \left(1 - \frac{\sqrt{nP}}{\|X^n\|}\right) - T_{1,i} + T_{2,i}\right). \tag{89}
\]
Using (89) together with the inequality
\[
P[A + B \leq a + b] \leq P[A \leq a] + P[B \leq b] \tag{90}
\]
we conclude that for every \(\gamma, \gamma_1, \) and \(\gamma_2\),
\[
P_{X^n Y^n} \left[\log \frac{dP_Y|X^n}{dQ_Y|X^n}(X^n, Y^n) \leq \gamma - \gamma_1 - \gamma_2\right] \leq P \left[\sum_{i=1}^n A_{1,i} + f'(\hat{X}_i + Z_i)\frac{\hat{X}_i}{\|X^n\|} \left(1 - \frac{\sqrt{nP}}{\|X^n\|}\right) \leq \gamma\right] + P \left[\sum_{i=1}^n T_{1,i} \geq \gamma_1\right] + P \left[-\sum_{i=1}^n T_{2,i} \geq \gamma_2\right]. \tag{91}
\]
We next upper-bound the three probability terms on the RHS of (91) separately. To bound the first term, we shall use the central-limit theorem for functions [26, Prop. 1] (see also [27, Prop. 1]) and follow similar steps as in [26, Sec. IV.D]. Let
\[
A_{2,i} \triangleq f'(\hat{X}_i + Z_i)\hat{X}_i \tag{92}
\]
\[
A_{3,i} \triangleq \hat{X}_i^2 - P. \tag{93}
\]
It follows that \(\{[A_{1,i}, A_{2,i}, A_{3,i}]\}\) are i.i.d. random vectors. Note also that
\[
E[A_{1,i}] = I(P), \quad E[A_{3,i}] = 0 \tag{94}
\]
and that
\[
E[A_{2,i}] = E \left[f'(\hat{X}_1 + Z_1)\hat{X}_1\right] \tag{95}
\]
\[
= \int x p_X(x)p_Z(x) \frac{\log e}{P} e^{-x} dx dx \tag{96}
\]
\[
= -\frac{\log e}{P} \int x^2 p_X(x)p_Z(x)p_X|Y(x|x+z)dxdz \tag{97}
\]
\[
= -\frac{\log e}{P} \int x p_X(x)p_Y|X(x|y)p_X|Y(x|y)dxdy \tag{98}
\]
\[
= -\frac{\log e}{P} \Var[Y|X] \tag{99}
\]
\[
= \frac{\log e}{P} \mmse(X|Y) - P. \tag{100}
\]
The conditional expectations in (96) and (99) are computed with respect to \((X,Y) \sim Q_X P_{Y|X}\); the functions \(p_X, p_{Y|X}\), and \(p_{Y|X}\) are the (conditional) pdfs corresponding to \(Q_X, P_Y|X,\) and \(P_X|Y\), respectively, and \(\mmse(X|Y)\) in (100) is defined in (41). Here, (96) follows from [28, Eq. (15)]; in (98) we have used the change of variables \(y = x + z\) and that \(p_{Y|X}(y|x) = p_Z(y-x)\); and finally (100) follows because
\[
\Var[X|Y] = P. \tag{101}
\]
Furthermore, we have
\[
\Var[A_{2,i}]^3 \leq \Var[\hat{X}_i]^3 (c_1 |\hat{X}_1| + c_2)^3 \leq c_3 \Var[\hat{X}_i]^6 + c_4 \Var[\hat{X}_i]^3 \Var[Z_i] < \infty \tag{102}
\]
where \(c_1, c_2, c_3, c_4\) are finite constants. Here, (101) follows from (92) and [28, Prop. 2], and (102) follows because \(\Var[Z_i]^3 \leq \sqrt{\Var[Z_i]^6} < \infty\). Since \(\Var[A_{1,i} - I(P)]^3 < \infty\) by assumption and since \(\Var[A_{3,i}]^3 < \infty\), we have verified that the vector \([A_{1,i}, A_{2,i}, A_{3,i}]\) has finite third central moment. Let now
\[
g(a_1, a_2, a_3) \triangleq a_1 + a_2 \left(1 - \frac{\sqrt{P}}{P + a_3}\right). \tag{103}
\]
We have
\[
g \left(\frac{1}{n} \sum_{i=1}^n A_{1,i}, \frac{1}{n} \sum_{i=1}^n A_{2,i}, \frac{1}{n} \sum_{i=1}^n A_{3,i}\right) = \frac{1}{n} \sum_{i=1}^n \left(A_{1,i} + f'(\hat{X}_i + Z_i)\hat{X}_i \left(1 - \frac{\sqrt{nP}}{\|X^n\|}\right)\right). \tag{104}
\]
Let \(j\) denote the Jacobian of \(g\) at \((I(P), E[A_{2,i}], 0)\), and let \(V\) denote the covariance matrix of \([A_{1,i}, A_{2,i}, A_{3,i}]\). It follows
where $c$ is defined in (40). Furthermore,

