Minimum Energy to Send k Bits Over Multiple-Antenna Fading Channels

Wei Yang, *Member, IEEE*, Giuseppe Durisi, *Senior Member, IEEE*, and Yury Polyanskiy, *Senior Member, IEEE*

***Abstract*— This paper investigates the minimum energy required to transmit k information bits with a given reliability over a multiple-antenna Rayleigh block-fading channel, with and without channel state information (CSI) at the receiver. No feedback is assumed. It is well known that the ratio between the minimum energy per bit and the noise level converges to -1.59 dB as k goes to infinity, regardless of whether CSI is available at the receiver or not. This paper shows that the lack of CSI at the receiver causes a slowdown in the speed of convergence to -1.59 dB as $k \to \infty$ compared with the case of perfect receiver CSI. Specifically, we show that, in the no-CSI case, the gap to -1.59 dB is proportional to $((\log k)/k)^{1/3}$, whereas when perfect CSI is available at the receiver, this gap is proportional to $1/\sqrt{k}$. In both cases, the gap to -1.59 dB is independent of the number of transmit antennas and of the channel's coherence time. Numerically, we observe that, when the receiver is equipped with a single antenna, to achieve an energy per bit of -1.5 dB in the no-CSI case, one needs to transmit at least 7×10^7 information bits, whereas 6×10^4 bits suffice for the case of perfect CSI at the receiver.**

***Index Terms*— Channel coding, energy efficiency, minimum energy per bit, multiple-antenna fading channels, nonasymptotic analysis.**

I. Introduction

A CLASSIC result in information theory is that, for a wide range of channels including AWGN channels and fading channels, the minimum energy per bit E_b required for reliable communication satisfies [1], [2]

$$\frac{E_\mathrm{b}}{N_0}_{\min} = \log_e 2 = -1.59\,\mathrm{dB}. \tag{1}$$

Here, N_0 is the noise power per complex degree of freedom. For fading channels, (1) holds regardless of whether the instantaneous fading realizations are known to the receiver or not [2, Th. 1], [3].[1]

The expression in (1) is asymptotic in several aspects:

- the blocklength n of each codeword is infinite;
- the number of information bits k, or equivalently, the number of messages $M = 2^k$ is infinite;
- the error probability ϵ vanishes;
- the total energy E is infinite;
- E/n vanishes.

For many channels, the limit in (1) does not change if we allow the error probability to be positive. However, keeping any of the other parameters fixed results in a backoff from (1) [2], [4]–[8].

In this paper, we study the maximum number of information bits k that can be transmitted with a finite energy E and a fixed error probability $\epsilon > 0$ over a multiple-input multiple-output (MIMO) Rayleigh block-fading channel, when there is no constraint on the blocklength n. Equivalently, we determine the minimum energy E required to transmit k information bits with error probability ϵ. We consider two scenarios:

1) neither the transmitter nor the receiver have *a priori* channel state information (CSI);
2) perfect CSI is available at the receiver (CSIR) and no CSI is available at the transmitter.

Throughout the paper, we shall refer to these two scenarios as no-CSI case and perfect-CSIR case, respectively.

Related work: For nonfading AWGN channels with unlimited blocklength, Polyanskiy *et al.* [8] showed that the maximum number of codewords $M^*(E, \epsilon)$ that can be transmitted with energy E and error probability ϵ satisfies[2]

$$\log M^*(E,\epsilon) = \frac{E}{N_0}\log e - \sqrt{\frac{2E}{N_0}}Q^{-1}(\epsilon)\log e + \frac{1}{2}\log\frac{E}{N_0} + \mathcal{O}(1), \quad E \to \infty. \tag{2}$$

Here, $Q^{-1}(\cdot)$ denotes the inverse of the Gaussian Q-function. The first term on the right-hand side (RHS) of (2) gives the -1.59 dB limit. The second term captures the penalty due to the stochastic variations of the channel. This term plays the same role as the *channel dispersion* in finite-blocklength analyses [7], [9]. In terms of the minimum energy

Manuscript received July 14, 2015; revised May 19, 2016; accepted September 10, 2016. Date of publication October 6, 2016; date of current version November 18, 2016. This work was supported in part by the Swedish Research Council under Grant 2012-4571, and in part by the National Science Foundation CAREER Award under Grant CCF-12-53205. This paper was presented at the 2015 IEEE Information Theory Workshop and the 2015 IEEE International Symposium on Information Theory.

W. Yang is with the Department of Electrical Engineering, Princeton University, Princeton, NJ 08544 USA (e-mail: weiy@princeton.edu).

G. Durisi is with the Department of Signals and Systems, Chalmers University of Technology, 41296 Gothenburg, Sweden (e-mail: durisi@chalmers.se).

Y. Polyanskiy is with the Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, Cambridge, MA 02139 USA (e-mail: yp@mit.edu).

Communicated by D. Tuninetti, Associate Editor for Communications.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIT.2016.2615629

[1] Knowledge of the fading realizations at the transmitter may improve (1), because it enables the transmitter to signal on the channel maximum-eigenvalue eigenspace [2].

[2] Unless otherwise indicated, the log and the exp functions are taken with respect to an arbitrary fixed base.

per bit $E_{\mathrm{b}}^*(k,\epsilon)$ necessary to transmit k bits with error probability ϵ, (2) implies that, for large E,

$$\frac{E_{\mathrm{b}}^*(k,\epsilon)}{N_0} \approx \log_e 2 + \sqrt{\frac{2\log_e 2}{k}}\, Q^{-1}(\epsilon) \tag{3}$$

i.e., that the gap to -1.59 dB is proportional to $1/\sqrt{k}$. The asymptotic expansion (2) is established in [8] by showing that in the limit $E \to \infty$ a nonasymptotic achievability bound and a nonasymptotic converse bound match up to third order. The achievability bound is obtained by computing the error probability under maximum-likelihood decoding of a codebook consisting of M orthogonal codewords (e.g., uncoded M-ary pulse-position modulation (PPM)). The converse bound follows from the meta-converse theorem [7, Th. 27] with auxiliary distribution chosen equal to the noise distribution. Kostina *et al.* [10] generalized (2) to the setting of joint source and channel coding, and characterized the minimum energy required to reproduce k source samples with a given fidelity after transmission over an AWGN channel.

Moving to fading channels, for the case of no CSI, *flash signalling* [2, Definition 2] (i.e., peaky signals) must be used to reach the -1.59 dB limit [2]. In the presence of a peak-power constraint, (1) can not be achieved [11]–[14]. Verdú [2] studied the rate of convergence of the minimum energy per bit to -1.59 dB as the spectral efficiency vanishes. He showed that, differently from the perfect-CSIR case, in the no-CSI case the -1.59 dB limit is approached with *zero wideband slope*. Namely, the slope of the spectral-efficiency versus energy-per-bit function at -1.59 dB is zero. This implies that operating close to the -1.59 dB limit is very expensive in terms of bandwidth in the no-CSI case. For the scenario of finite blocklength n, fixed energy budget E, and fixed probability of error ϵ, bounds and approximations on the maximum channel coding rate over fading channels (under various CSI assumptions) are reported in [15]–[21].

Contributions: Focusing on the regime of unlimited blocklength, but finite energy E, and finite error probability ϵ, we provide upper and lower bounds on the maximum number of codewords $M^*(E,\epsilon)$ that can be transmitted over an $m_{\mathrm{t}} \times m_{\mathrm{r}}$ MIMO Rayleigh block-fading channel with channel's coherence interval of n_{c} symbols. For the no-CSI case, we show that for every $\epsilon \in (0, 1/2)$

$$\begin{aligned}\log M^*(E,\epsilon) &= \frac{m_{\mathrm{r}}E}{N_0}\log e - V_0 \cdot \left(\frac{m_{\mathrm{r}}E}{N_0}Q^{-1}(\epsilon)\right)^{2/3}\left(\log\frac{m_{\mathrm{r}}E}{N_0}\right)^{1/3} \\ &\quad + \mathcal{O}\left(\frac{E^{2/3}\log\log E}{(\log E)^{2/3}}\right), \quad E \to \infty \end{aligned} \tag{4}$$

where

$$V_0 = \left(12^{-1/3} + \left(\frac{2}{3}\right)^{1/3}\right)(\log e)^{2/3}. \tag{5}$$

Note that the asymptotic expansion (4) does not depend on the number of transmit antennas m_{t} and the channel's coherence interval n_{c}. The fact that the first term does not depend on n_{c} and m_{t} follows directly from [2, Eq. (52)] by noting that an $m_{\mathrm{t}} \times m_{\mathrm{r}}$ block-fading MIMO channel with coherence interval n_{c} is equivalent to an $m_{\mathrm{t}}n_{\mathrm{c}} \times m_{\mathrm{r}}n_{\mathrm{c}}$ memoryless MIMO fading channel with block-diagonal channel matrix [2, p. 1339]. Our result (4) shows that the same holds for the second term in the expansion of $\log M^*(E,\epsilon)$ for $E \to \infty$. In terms of minimum (received) energy per bit $E_{\mathrm{b}}^*(k,\epsilon)$, (4) implies that, for large E,[3]

$$\frac{E_{\mathrm{b}}^*(k,\epsilon)}{N_0} \approx \log_e 2 + V_0 \cdot \left(\frac{\log_e k}{k}\right)^{1/3}\left(Q^{-1}(\epsilon)\right)^{2/3}(\log_e 2)^{4/3} \tag{6}$$

i.e., the gap to -1.59 dB is proportional to $((\log_e k)/k)^{1/3}$.