\[
\begin{align*}
  jV_j^T &= \text{Var}[A_{1,1} + c \sqrt{n} \mathbb{E}_Z i(\tilde{X}_1; \tilde{X}_1 + Z_i)] \\
  &= \text{Var}[A_{1,1} + c \tilde{X}_1^2] \\
  &= \text{Var}[\tilde{X}_1 + Z_i][\tilde{X}_1] \\
  &\quad + \text{Var}_{\tilde{X}_1} [\mathbb{E}_{Z_i} i(\tilde{X}_1; \tilde{X}_1 + Z_i)] + c \tilde{X}_1^2 \\
  &= V(P)
\end{align*}
\]

where $V(P)$ is defined in (39). We now invoke [27, Prop. 1] and obtain

\[
\Pr \left[ \sum_{i=1}^n A_{1,i} + f'(\tilde{X}_i + Z_i) \tilde{X}_i \left( 1 - \frac{\sqrt{n}P \cdot \tilde{X}_i}{\|X^n\|} \right) \leq c \right] \\
\leq Q \left( \frac{nI(P) - \gamma}{\sqrt{nV(P)}} \right) + O \left( \frac{1}{\sqrt{n}} \right) .
\]

We next upper-bound the second term on the RHS of (91). Note first that, by (132),

\[
0 \leq \sqrt{n}P - \|X^n\| \\
\leq \sqrt{n}P - \sqrt{n}P - \log n \leq \tilde{c}_1 n^{-1/2} \log n
\]

for some $\tilde{c}_1 > 0$ and sufficiently large $n$. Evaluating the integral on the RHS of (84), using (86) and (112), and using that $(a + b)^2 \leq 2(a^2 + b^2)$, we obtain

\[
\frac{P}{\log e} T_{1,i} = \Delta_i^2 \left( c_0 + \frac{2}{P} (\tilde{X}_i + Z_i - \Delta_i/2)^2 + \frac{\Delta_i^2}{6P} \right) \\
\leq 2 \left( 1 - \frac{\sqrt{n}P}{\|X^n\|} \right)^2 \tilde{X}_i^2 \left( c_0 + \frac{4}{P} (\tilde{X}_i + Z_i)^2 \right) \\
\leq \tilde{T}_{1,i} \\
\leq \tilde{T}_{1,i}
\]

\[
\leq \tilde{T}_{1,i} \\
\leq \tilde{T}_{1,i}
\]

Set $\gamma_1 = (\tilde{c}_2 \tilde{c}_3 + 1)(\log n) \cdot (\log e)/P$, where $\tilde{c}_2$ and $\tilde{c}_3$ are sufficiently large constants. We have

\[
\Pr \left[ \sum_{i=1}^n T_{1,i} \geq \gamma_1 \right] \leq \Pr \left[ T_3 \geq \frac{\tilde{c}_2 \log n}{n} \right] + \Pr \left[ \sum_{i=1}^n T_{4,i} \geq \tilde{c}_3 n \right] \\
\leq \Pr \left[ \sum_{i=1}^n T_{5,i} \geq \log n \right]
\]

which follows by a repeated use of (90). The first term on the RHS of (115) is upper-bounded by

\[
\Pr \left[ T_3 \geq \frac{\tilde{c}_2 \log n}{n} \right] \\
\leq \Pr \left[ \|X^n\| \geq \frac{n\sqrt{P}}{\sqrt{n} - (\tilde{c}_2/2) \log n} \right] \\
+ \Pr \left[ \|X^n\| \leq \frac{n\sqrt{P}}{\sqrt{n} + (\tilde{c}_2/2) \log n} \right].
\]

The first term on the RHS of (116) can be further upper-bounded as

\[
\Pr \left[ \|X^n\| \geq \frac{n\sqrt{P}}{\sqrt{n} - (\tilde{c}_2/2) \log n} \right] \\
\leq \Pr \left[ \|X^n\|^2 \geq nP(1 + \sqrt{\tilde{c}_2 (\log n)/(2n)})^2 \right] \\
\leq Q \left( \sqrt{\tilde{c}_2 \log n + \frac{\tilde{c}_2 \log n}{2\sqrt{2n}}} + O \left( \frac{1}{\sqrt{n}} \right) \right) \\
= O \left( \frac{1}{\sqrt{n}} \right).
\]

Here, in (117) we used that $1/(1-x) \geq (1+x)$ for every $x \in (0,1)$; (118) follows from the Berry-Esseen theorem; (119) follows by using $Q(x) \leq e^{-x^2/2}$ and by taking $\tilde{c}_2$ sufficiently large.

We can upper-bound the second term on the RHS of (116) using similar methods and obtain

\[
\Pr \left[ T_3 \geq \frac{\tilde{c}_2 \log n}{n} \right] \leq O \left( \frac{1}{\sqrt{n}} \right).
\]

Furthermore, we can upper-bound the second term on the RHS of (115) using again the Berry-Esseen theorem and the assumption $E \left| Z_i \right| < \infty$. Doing so we obtain that, for sufficiently large $\tilde{c}_3$,

\[
\Pr \left[ \sum_{i=1}^n T_{4,i} \geq \tilde{c}_3 n \right] \leq O \left( \frac{1}{\sqrt{n}} \right).
\]

Finally, to bound the last term on the RHS of (115), we observe that

\[
E \left[ \sum_{i=1}^n T_{5,i} \right] = O \left( \frac{\log^2 n}{n} \right)
\]

which follows from algebraic manipulations. Since $T_{5,i} \geq 0$, by Markov’s inequality, this implies that

\[
\Pr \left[ \sum_{i=1}^n T_{5,i} \geq \log n \right] \leq O \left( \frac{\log n}{n} \right).
\]

Substituting (120), (121), and (123) into (115), we conclude that

\[
\Pr \left[ \sum_{i=1}^n T_{1,i} \geq \gamma_1 \right] \leq O \left( \frac{1}{\sqrt{n}} \right).
\]

To bound the third term on the RHS of (91), we notice that, by the analysis in (92)–(110), the random variable

\[
\|X^n\|^{-1} \sum_{i=1}^n f'(\tilde{X}_i + Z_i) \tilde{X}_i - \frac{\sqrt{n} E[A_{2,1}]}{\sqrt{P}}
\]
By construction, the data-processing inequality and the Berry-Esseen Theorem.

For the exponential-noise channel, $\beta_{1-\epsilon+\tau}(P_{X_n}^{Y_n}, P_{X_n}^{Q_{Y_n}})$ is easy to compute. Indeed, under $P_{X_n}^{Y_n}$, the random variable $\log d_{p_{Y_n|i^n}}(X^n, Y_n)$ has the same distribution as

$$n \log (1 + \sigma) + \frac{\log e}{1 + \sigma} \sum_{i=1}^{n} X_i - \frac{\sigma}{1 + \sigma} \sum_{i=1}^{n} Z_i.$$ (134)

This random variable depends on the codeword $X^n$ only through $\sum_{i=1}^{n} X_i$. Furthermore, given $\sum_{i=1}^{n} X_i = X_n$, this random variable is the sum of $n$ i.i.d. random variables. Using the Berry-Esseen theorem and (132) to evaluate (134), we conclude that

$$\log \beta_{1-\epsilon+\tau}(P_{X_n}^{Y_n}, P_{X_n}^{Q_{Y_n}}) = n \log (1 + P) - \sqrt{n} (\sigma Q^{-1}(\epsilon) + O(\log n)).$$ (135)

Substituting (135) and (133) into (8), we establish that (44) is achievable. The converse follows from the meta-converse theorem [11, Th. 27] and from (135).

**D. Proof of Theorem 5**

Due to the spherical symmetry of $S_n$ and $Q_{Y^n}$, we have that $\beta_{\sigma}(P_{Y^n|x^n}=x^n, Q_{Y^n})$ is independent of $x^n \in S_n$. Let $\tilde{x}^n = \{\sqrt{P}0, \ldots, 0\}$. By [11, Lemma 29], for every $P_X^n$ supported on $S_n$,

$$\beta_{\sigma}(P_{X^n}^{Y^n}, P_{X^n}^{Q_{Y^n}}) = \beta_{\sigma}(P_{Y^n|x^n=\tilde{x}^n}, Q_{Y^n}) = \beta_{\sigma}(CN(\sqrt{n}P, 1), CN(0, 1)).$$ (136)

We obtain (47) by applying the Neyman-Pearson lemma to the RHS of (137).

To prove (48), it suffices to observe that $Z(y^n) = 1\{2\|y^n\|^2 \geq \gamma\}$ defines a test between $P_{X^n}$ and $Q_{Y^n}$. Furthermore, under $P_{X^n}$, the random variable $2\|Y^n\|^2$ has the same distribution as $S_n$ regardless of $P_{X^n}$, and under $Q_{Y^n}$, it has the same distribution as $L_n$.