We establish (4) by analyzing in the limit $E \to \infty$ an achievability bound and a converse bound. The achievability bound follows from a nonasymptotic extension of Verdú's capacity-per-unit-cost achievability scheme [5, pp. 1023–1024]. This scheme relies on a codebook consisting of the concatenation of uncoded PPM and a repetition code, and on a decoder that performs binary hypothesis testing. The converse bound relies on the meta-converse theorem [7, Th. 31] with auxiliary distribution chosen as in the AWGN case. The resulting bound involves an optimization over the infinite-dimensional space of input codewords (recall that in our setup there is no constraint on the blocklength n). By exploiting the Gaussianity of the fading process, we show that this infinite-dimensional optimization problem can be reduced to a three-dimensional one. The tools needed to establish this result are the ones developed by Abbe *et al.* [22] to prove Telatar's minimum outage probability conjecture for multiple-input single-output (MISO) Rayleigh-fading channels. Indeed, both problems involve the optimization of quantiles of a weighted convolution of exponential distributions.

The asymptotic analysis of achievability and converse bounds reveals the following tension: on the one hand, one would like to make the codewords peaky to overcome lack of channel knowledge; on the other hand, one would like to spread the energy of the codewords uniformly over multiple coherence intervals to mitigate the stochastic variations in the received signal energy due to the fading.

For the case of perfect CSIR, we prove that for every $\epsilon \in (0, 1/2)$

$$\begin{aligned}\log M^*(E,\epsilon) &= \frac{m_{\mathrm{r}}E}{N_0}\log e - \sqrt{\frac{2m_{\mathrm{r}}E}{N_0}}\,Q^{-1}(\epsilon)\log e \\ &\quad + \frac{1}{2}\log\frac{m_{\mathrm{r}}E}{N_0} + \mathcal{O}\left(\sqrt{\log E}\right), \quad E \to \infty. \end{aligned} \tag{7}$$

Note that the asymptotic expansion (7) is also independent of the number of transmit antennas m_{t} and the channel's coherence interval n_{c}. Furthermore, apart from an energy normalization resulting from the array gain, this asymptotic expansion coincides with the one given in (2) for the AWGN case up to a $\mathcal{O}\left(\sqrt{\log E}\right)$ term. In terms of minimum (received)

[3]By considering the received energy per bit instead of the transmit energy per bit, we account for the array gain resulting from the use of multiple receive antennas.

energy per bit, (7) implies that (3) holds also for the perfect-CSIR case.

To establish (7), we show that every code for the AWGN channel can be transformed into a code for the MIMO block-memoryless Rayleigh-fading channel having the same probability of error. This is achieved by concatenating the AWGN code with a rate $1/N$ repetition code, by performing maximum ratio combining at the receiver, and then by letting $N \to \infty$. We obtain a converse bound that matches the achievability bound up to third order as $E \to \infty$ by using again the meta-converse theorem and then by optimizing over all input codewords. The asymptotic analysis of the converse bound reveals that spreading the energy of the codewords uniformly across many coherence intervals is necessary to mitigate the stochastic variations in the energy of the received signal due to fading.

In both the no-CSI and the perfect-CSIR case, the asymptotic analysis of the achievability bound is based on a standard application of the Berry-Esseen central-limit theorem (see, e.g., [23, Ch. XVI.5]). The asymptotic analysis of the converse part in both cases is not as straightforward. The main difficulty is that, unlike for discrete memoryless channels and AWGN channels, we can not directly invoke the central-limit theorem to evaluate the information density, because the central-limit theorem may not hold if the energy of a codeword is concentrated on few of its symbols. To solve this problem, we develop new tools that rely explicitly on the Gaussianity of the fading process. Specifically, for the no-CSI case, we exploit the log-concavity of the information density to lower-bound its cumulative distribution function (cdf). The resulting bound allows us to eliminate the codewords for which the central-limit theorem does not apply. For the perfect-CSIR case, we show that the distribution of the information density is unimodal and *right-skewed* (i.e., its mean is greater than its mode). Using this result, we then prove that to optimize the cdf of the information density, it is necessary to reduce its "skewness", thereby showing that the optimized information density must converge as $E \to \infty$ to a (non-skewed) Gaussian distribution.

By comparing (7) with (4), we see that, although the minimum (received) energy per bit approaches (1) as k increases regardless of whether CSIR is available or not, the convergence is slower for the no-CSI case. For the case $m_{\mathrm{r}} = 1$, our nonasymptotic bounds reveal that to achieve an energy per bit of -1.5 dB, one needs to transmit at least 7×10^7 information bits in the no-CSI case, whereas 6×10^4 bits suffice in the perfect-CSIR case. Furthermore, the bounds also reveal that it takes 2 dB more of energy to transmit 1000 information bits in the no-CSI case compared to the perfect-CSIR case.

Notation: Upper case letters such as X denote scalar random variables and their realizations are written in lower case, e.g., x. We use boldface upper case letters to denote random vectors, e.g., $\boldsymbol{X}$, and boldface lower case letters for their realizations, e.g., $\boldsymbol{x}$. Upper case letters of two special fonts are used to denote deterministic matrices (e.g., Y) and random matrices (e.g., $\mathbb{Y}$). The symbol $\mathbb{N}$ denotes the set of natural numbers, and $\mathbb{R}_+$ denotes the set of nonnegative real numbers. The superscripts ^{T} and ^{H} stand for transposition and Hermitian transposition, respectively, and $\bar{\cdot}$ stands for the complex conjugate. We use $\mathrm{tr}(\mathsf{A})$ and $\det(\mathsf{A})$ to denote the trace and determinant of the matrix A, respectively, and use $\|A\|_{\mathsf{F}} \triangleq \sqrt{\mathrm{tr}(\mathsf{A}\mathsf{A}^{\mathrm{H}})}$ to designate the Frobenius norm of A. For an infinite-dimensional complex vector $\boldsymbol{x} \in \mathbb{C}^\infty$, we use $\|\boldsymbol{x}\|_p$ to denote the ℓ_p-norm of $\boldsymbol{x}$, i.e., $\|\boldsymbol{x}\|_p \triangleq \left(\sum_{i=1}^{\infty} |x_i|^p\right)^{1/p}$. The ℓ_∞-norm of $\boldsymbol{x}$ is defined as $\|\boldsymbol{x}\|_\infty \triangleq \sup_i |x_i|$. We use $\boldsymbol{e}_j$ to denote the infinite dimensional vector that has 1 in the jth entry and 0 elsewhere, and use I_a to denote the identity matrix of size $a \times a$. The distribution of a circularly symmetric Gaussian random vector with covariance matrix A is denoted by $\mathcal{CN}(\mathbf{0}, \mathsf{A})$. We use $\mathrm{Exp}(\mu)$ to denote the exponential distribution with mean μ, and use $\mathrm{Gamma}(a, b)$ to denote the Gamma distribution with shape parameter a and scale parameter b [24, Ch. 17]. For two functions f and g, we use $f \star g$ to denote the convolution of f and g. Furthermore, the notation $f(x) = \mathcal{O}(g(x))$, $x \to \infty$, means that $\limsup_{x\to\infty} \left|f(x)/g(x)\right| < \infty$, and $f(x) = o(g(x))$, $x \to \infty$, means that $\lim_{x\to\infty} \left|f(x)/g(x)\right| = 0$. For two measures μ and ν, we write $\mu \ll \nu$ if μ is absolutely continuous [25, p. 88] with respect to ν. Finally, $|\cdot|^+ \triangleq \max\{0, \cdot\}$.

Next, we introduce two definitions related to the performance of optimal hypothesis testing. Given two probability distributions P and Q on a common measurable space $\mathcal{W}$, we define a randomized test between P and Q as a random transformation $P_{Z\,|\,W} : \mathcal{W} \to \{0, 1\}$ where 0 indicates that the test chooses Q. We shall need the following performance metric for the test between P and Q:

$$\beta_\alpha(P, Q) \triangleq \min_{P_{Z|W}:\int P_{Z\,|\,W}(1\,|\,w)P(dw)\geq\alpha} \int P_{Z\,|\,W}(1\,|\,w)Q(dw) \tag{8}$$

where the minimum is over all probability distributions $P_{Z\,|\,W}$ satisfying

$$\int P_{Z\,|\,W}(1\,|\,w)P(dw) \geq \alpha. \tag{9}$$

The minimum in (8) is guaranteed to be achieved by the Neyman-Pearson lemma [26]. For an arbitrary set $\mathcal{F}$, we define the following performance metric for the composite hypothesis testing between Q_Y and the collection $\{P_{Y|X=x}\}_{x\in\mathcal{F}}$:

$$\kappa_\tau(\mathcal{F}, Q_Y) \triangleq \inf \int P_{Z|Y}(1|y)Q_Y(dy). \tag{10}$$

Here, the infimum is over all conditional probability distributions $P_{Z|Y} : \mathcal{W} \to \{0, 1\}$ satisfying

$$\inf_{x\in\mathcal{F}} \int P_{Z|Y}(1|y)P_{Y|X=x}(dy) \geq \tau. \tag{11}$$

II. Problem Formulation

A. Channel Model and Codes

We consider a MIMO Rayleigh block-fading channel with m_{t} transmit antennas and m_{r} receive antennas that stays constant over a block of n_{c} channel uses (coherence interval)

and changes independently from block to block. The channel input-output relation within the ith coherence interval is given by

$$\mathbb{V}_i = \mathsf{U}_i \mathbb{H}_i + \mathbb{Z}_i. \tag{12}$$

Here, $\mathsf{U}_i \in \mathbb{C}^{n_\mathrm{c} \times m_\mathrm{t}}$ and $\mathbb{V}_i \in \mathbb{C}^{n_\mathrm{c} \times m_\mathrm{r}}$ are the transmitted and received signals, respectively, expressed in matrix form; $\mathbb{H}_i \in \mathbb{C}^{m_\mathrm{t} \times m_\mathrm{r}}$ is the channel matrix, which is assumed to have i.i.d. $\mathcal{CN}(0,1)$ entries; $\mathbb{Z}_i \in \mathbb{C}^{n_\mathrm{c} \times m_\mathrm{r}}$ is the additive noise matrix, also with i.i.d. $\mathcal{CN}(0, N_0)$ entries. We assume that $\{\mathbb{H}_i\}$ and $\{\mathbb{Z}_i\}$ are mutually independent, and take on independent realizations over successive coherence intervals (block-memoryless assumption). In the remainder of the paper, we shall set $N_0 = 1$, for notational convenience.

We are interested in the scenario where the blocklength is unlimited, and we aim at characterizing the minimum energy required to transmit k information bits over the channel (12) with a given reliability. We shall use U^∞ and $\mathbb{V}^\infty$ to denote the infinite sequences $\{\mathsf{U}_i\}$ and $\{\mathbb{V}_i\}$, respectively. At times, we shall interpret U^∞ as the infinite-dimensional matrix obtained by stacking the matrices $\{\mathsf{U}_i\}$, $i \in \mathbb{N}$, on top of each other. In this case, the matrix U^∞ has m_t columns and infinitely many rows, and its tth column vector represents the signal sent from the tth transmit antenna. The energy of the input matrix U^∞ is measured as follows

$$\left\|\mathsf{U}^\infty\right\|_\mathsf{F}^2 = \sum_{i=1}^{\infty} \|\mathsf{U}_i\|_\mathsf{F}^2. \tag{13}$$

Furthermore, we denote the set of all input matrices U^∞ by $\mathcal{A}$ and the set of all output matrices V^∞ by $\mathcal{B}$. Finally, we let $\mathcal{H}$ be the set of channel matrices H^∞.

Next, we define channel codes for the channel (12) for both the no-CSI and the perfect-CSIR case.

Definition 1: An (E, M, ϵ)-code for the channel (12) for the no-CSI case consists of a set of codewords $\{\mathsf{C}_1, \ldots, \mathsf{C}_M\} \in \mathcal{A}^M$ satisfying the energy constraint

$$\left\|\mathsf{C}_j\right\|_\mathsf{F}^2 \le E, \quad j \in \{1, \ldots, M\} \tag{14}$$

and a decoder $g : \mathcal{B} \to \{1, \ldots, M\}$ satisfying the maximum error probability constraint

$$\max_{j \in \{1,\ldots,M\}} \mathbb{P}[g(\mathbb{V}^\infty) \neq j \mid \mathbb{U}^\infty = \mathsf{C}_j] \le \epsilon. \tag{15}$$

Here, $\mathbb{V}^\infty$ is the output induced by the codeword $\mathbb{U}^\infty = \mathsf{C}_j$ according to (12). The maximum number of messages that can be transmitted with energy E and maximum error probability ϵ is

$$M^*(E, \epsilon) \triangleq \max\left\{M : \exists\, (E, M, \epsilon)\text{-code}\right\}. \tag{16}$$

Similarly, the minimum energy per bit is defined as

$$E_\mathrm{b}^*(k, \epsilon) \triangleq \frac{1}{k} \inf\left\{E : \exists\, (E, 2^k, \epsilon)\text{-code}\right\}. \tag{17}$$

Definition 2: An (E, M, ϵ)-code for the channel (12) for the perfect-CSIR case consists of a set of codewords $\{\mathsf{C}_1, \ldots, \mathsf{C}_M\} \in \mathcal{A}^M$ satisfying the energy constraint (14), and a decoder $g : \mathcal{B} \times \mathcal{H} \to \{1, \ldots, M\}$ satisfying the maximum error probability constraint

$$\max_{j \in \{1,\ldots,M\}} \mathbb{P}[g(\mathbb{V}^\infty, \mathbb{H}^\infty) \neq j \mid \mathbb{U}^\infty = \mathsf{C}_j] \le \epsilon. \tag{18}$$

The maximum number of messages that can be transmitted with energy E and maximum error probability ϵ for the perfect-CSIR case is defined as in (16).

As we shall show in the next section, one can derive tight bounds on $M^*(E, \epsilon)$ (for both the no-CSI and the perfect-CSIR case) by focusing exclusively on the memoryless single-input multiple-output (SIMO) scenario $n_\mathrm{c} = m_\mathrm{t} = 1$. Therefore, we shall next develop a specific notation to address this setup. In the SIMO case, the input-output relation reduces to

$$V_{r,i} = H_{r,i} u_i + Z_{r,i}, \quad r \in \{1, \ldots, m_\mathrm{r}\}, \quad i \in \mathbb{N}. \tag{19}$$

Here, $V_{r,i} \in \mathbb{C}$ denotes the received symbol at the rth receive antenna on the ith channel use, and $H_{r,i}$ and $Z_{r,i}$ denote the fading coefficient and the additive noise, respectively. We shall set $\boldsymbol{u} \triangleq [u_1, u_2, \ldots]$ and $\boldsymbol{V}_r \triangleq [V_{r,1}, V_{r,2}, \ldots]$.

B. An Equivalent Channel Model for the No-CSI case

Focusing on the no-CSI case, we define next a channel model that is equivalent to (19). Observe that, given $\boldsymbol{U} = \boldsymbol{u}$, the output vectors $\boldsymbol{V}_1, \ldots, \boldsymbol{V}_{m_\mathrm{r}}$ are i.i.d. Gaussian, i.e.,

$$P_{\boldsymbol{V}_r \mid \boldsymbol{U} = \boldsymbol{u}} = \prod_{i=1}^{\infty} \mathcal{CN}(0, (1 + |u_i|^2)), \quad r \in \{1, \ldots, m_\mathrm{r}\}. \tag{20}$$

Since the $\{\boldsymbol{V}_r\}$ depend on the input symbols $\{u_i\}$ only through their squared magnitude $\{|u_i|^2\}$, we can reduce without loss of generality the input space to $\mathbb{R}_+^\infty$. We also note that, given $\boldsymbol{U} = \boldsymbol{u}$, the joint conditional probability distribution of the random variables $\{V_{r,i}\}$ in (19) does not change if we multiply $\{V_{r,i}\}$ with arbitrary deterministic phases. This means that the $\{|V_{r,i}|^2\}$ are a sufficient statistics for the detection of $\boldsymbol{u}$ from $\{\boldsymbol{V}_r\}$. Letting $x_i \triangleq |u_i|^2$ and $Y_{r,i} \triangleq |V_{r,i}|^2$, $r \in \{1, \ldots, m_\mathrm{r}\}$, $i \in \mathbb{N}$, we obtain the following input-output relation, which is equivalent to (19):

$$Y_{r,i} = (1 + x_i) S_{r,i}, \quad r \in \{1, \ldots, m_\mathrm{r}\}, \quad i \in \mathbb{N}. \tag{21}$$

Here, the input x_i and the output $Y_{r,i}$ are nonnegative real numbers, and $\{S_{r,i}\}$ are i.i.d. Exp(1)-distributed. We shall denote the input of the channel (21) by $\boldsymbol{x} \triangleq [x_1, x_2, \ldots] \in \mathbb{R}_+^\infty$ and denote the output by the matrix $\mathbb{Y}$, whose entry on the rth row and the ith column is $Y_{r,i}$. Since $\|\boldsymbol{x}\|_1 = \|\boldsymbol{u}\|_2^2$ and since $\|\boldsymbol{x}\|_\infty = \|\boldsymbol{u}\|_\infty^2$, we shall measure the energy and the peakiness of an input codeword $\boldsymbol{x}$ for the channel (21) by its ℓ_1-norm $\|\boldsymbol{x}\|_1$, and by its ℓ_∞-norm $\|\boldsymbol{x}\|_\infty$, respectively.