It remains to show that (48) holds with equality if $P_{X^n}$ is the uniform distribution over $S_n$. In this case, both $P_{X^n}$ and $Q_{Y^n}$ are isotropic, and, hence, $2\|Y^n\|^2$ is a sufficient statistics for testing between $P_{X^n}$ and $Q_{Y^n}$. Let $p_0$ and $p_1$ denote the pdfs of $\chi_2^n(2nP)$ and $\chi_2^n(0)$, respectively. Following simple algebraic manipulations, it can be shown that $t \mapsto \frac{p_1(t)}{p_0(t)}$ is monotonically nondecreasing on $(0, \infty)$. Hence, the test $Z(y^n) = 1\{2\|y^n\|^2 \geq \gamma\}$ coincides with the Neyman-Pearson test between $\chi_2^n(2nP)$ and $\chi_2^n(0)$. The desired result follows then from the Neyman-Pearson lemma.

**E. Proof of Theorem 6**

Choosing $P_{X^n}$ to be the uniform distribution over $S_n$, substituting (47) and (48) into (8), and setting $a = \tau_n \triangleq \max\{(1 + 3\sqrt{2})n^{-1/2}, e^{-n\tau_n^2/2}\}$, we obtain

$$R_c^a(n, \epsilon, P_n) \geq \frac{1}{n} \log \frac{P[L_n \geq \gamma]}{Q(\sqrt{2n}P_n + Q^{-1}(1 - \epsilon + \tau_n))},$$ (138)

where $L_n$ and $\gamma$ are defined in Theorem 5. Using the expansion of the $Q$-function given in [29, Eq. (3.53)], we obtain that as
Next, we compute the numerator of (138). Since $S_n$ in (49) has the same distribution as $\sum_{i=1}^n (Z_i + \sqrt{P} Z_n)^2$ with $Z_i \sim N(0, 1)$, we can estimate $\mathbb{P}[S_n \geq \gamma]$ using the Berry-Esseen theorem as

$$\left| \mathbb{P}[S_n \geq \gamma] - Q\left( \frac{\gamma - 2n(1 + P_n)}{\sqrt{4n(1 + 2P_n)}} \right) \right| \leq \frac{2^{1/2}(1 + 3P_n)}{(1 + 2P_n)^{3/2}\sqrt{n}} \leq k_1/\sqrt{n} \quad (140)$$

where $k_1 \triangleq 2\sqrt{2}$. Using (49) and recalling $a = \tau_n$, we obtain

$$\gamma \leq 2n(1 + P_n) + \sqrt{4n(1 + 2P_n)}Q^{-1}(\tau_n - k_1/\sqrt{n}) \triangleq \tilde{\gamma}. \quad (142)$$

Furthermore, we have

$$\log \mathbb{P}[L_n \geq \gamma] \geq \log \mathbb{P}[L_n \geq \tilde{\gamma}] \geq \frac{1}{2} \left( (\tilde{\gamma} - 2n) \log e + (2n - 2) \log \frac{\tilde{\gamma}}{2n} + \log(2n) \right) - \log 2 \quad (144)$$

$$= -\frac{1}{2}nP_n \log e + o(nP_n^2), \quad nP_n \rightarrow \infty. \quad (145)$$

Here, (144) follows from [30, Lemma 5] and because $L_n \sim \chi^2_{2n}(0)$, and (145) follows from (142) and from algebraic manipulations. Substituting (139) and (145) into (138), we conclude that (50) is achievable.

To prove the converse, we substitute (47) and (48) into (4), and set $a = \alpha_n = 1 - \tau_n$. Doing so we obtain

$$R^*(n, e, P_n) \leq -\frac{1}{n} \log Q\left( \frac{\gamma'}{\sqrt{2nP_n} + Q^{-1}(\alpha_n - \epsilon)} \right) \quad (146)$$

where $\gamma'$ satisfies $\mathbb{P}[S_n \geq \gamma'] = \alpha_n$. The denominator in the RHS of (146) admits the same asymptotic expansion as (139). To evaluate the numerator in the RHS of (146), we repeat the steps as in (140)–(142) for $\gamma'$ and obtain

$$\gamma' \geq 2n(1 + P_n) + \sqrt{4n(1 + 2P_n)}Q^{-1}(\alpha_n + k_1/\sqrt{n}) \triangleq \gamma''. \quad (147)$$

Furthermore, we have

$$\log \mathbb{P}[L_n \geq \gamma'] \leq \log \mathbb{P}[L_n \geq \tilde{\gamma}'] \leq -\frac{1}{2}nP_n \log e + o(nP_n^2) \quad (149)$$

$$= -\frac{1}{2}nP_n \log e + o(nP_n^2), \quad nP_n \rightarrow \infty. \quad (150)$$

Here, (149) follows from [31, Eq. (4.3)], and (150) follows from (147) and from algebraic manipulations. Finally, we conclude the proof of Theorem 6 by substituting (139) and (150) into (146).

REFERENCES