III. Minimum Energy Per Bit

We shall now characterize $M^*(E, \epsilon)$ for both the no-CSI and the perfect-CSIR case. The organization of this section is as follows. In Section III-A, we first present nonasymptotic achievability and converse bounds on $M^*(E, \epsilon)$ for general channels subject to a cost constraint. In Section III-B, we then particularize these bounds to the channel (12) for the no-CSI case. Both the converse and achievability bounds in Section III-B are derived by reducing the MIMO channel (12) to the SIMO channel (21). We then show in Section III-C that these bounds match asymptotically as $E \to \infty$ up to

second order, thus establishing (4). In Section III-D, we derive bounds on $M^*(n,\epsilon)$ for the perfect-CSIR case and prove the asymptotic expansion (7). Finally, the nonasymptotic bounds for both the no-CSI and the perfect-CSIR case are evaluated numerically in Section III-E.

A. General Nonasymptotic Bounds

We consider in this section general stationary memoryless channels $(\mathcal{X}, P_{Y|X}, \mathcal{Y})$ with input codewords subject to a cost constraint. As in [5], we use $b[x]$ to denote the cost of the symbol x in the input alphabet $\mathcal{X}$. We shall also assume that there exists a zero-cost symbol, which we label as "0". With a slight abuse of notation, we use E to denote the cost constraint imposed on a codeword. An (E, M, ϵ)-code for this general channel consists of a set of M codewords $\boldsymbol{c}_j = [c_{j,1}, c_{j,2}, \ldots]$, $j = 1, \ldots, M$ that satisfy the cost constraint

$$\sum_{i=1}^{\infty} b[c_{j,i}] \le E, \quad j = 1, \ldots, M \tag{22}$$

and has maximum error probability not exceeding ϵ. We next present two achievability bounds on $M^*(E,\epsilon)$ that are finite-energy generalizations of Verdú's lower bound [5, pp. 1023–1024] on the capacity per unit cost.[4]

Theorem 1: Consider a stationary memoryless channel $(\mathcal{X}, P_{Y|X}, \mathcal{Y})$ that has a zero-cost input symbol. For every $N \in \mathbb{N}$, every $0 < \epsilon < 1$, and every input symbol $x_0 \in \mathcal{X}$ satisfying $b[x_0] > 0$, there exists an (E, M, ϵ)-code for which $E = b[x_0]N$ and

$$M - 1 \ge \sup_{0<\tau<\epsilon} \frac{\tau}{\beta_{1-\epsilon+\tau}(P_{Y|X=x_0}^{\otimes N}, P_{Y|X=0}^{\otimes N})}. \tag{23}$$

Here, $\beta_{(\cdot)}(\cdot,\cdot)$ is given in (8), and

$$P_{Y|X=x}^{\otimes N} \triangleq \underbrace{P_{Y|X=x} \times \cdots \times P_{Y|X=x}}_{N \text{ times}} \tag{24}$$

for every $x \in \mathcal{X}$.

Proof: As in [5], we choose the codewords $\boldsymbol{c}_j \in \mathcal{X}^\infty$, $j = 1, \ldots, M$, as follows:

$$\boldsymbol{c}_j \triangleq [\underbrace{0, \ldots, 0}_{(j-1)N}, \underbrace{x_0, \ldots, x_0}_{N}, 0, \ldots]. \tag{25}$$

Fix an arbitrary $\tau \in (0,\epsilon)$. For a given received signal $\boldsymbol{Y} \in \mathcal{Y}^\infty$, the decoder runs M parallel binary hypothesis tests Z_j, $j = 1, \ldots, M$, between $P_{\boldsymbol{Y}\,|\,\boldsymbol{X}=\boldsymbol{0}}$ and $P_{\boldsymbol{Y}\,|\,\boldsymbol{X}=\boldsymbol{c}_j}$. Here, $Z_j = 1$ indicates that the test selects $P_{\boldsymbol{Y}\,|\,\boldsymbol{X}=\boldsymbol{c}_j}$. The tests $\{Z_j\}$, $j = 1, \ldots, M$, are chosen to satisfy

$$\mathbb{P}[Z_j = 1 \,|\, \boldsymbol{X} = \boldsymbol{c}_j] \ge 1 - \epsilon + \tau \tag{26}$$

$$\mathbb{P}[Z_j = 1 \,|\, \boldsymbol{X} = \boldsymbol{0}] = \beta_{1-\epsilon+\tau}(P_{\boldsymbol{Y}\,|\,\boldsymbol{X}=\boldsymbol{c}_j}, P_{\boldsymbol{Y}\,|\,\boldsymbol{X}=\boldsymbol{0}}). \tag{27}$$

The existence of tests that satisfy (26) and (27) is guaranteed by the Neyman-Pearson lemma [26]. The decoder outputs the index m if $Z_m = 1$ and $Z_j = 0$ for all $j \ne m$. It outputs 1 if no such index can be found.

[4]For stationary memoryless channels, the capacity per unit cost is given by $\lim_{\epsilon\to 0}\lim_{E\to\infty}(\log M^*(E,\epsilon))/E$.

By construction, the maximum probability of error of the code just defined is upper-bounded by

$$\epsilon \le \mathbb{P}[Z_1 = 0 \,|\, \boldsymbol{X} = \boldsymbol{c}_1] + (M-1)\mathbb{P}[Z_1 = 1 \,|\, \boldsymbol{X} = \boldsymbol{0}] \tag{28}$$

$$\le \epsilon - \tau + (M-1)\beta_{1-\epsilon+\tau}(P_{\boldsymbol{Y}\,|\,\boldsymbol{X}=\boldsymbol{c}_1}, P_{\boldsymbol{Y}\,|\,\boldsymbol{X}=\boldsymbol{0}}). \tag{29}$$

Here, (28) follows because for each test Z_j $(j \ne 1)$ satisfying (26) and (27),

$$\mathbb{P}[Z_j = 1 | \boldsymbol{X} = \boldsymbol{c}_1] = \mathbb{P}[Z_j = 1 | \boldsymbol{X} = \boldsymbol{0}] \tag{30}$$

$$= \mathbb{P}[Z_1 = 1 | \boldsymbol{X} = \boldsymbol{0}] \tag{31}$$

and (29) follows by (26) and (27). From (29), we conclude that

$$M - 1 \ge \frac{\tau}{\beta_{1-\epsilon+\tau}(P_{\boldsymbol{Y}\,|\,\boldsymbol{X}=\boldsymbol{c}_1}, P_{\boldsymbol{Y}\,|\,\boldsymbol{X}=\boldsymbol{0}})}. \tag{32}$$

The proof is completed by noting that

$$\beta_{1-\epsilon+\tau}(P_{\boldsymbol{Y}\,|\,\boldsymbol{X}=\boldsymbol{c}_1}, P_{\boldsymbol{Y}\,|\,\boldsymbol{X}=\boldsymbol{0}}) = \beta_{1-\epsilon+\tau}(P_{Y|X=x_0}^{\otimes N}, P_{Y|X=0}^{\otimes N}) \tag{33}$$

and by maximizing the RHS of (32) over $\tau \in (0,\epsilon)$. ■

The proof of Theorem 1 is based on the same binary hypothesis-testing decoder that is used in the proof of the $\kappa\beta$ bound [7, Th. 25]. In fact, if $P_{Y|X=x_0} \ll P_{Y|X=0}$, a slightly weakened version of (32), with $M-1$ replaced by M, follows directly from the $\kappa\beta$ bound [7, Th. 25] upon setting $Q_{\boldsymbol{Y}} = P_{\boldsymbol{Y}\,|\,\boldsymbol{X}=\boldsymbol{0}}$ and choosing the set $\mathcal{F}$ as

$$\mathcal{F} = \Big\{\boldsymbol{x} \in \mathcal{X}^\infty : \boldsymbol{x} = [\underbrace{0, \ldots, 0}_{(j-1)N}, \underbrace{x_0, \ldots, x_0}_{N}, 0, \ldots] \text{ for some } j \in \mathbb{N}\Big\}. \tag{34}$$

Since $\beta_{1-\epsilon+\tau}(P_{\boldsymbol{Y}\,|\,\boldsymbol{X}=\boldsymbol{x}}, Q_{\boldsymbol{Y}})$ takes the same value for all $\boldsymbol{x} \in \mathcal{F}$, to establish this looser bound it is sufficient to show that (proof omitted)

$$\kappa_\tau(\mathcal{F}, Q_{\boldsymbol{Y}}) = \tau \tag{35}$$

where $\kappa_{(\cdot)}(\cdot,\cdot)$ is given in (10).

Using the same codebook as in Theorem 1 together with a maximum likelihood decoder, we obtain a different achievability bound, which is stated in the following theorem.

Theorem 2: Consider a stationary memoryless channel $(\mathcal{X}, P_{Y|X}, \mathcal{Y})$ that has a zero-cost input symbol. For every $N \in \mathbb{N}$, every $0 < \epsilon < 1$, and every input symbol $x_0 \in \mathcal{X}$ satisfying $b[x_0] > 0$, there exists an (E, M, ϵ)-code for which $E = b[x_0]N$ and

$$\epsilon \le \mathbb{E}\Big[\min\Big\{1, (M-1)\mathbb{P}\Big[\imath_N(x_0; Y^N) \le \imath_N(x_0; \hat{Y}^N) \,|\, Y^N\Big]\Big\}\Big]. \tag{36}$$

Here, $P_{Y^N\hat{Y}^N}(y^N, \hat{y}^N) \triangleq P_{Y|X=x_0}^{\otimes N}(y^N) P_{Y|X=0}^{\otimes N}(\hat{y}^N)$ and

$$\imath_N(x; y^N) \triangleq \log \frac{dP_{Y|X=x}^{\otimes N}}{dP_{Y|X=0}^{\otimes N}}(y^N) \tag{37}$$

with $P_{Y|X=x}^{\otimes N}$, $x \in \mathcal{X}$, defined in (24).

Remark 1: For AWGN channels with cost function $b[x] = x^2$, one can recover [8, Eq. (15)] from (36) by setting $N = 1$ and $x_0 = \sqrt{E}$.

Proof: We use the same codebook as in Theorem 1, together with a maximum likelihood decoder. Let

$$\imath(\boldsymbol{x}, \boldsymbol{y}) \triangleq \log \frac{d P_{\boldsymbol{Y} \mid \boldsymbol{X}=\boldsymbol{x}}}{d P_{\boldsymbol{Y} \mid \boldsymbol{X}=\boldsymbol{0}}}(\boldsymbol{y}). \tag{38}$$

Let $Y^N = [Y_1, \ldots, Y_N]$ denote the vector containing the first N entries of $\boldsymbol{Y}$ and let $\hat{Y}^N \sim P_{Y|X=0}^{\otimes N}$ be independent of $\boldsymbol{Y}$. The probability of error ϵ is upper-bounded as follows:

$$\epsilon \leq P_{\boldsymbol{Y} \mid \boldsymbol{X}=\boldsymbol{c}_1}\left[\bigcup_{j=2}^{M}\left\{\imath(\boldsymbol{c}_1, \boldsymbol{Y}) \leq \imath(\boldsymbol{c}_j, \boldsymbol{Y})\right\}\right] \tag{39}$$

$$= \mathbb{E}\left[\mathbb{P}\left[\bigcup_{j=2}^{M}\left\{\imath(\boldsymbol{c}_1, \boldsymbol{Y}) \leq \imath(\boldsymbol{c}_j, \boldsymbol{Y})\right\}\middle| Y^N\right]\right] \tag{40}$$

$$\leq \mathbb{E}\left[\min\left\{1, (M-1)\mathbb{P}\left[\imath(\boldsymbol{c}_1, \boldsymbol{Y}) \leq \imath(\boldsymbol{c}_2, \boldsymbol{Y})\middle| Y^N\right]\right\}\right] \tag{41}$$

$$= \mathbb{E}\left[\min\left\{1, (M-1)\mathbb{P}\left[\imath_N(x_0; Y^N) \leq \imath_N(x_0; \hat{Y}^N) \mid Y^N\right]\right\}\right]. \tag{42}$$

Here, (39) follows because all codewords have the same error probability under maximum likelihood decoding; (41) follows by choosing the tighter bound between 1 and the union bound; (42) follows because $\boldsymbol{c}_1 = [\underbrace{x_0, \ldots, x_0}_{N}, \underbrace{0, \ldots, 0}_{N}, 0, \ldots]$ and $\boldsymbol{c}_2 = [\underbrace{0, \ldots, 0}_{N}, \underbrace{x_0, \ldots, x_0}_{N}, 0, \ldots]$, and because, under $P_{\boldsymbol{Y} \mid \boldsymbol{X}=\boldsymbol{c}_1}$, the sequence Y_{N+1}^{2N} has the same distribution as $\hat{Y}^N \sim P_{Y|X=0}^{\otimes N}$. Furthermore, Y_{N+1}^{2N} is independent of Y^N since the channel is stationary and memoryless. ■

On the converse side, we have the following result, which follows by applying the meta-converse theorem [7, Th. 31] with $Q_{\boldsymbol{Y}} = P_{\boldsymbol{Y} \mid \boldsymbol{X}=\boldsymbol{0}}$.

Theorem 3: Consider a channel $(\mathcal{X}, P_{Y|X}, \mathcal{Y})$ that has a zero-cost input symbol. Every (E, M, ϵ)-code with codewords satisfying the cost constraint (22) satisfies

$$M \leq \sup_{\boldsymbol{x}: \sum_{i=1}^{\infty} b[x_i] \leq E} \frac{1}{\beta_{1-\epsilon}(P_{\boldsymbol{Y} \mid \boldsymbol{X}=\boldsymbol{x}}, P_{\boldsymbol{Y} \mid \boldsymbol{X}=\boldsymbol{0}})}. \tag{43}$$

The bound (43) is in general not computable because it involves an optimization over infinite-dimensional codewords. As we shall see in the next section, in the MIMO Rayleigh block-fading case it is possible to reduce this infinite-dimensional optimization problem to a three-dimensional one, which can be solved numerically.

We would like to remark that the general bounds developed in this section apply to both the no-CSI case and the perfect-CSIR case. For the perfect-CSIR case, we view the pair $(\mathbb{V}, \mathbb{H})$ as the channel output, and identify the channel law with $P_{\mathbb{V},\mathbb{H}|\mathbb{U}} = P_{\mathbb{H}} P_{\mathbb{V} \mid \mathbb{H},\mathbb{U}}$. For the no-CSI case, we view $\mathbb{V}$ as the output and identify the channel law with $P_{\mathbb{V}|\mathbb{U}}$, which is obtained by averaging $P_{\mathbb{V} \mid \mathbb{H},\mathbb{U}}$ over the fading matrix $\mathbb{H}$. In both cases, the channel is stationary and memoryless.

B. Nonasymptotic Bounds: the No-CSI Case

Particularizing Theorems 1 and 2 to the channel (12) for the no-CSI case, we obtain the achievability bounds given below in Corollaries 4 and 5.

Corollary 4: For every $E > 0$ and every $0 < \epsilon < 1$, there exists an (E, M, ϵ)-code for the MIMO Rayleigh block-fading channel (12) for the case of no CSI satisfying

$$M - 1 \geq \sup_{0<\tau<\epsilon,\, N \in \mathbb{N}} \frac{\tau}{\mathbb{P}[G_N \geq (1 + E/N)\xi]} \tag{44}$$

where $G_N \sim \text{Gamma}(m_{\text{r}} N, 1)$ and ξ satisfies

$$\mathbb{P}[G_N \leq \xi] = \epsilon - \tau. \tag{45}$$

Proof: Every code for the memoryless SIMO Rayleigh-fading channel ($m_{\text{t}} = n_{\text{c}} = 1$) can be used on a MIMO Rayleigh block-fading channel with $m_{\text{t}} > 1$ and $n_{\text{c}} > 1$. Indeed, it is sufficient to switch off all transmit antennas but one, and to limit transmissions to the first channel use in each coherence interval. Therefore, it is sufficient to prove that (44) is achievable for the memoryless SIMO Rayleigh-fading channel (21). In the SIMO case, we have (see (21))

$$\log \frac{d P_{\boldsymbol{Y}|X=x_0}^{\otimes N}}{d P_{\boldsymbol{Y}|X=0}^{\otimes N}}\left(\boldsymbol{y}^N\right) = \frac{x_0 \log e}{1 + x_0} \sum_{r=1}^{m_{\text{r}}} \sum_{i=1}^{N} y_{r,i} - m_{\text{r}} N \log(1 + x_0). \tag{46}$$

Let $x_0 = E/N$ for some $N \in \mathbb{N}$. Then, under $P_{\boldsymbol{Y}|X=x_0}^{\otimes N}$, the random variable $\log \frac{d P_{\boldsymbol{Y}|X=x_0}^{\otimes N}}{d P_{\boldsymbol{Y}|X=0}^{\otimes N}}(\boldsymbol{Y}^N)$ has the same distribution as

$$\frac{E}{N} G_N \log e - m_{\text{r}} N \log(1 + E/N) \tag{47}$$

where $G_N \sim \text{Gamma}(m_{\text{r}} N, 1)$, and, under $P_{\boldsymbol{Y}|X=0}^{\otimes N}$, it has the same distribution as

$$\frac{E}{N} \frac{G_N \log e}{1 + E/N} - m_{\text{r}} N \log(1 + E/N). \tag{48}$$

The proof of (44) is concluded by using (47) and (48) in (23) together with the Neyman-Pearson lemma [26], and by optimizing over $N \in \mathbb{N}$. ■

Corollary 5: For every $M > 0$ and every $0 < \epsilon < 1$, there exists an (E, M, ϵ)-code for the MIMO Rayleigh block-fading channel (12) for the case of no CSI satisfying

$$\epsilon \leq \min_{N \in \mathbb{N}} \mathbb{E}\left[\min\left\{1, (M-1)\mathbb{P}\left[\bar{G}_N \geq (1 + E/N) G_N \middle| G_N\right]\right\}\right] \tag{49}$$

where G_N and $\bar{G}_N$ are i.i.d. $\text{Gamma}(m_{\text{r}} N, 1)$ random variables.

Proof: We proceed first as in the proof of Corollary 4. Then, we use (47) and (48) in (36). ■

Numerical evidence (provided in Section III-E) suggests that (49) is tighter than (44). However, (44) is more suitable for asymptotic analyses.

We now provide a converse bound, which is based on Theorem 3.

Theorem 6: Let $\{S_i\}$ be i.i.d. Exp(1)-distributed random variables. Every (E, M, ϵ)-code for the MIMO Rayleigh block-

fading channel (12) for the case of no CSI satisfies

$$\frac{1}{M} \geq \sup_{\eta \in \mathbb{R}} \frac{\inf_{\boldsymbol{x}} \mathbb{P}\left[\sum_{i=1}^{\infty}\left(x_i S_i \log e - \log(1+x_i)\right) \leq \eta\right] - \epsilon}{\exp(\eta)}. \tag{50}$$

The infimum in (50) is over all $\boldsymbol{x} \in \mathbb{R}_+^\infty$ taking one of the following two forms:

$$\boldsymbol{x} = [q_3, \underbrace{q_2, \ldots, q_2}_{N}, q_1, 0, 0, \ldots] \tag{51}$$

or

$$\boldsymbol{x} = [\underbrace{\tilde{q}_2, \ldots, \tilde{q}_2}_{\widetilde{N}_2}, \underbrace{\tilde{q}_1, \ldots, \tilde{q}_1}_{\widetilde{N}_1}, 0, 0, \ldots]. \tag{52}$$

Here, $N \in \mathbb{N}$ and $0 < q_1 < q_2 < q_3$ satisfy $q_1 + Nq_2 + q_3 = m_{\mathrm{r}} E$. Furthermore, $\widetilde{N}_1, \widetilde{N}_2 \in \mathbb{N}$ and $0 \leq \tilde{q}_1 \leq \tilde{q}_2$ satisfy $\widetilde{N}_1 \tilde{q}_1 + \widetilde{N}_2 \tilde{q}_2 = m_{\mathrm{r}} E$.

Remark 2: The optimization over infinite-dimensional codewords in the converse bound (43) is reduced in (50) to a three-dimensional optimization problem. This makes (50) numerically computable. In words, the conditions in (51) and (52) imply that i) the entries of $\boldsymbol{x}$ can take at most three distinct nonzero values, and that ii) if the entries of $\boldsymbol{x}$ take exactly three distinct nonzero values, then both the largest and the smallest nonzero entries must appear only once.

Proof: Without loss of generality, we can assume that each codeword matrix C_j satisfies the energy constraint (14) with equality. Indeed, for an arbitrary code $\mathcal{C}$, we can construct a new code $\mathcal{C}'$ by appending to each codeword matrix C_j in $\mathcal{C}$ an extra $n_{\mathrm{c}} \times m_{\mathrm{t}}$ block of energy $E - \|\mathsf{C}_j\|_{\mathsf{F}}^2$ (recall that the number of transmitted symbols is unlimited). The resulting code $\mathcal{C}'$ has the same number of codewords as $\mathcal{C}$ and each codeword of $\mathcal{C}'$ satisfies (14) with equality. Moreover, the error probability of $\mathcal{C}'$ can not exceed that of $\mathcal{C}$.

We continue the proof of (50) by using Theorem 3, which implies

$$\frac{1}{M} \geq \inf_{\mathsf{U}^\infty \in \mathcal{A}:\ \|\mathsf{U}^\infty\|_{\mathsf{F}}^2 = E} \beta_{1-\epsilon}(P_{\mathbb{V}^\infty \mid \mathbb{U}^\infty = \mathsf{U}^\infty}, P_{\mathbb{V}^\infty \mid \mathbb{U}^\infty = \mathbf{0}}). \tag{53}$$

For a given $\mathsf{U}^\infty = \{\mathsf{U}_i\}$, let $\widetilde{\mathsf{U}}^\infty = \{\widetilde{\mathsf{U}}_i\}$ where $\widetilde{\mathsf{U}}_i \in \mathbb{R}_+^{n_{\mathrm{c}} \times m_{\mathrm{t}}}$ is a diagonal matrix whose diagonal elements are the singular values of U_i. We shall next show that

$$\begin{aligned}\beta_{1-\epsilon}&(P_{\mathbb{V}^\infty \mid \mathbb{U}^\infty = \mathsf{U}^\infty}, P_{\mathbb{V}^\infty \mid \mathbb{U}^\infty = \mathbf{0}}) \\ &= \beta_{1-\epsilon}(P_{\mathbb{V}^\infty \mid \mathbb{U}^\infty = \widetilde{\mathsf{U}}^\infty}, P_{\mathbb{V}^\infty \mid \mathbb{U}^\infty = \mathbf{0}}).\end{aligned} \tag{54}$$

This implies that to evaluate the RHS of (53), it suffices to focus on diagonal matrices $\{\mathsf{U}_i\}$. Note also that when the input matrices $\{\mathsf{U}_i\}$ are diagonal, the $m_{\mathrm{t}} \times m_{\mathrm{r}}$ MIMO block-fading channel (12) decomposes into $\min\{m_{\mathrm{t}}, n_{\mathrm{c}}\}$ noninteracting memoryless SIMO fading channels with m_{r} receive antennas. Therefore, exploiting the equivalence between (19) and (21), we conclude that the RHS of (53) coincides with

$$\inf_{\boldsymbol{x} \in \mathbb{R}_+^\infty : \|\boldsymbol{x}\|_1 = E} \beta_{1-\epsilon}(P_{\mathbb{Y} \mid \boldsymbol{X} = \boldsymbol{x}}, P_{\mathbb{Y} \mid \boldsymbol{X} = \mathbf{0}}) \tag{55}$$

where $P_{\mathbb{Y} \mid \boldsymbol{X}}$ is the conditional distribution of the output of the channel (21) given the input.

To prove (54), we note that given $\mathbb{U}_i = \mathsf{U}_i$, the column vectors of the output matrix $\mathbb{V}_i$ are i.i.d. $\mathcal{CN}\big(\mathbf{0}, \mathsf{I}_{n_{\mathrm{c}}} + \mathsf{U}_i \mathsf{U}_i^{\mathrm{H}}\big)$-distributed. Therefore, the probability distribution $P_{\mathbb{V}_i \mid \mathbb{U}_i = \mathsf{U}_i}$ depends on U_i only through $\mathsf{U}_i \mathsf{U}_i^{\mathrm{H}}$. In particular, it is invariant to right-multiplication of U_i by an arbitrary $m_{\mathrm{t}} \times m_{\mathrm{t}}$ unitary matrix G. Furthermore, since the noise matrix $\mathbb{Z}_i$ is isotropically distributed [27, Definition 6.21], for every $n_{\mathrm{c}} \times n_{\mathrm{c}}$ unitary matrix $\widetilde{\mathsf{G}}$ and every $\mathsf{U} \in \mathbb{C}^{n_{\mathrm{c}} \times m_{\mathrm{t}}}$, the conditional distribution of $\mathbb{V}_i$ given $\mathbb{U}_i = \mathsf{U}$ coincides with that of $\widetilde{\mathsf{G}}^{\mathrm{H}} \mathbb{V}_i$ given $\mathbb{U}_i = \widetilde{\mathsf{G}}\mathsf{U}$. Therefore, for every $i \in \mathbb{N}$, and every unitary matrices G and $\widetilde{\mathsf{G}}$, we have

$$\begin{aligned}&\beta_{1-\epsilon}\big(P_{\mathbb{V}_i \mid \mathbb{U}_i = \mathsf{U}}, P_{\mathbb{V}_i \mid \mathbb{U}_i = \mathbf{0}}\big) \\ &\quad = \beta_{1-\epsilon}\Big(P_{\widetilde{\mathsf{G}}^{\mathrm{H}} \mathbb{V}_i \mid \mathbb{U}_i = \widetilde{\mathsf{G}}\mathsf{U}\mathsf{G}}, P_{\widetilde{\mathsf{G}}^{\mathrm{H}} \mathbb{V}_i \mid \mathbb{U}_i = \mathbf{0}}\Big) \qquad (56) \\ &\quad = \beta_{1-\epsilon}\Big(P_{\mathbb{V}_i \mid \mathbb{U}_i = \widetilde{\mathsf{G}}\mathsf{U}\mathsf{G}}, P_{\mathbb{V}_i \mid \mathbb{U}_i = \mathbf{0}}\Big). \qquad (57)\end{aligned}$$

Here, the second step follows because $\beta_{1-\epsilon}(\cdot, \cdot)$ stays unchanged under the change of variables $\mathsf{V}_i \mapsto \widetilde{\mathsf{G}}^{\mathrm{H}} \mathsf{V}_i$. Since G, $\widetilde{\mathsf{G}}$, and i are arbitrary, and since the channel $P_{\mathbb{V}^\infty \mid \mathbb{U}^\infty}$ is block-memoryless, (57) implies (54).

Next, we lower-bound $\beta_{1-\epsilon}(P_{\mathbb{Y} \mid \boldsymbol{X} = \boldsymbol{x}}, P_{\mathbb{Y} \mid \boldsymbol{X} = \mathbf{0}})$ in (55) using [7, Eq. (102)]. Specifically, we fix an arbitrary $\eta \in \mathbb{R}$ and obtain

$$\begin{aligned}&\beta_{1-\epsilon}(P_{\mathbb{Y} \mid \boldsymbol{X} = \boldsymbol{x}}, P_{\mathbb{Y} \mid \boldsymbol{X} = \mathbf{0}}) \\ &\quad \geq \exp(-\eta)\Big(P_{\mathbb{Y} \mid \boldsymbol{X} = \boldsymbol{x}}[\imath(\boldsymbol{x}, \mathbb{Y}) \leq \eta] - \epsilon\Big)\end{aligned} \tag{58}$$

where $\imath(\cdot, \cdot)$ was defined in (38). Under $P_{\mathbb{Y} \mid \boldsymbol{X} = \boldsymbol{x}}$, the random variable $\imath(\boldsymbol{x}, \mathbb{Y})$ has the same distribution as

$$\sum_{r=1}^{m_{\mathrm{r}}} \sum_{i=1}^{\infty} \left(x_i S_{r,i} \log e - \log(1+x_i)\right) \tag{59}$$

where $\{S_{r,i}\}$ are i.i.d. Exp(1)-distributed. Substituting (59) into (58), and then (58) into (53), we obtain

$$\frac{1}{M} \geq \frac{\inf_{\boldsymbol{x}} \mathbb{P}\left[\sum_{r=1}^{m_{\mathrm{r}}} \sum_{i=1}^{\infty}\left(x_i S_{r,i} \log e - \log(1+x_i)\right) \leq \eta\right] - \epsilon}{\exp(\eta)} \tag{60}$$

$$\geq \frac{\inf_{\boldsymbol{x}} \mathbb{P}\left[\sum_{i=1}^{\infty}\left(x_i S_i \log e - \log(1+x_i)\right) \leq \eta\right] - \epsilon}{\exp(\eta)}. \tag{61}$$

Here, the infimum in (60) is over all $\boldsymbol{x} \in \mathbb{R}_+^\infty$ satisfying $\|\boldsymbol{x}\|_1 = E$, the infimum in (61) is over all $\boldsymbol{x} \in \mathbb{R}_+^\infty$ satisfying $\|\boldsymbol{x}\|_1 = m_{\mathrm{r}} E$, and $\{S_i\}$ in (61) are again i.i.d. Exp(1)-distributed. The inequality (61) follows because the feasible region of the optimization problem in (60) is contained in the feasible region of the optimization problem in (61).

Lemma 7 below, which is proven in Appendix I, sheds light on the structure of the vectors $\boldsymbol{x}^*$ that minimize the RHS of (61).

Lemma 7: Let $\boldsymbol{x}^*$ be a minimizer of

$$\inf_{\boldsymbol{x} \in \mathbb{R}_+^\infty : \|\boldsymbol{x}\|_1 = m_{\mathrm{r}} E} \mathbb{P}\left[\sum_{i=1}^{\infty}\left(x_i S_i \log e - \log(1+x_i)\right) \leq \eta\right]. \tag{62}$$

Assume without loss of generality that the entries of $\boldsymbol{x}^*$ are in nonincreasing order. Then, $\boldsymbol{x}^*$ must be of the form given in (51) or in (52).

The proof of Theorem 6 is concluded by using Lemma 7 in (61) and by maximizing the RHS of (61) over η. ■

Remark 3: The proof of Lemma 7 relies on an elegant argument of Abbe *et al.* [22], used in the proof of Telatar's minimum outage probability conjecture for MISO Rayleigh-fading channels. Indeed, both [22] and Lemma 7 deal with the optimization of quantiles of a weighted convolution of exponential distributions.

C. Asymptotic Analysis

Evaluating the bounds in Corollary 4 and Theorem 6 in the limit $E \to \infty$, we obtain the asymptotic closed-form expansion for $M^*(E, \epsilon)$ provided in the following theorem.

Theorem 8: The maximum number of messages $M^*(E, \epsilon)$ that can be transmitted with energy E and error probability $\epsilon \in (0, 1/2)$ over the MIMO Rayleigh block-fading channel (12) for the case of no CSI admits the following expansion

$$\begin{aligned}&\log M^*(E, \epsilon)\\ &= m_{\mathrm{r}} E \log e - V_0 \cdot \left(m_{\mathrm{r}} E Q^{-1}(\epsilon)\right)^{2/3} \left(\log(m_{\mathrm{r}} E)\right)^{1/3}\\ &\quad + \mathcal{O}\left(\frac{E^{2/3} \log\log E}{(\log E)^{2/3}}\right), E \to \infty. \end{aligned} \tag{63}$$

Here, V_0 is given in (5).

Proof: See Appendix III. ■

The intuition behind (63) is as follows. It is well known that in the no-CSI case, to achieve the asymptotic limit -1.59 dB, it is necessary to use flash signalling [2]. If all codewords satisfy a peak-power constraint $\|\boldsymbol{x}\|_\infty \le A$ in addition to (14), then $\log M(E, \epsilon)/(m_{\mathrm{r}} E)$ converges as $E \to \infty$ to (see [13] and [14, Eq. (59)])

$$\log e - \frac{\log(1 + A)}{A}. \tag{64}$$

The second term in (64) can be interpreted as the penalty due to bounded peakiness, which vanishes as $A \to \infty$. When the energy E is finite, as in our setup, it turns out that for larg E

$$\frac{\log M(E, \epsilon)}{m_{\mathrm{r}} E} \approx \log e - \frac{\log(1 + A)}{A} - \sqrt{\frac{A}{m_{\mathrm{r}} E}} Q^{-1}(\epsilon) \log e. \tag{65}$$

The second term on the RHS of (65) captures the fact that codewords that satisfy (14) for a finite E are necessarily peak-power limited. The third term captures the penalty resulting from the stochastic variations of the fading and the noise processes, which cannot be averaged out for finite E. This penalty increases with the peak power. Coarsely speaking, peakier codewords result in less channel averaging. To summarize, peakiness in the codewords reduces the second term on the RHS of (65) but increases the third term. The optimal peak power A^* that minimizes the sum of these two penalty terms turns out to be

$$A^* = \left(\frac{3}{2} Q^{-1}(\epsilon) \log e\right)^{-\frac{2}{3}} (m_{\mathrm{r}} E)^{\frac{1}{3}} \log^{\frac{2}{3}}(m_{\mathrm{r}} E) + o(E^{\frac{1}{3}}). \tag{66}$$

Substituting (66) into (65) we obtain (63). See Appendix III for a rigorous proof.

D. The Perfect-CSIR Case

In this section, we provide achievability and converse bounds on $M^*(E, \epsilon)$ for the case of perfect CSIR. To state our achievability bound, it is convenient to introduce the following complex AWGN channel

$$Y_i = X_i + Z_i, \quad i \in \mathbb{N}. \tag{67}$$

Here, $\{Z_i\}$ are i.i.d. $\mathcal{CN}(0, 1)$-distributed random variables. Theorem 9 below allows us to relate the performance of optimal codes for the AWGN channel (67) to the performance of optimal codes for the MIMO Rayleigh block-fading channel (12).

Theorem 9: Consider an arbitrary $(m_{\mathrm{r}} E, M, \epsilon)$-code for the AWGN channel (67). There exists a sequence of (E, M, ϵ_N)-codes for the MIMO Rayleigh block-fading channel (12) with perfect CSIR, for which $\lim_{N\to\infty} \epsilon_N \le \epsilon$.

Remark 4: Theorem 9 holds also if the fading is not Rayleigh, provided that the entries $\{H_{i,j,k}\}$ of $\mathbb{H}_i$ are i.i.d. and satisfy $\mathbb{E}\left[|H_{i,j,k}|^2\right] = 1$.

Proof: As in the proof of Corollary 4, it is sufficient to consider the case $m_{\mathrm{t}} = n_{\mathrm{c}} = 1$. Take an arbitrary $(m_{\mathrm{r}} E, M, \epsilon)$-code for the AWGN channel. We assume without loss of generality that only the first M entries of each codeword are nonzeros. This is because, for the AWGN channel, the error probability under maximal likelihood decoding depends only on the Euclidean distance between codewords, and because we can embed the M codewords in an M-dimensional space without changing their Euclidean distances.

Next, we transform the SIMO memoryless fading channel (with perfect CSIR) into an AWGN channel as follows. Fix an arbitrary $N \in \mathbb{N}$; for every codeword $\boldsymbol{u} = [u_1, \ldots, u_M, 0, \ldots]$ for the AWGN channel, we generate the following codeword $\tilde{\boldsymbol{u}}$ for the memoryless SIMO fading channel (19)

$$\tilde{\boldsymbol{u}} \triangleq \frac{1}{\sqrt{m_{\mathrm{r}} N}} [\underbrace{u_1, \ldots, u_1}_{N}, \underbrace{u_2, \ldots, u_2}_{N}, \ldots]. \tag{68}$$

By construction, $\|\tilde{\boldsymbol{u}}\|_2^2 = \|\boldsymbol{u}\|_2^2 / m_{\mathrm{r}}$. For a given channel output $\{V_{r,i}\}$ (see (19)), the receiver performs coherent combining across the m_{r} receive antennas and the length-N repetition block:

$$\widetilde{V}_j \triangleq \frac{1}{\sqrt{m_{\mathrm{r}} N}} \sum_{r=1}^{m_{\mathrm{r}}} \sum_{i=1}^{N} \bar{H}_{r,(j-1)N+i} V_{r,(j-1)N+i} \tag{69}$$

$$\begin{aligned}&= \frac{u_j}{m_{\mathrm{r}} N} \sum_{r=1}^{m_{\mathrm{r}}} \sum_{i=1}^{N} |H_{r,(j-1)N+i}|^2\\ &\quad + \frac{1}{\sqrt{m_{\mathrm{r}} N}} \sum_{r=1}^{m_{\mathrm{r}}} \sum_{i=1}^{N} \bar{H}_{r,(j-1)N+i} Z_{r,(j-1)N+i},\\ &\qquad j = 1, \ldots, M. \end{aligned} \tag{70}$$

If we let $N \to \infty$, the first term in (70) converges in distribution to u_j by the law of large numbers, and the second term converges in distribution to $Z_j \sim \mathcal{CN}(0, 1)$ by the

central limit theorem. Therefore, $\widetilde{V}_j$ converges in distribution to $u_j + Z_j$. Thus, $P_{\widetilde{V}^M|U^M=u^M}$ converges in distribution to an AWGN channel law $P^{\text{AWGN}}_{V^M|U^M=u^M} = \mathcal{CN}(u^M, \mathrm{I}_M)$ as $N \to \infty$.

We next evaluate the error probability ϵ_N of the code that we constructed above. Let $\mathcal{D}_j$ denote the decoding region for message j, $1 \le j \le M$, and let $\text{Int}(\mathcal{D}_j)$ denote the interior of $\mathcal{D}_j$. It follows that for every $1 \le j \le M$

$$\begin{aligned}\lim_{N\to\infty} 1-\epsilon_N &= \lim_{N\to\infty} P_{\widetilde{V}^M|U^M=\boldsymbol{u}_j}[\mathcal{D}_j] &(71)\\ &\ge \lim_{N\to\infty} P_{\widetilde{V}^M|U^M=\boldsymbol{u}_j}[\text{Int}(\mathcal{D}_j)] &(72)\\ &= P^{\text{AWGN}}_{V^M|U^M=\boldsymbol{u}_j}[\text{Int}(\mathcal{D}_j)] &(73)\\ &= P^{\text{AWGN}}_{V^M|U^M=\boldsymbol{u}_j}[\mathcal{D}_j] &(74)\\ &\ge 1-\epsilon. &(75)\end{aligned}$$

Here, (73) follows because $P_{\widetilde{V}^M|U^M=\boldsymbol{u}_j}$ converges in distribution to $P^{\text{AWGN}}_{V^M|U^M=\boldsymbol{u}_j}$ and because $\text{Int}(\mathcal{D}_j)$ is open; (74) follows because the boundary of the maximum likelihood decoding region $\mathcal{D}_j$ has zero probability measure under $P^{\text{AWGN}}_{V^M|U^M=\boldsymbol{u}_j}$. ■

Note that the proof of Theorem 9 above requires perfect CSIR. The approach just described does not necessarily work if only partial CSI is available at the receiver. For example, consider the following partial-CSI model [28]

$$V_i = (\bar{H}_i + \hat{H}_i)U_i + Z_i, \quad i \in \mathbb{N} \tag{76}$$

where $\bar{H}_i \sim \mathcal{CN}(0, \rho)$, $\rho \in (0, 1)$, $\hat{H}_i \sim \mathcal{CN}(0, 1-\rho)$, and $\{\bar{H}_i\}$ and $\{\hat{H}_i\}$ are independent. We assume that the receiver has perfect knowledge of $\{\bar{H}_i\}$, but knows only the statistics of $\{\hat{H}_i\}$. The random variables $\{\bar{H}_i\}$ and $\{\hat{H}_i\}$ can be viewed as the estimation of the channel coefficients and the estimation errors, respectively [28]. Following steps similar to the ones in the proof of [2, Th. 7], one can show that flash-signalling is necessary to achieve the -1.59 dB limit. Hence, spreading the energy as it is done in the proof of Theorem 9 is not first-order optimal.

For the case where perfect CSI is available at both the transmitter and the receiver, and where the fading distribution has infinite support (e.g., Rayleigh distribution), it is well known that the minimum energy per bit $E^*_{\text{b}}(k, \epsilon)$ converges to 0 in the limit $k \to \infty$ and $\epsilon \to 0$ [2, p. 1325]. Using the approach used in the proof of Theorem 9, one can show that $E^*_{\text{b}}(k, \epsilon) = 0$ for *every* k and $\epsilon > 0$. Indeed, since both the transmitter and the receiver have perfect CSI, they can agree to use the channel only if the fading gain $|H|^2$ is above a threshold Γ. By doing so, we have transformed the original fading channel into a channel with a fading distribution $\tilde{P}_H$ that satisfies $\mathbb{E}_{\tilde{P}_H}[|H|^2] \ge \Gamma$. Proceeding as in the proof of Theorem 9, we conclude that every $(E, 2^k, \epsilon)$ code for the AWGN channel can be converted into an $(E/\mathbb{E}_{\tilde{P}_H}[|H|^2], 2^k, \epsilon)$ code for the fading channel with distribution $\tilde{P}_H$. Since Γ can be taken arbitrarily large, we conclude that the minimum energy per bit $E^*_{\text{b}}(k, \epsilon)$ is 0.

Theorem 9 implies that the asymptotic expansion (2) with E replaced by $m_{\text{r}}E$ is achievable in the perfect-CSIR case. Theorem 10 below establishes that, for $0 < \epsilon < 1/2$, the converse is also true.

Theorem 10: The maximum number of messages $M^*(E, \epsilon)$ that can be transmitted with energy E and error probability $0 < \epsilon < 1/2$ over the MIMO Rayleigh block-fading channel (12) for the case of perfect CSIR satisfies

$$\log M^*(E, \epsilon) = m_{\text{r}}E \log e - \sqrt{2m_{\text{r}}E}\,Q^{-1}(\epsilon)\log e + \frac{1}{2}\log(m_{\text{r}}E) + \mathcal{O}\Big(\sqrt{\log E}\Big) \tag{77}$$

as $E \to \infty$.

Proof: See Appendix IV. ■

Unlike Theorem 9, the converse part of Theorem 10 relies on the Gaussianity of the fading coefficients and does not necessarily hold for other fading distributions. Indeed, consider a single-input single-output (SISO) on-off fading channel $P_{V,H|U}$ where the channel coefficients $\{H_i\}$ are i.i.d. and satisfy

$$\mathbb{P}[H_i = 0] = \epsilon', \quad \mathbb{P}[|H_i|^2 = 1/(1-\epsilon')] = 1-\epsilon' \tag{78}$$

where $0 < \epsilon' < \epsilon$. Such a fading distribution satisfies $\mathbb{E}\big[|H_i|^2\big] = 1$. Set now $N = 1$, $x_0 = \sqrt{E}$, and

$$\frac{1}{M} = Q\left(\sqrt{\frac{2E}{1-\epsilon'}} + Q^{-1}\left(1 - \frac{\epsilon-\epsilon'}{1-\epsilon'} + \sqrt{\frac{2(1-\epsilon')}{E}}\right)\right). \tag{79}$$

Let

$$\imath(u; v, h) \triangleq \log \frac{dP_{V,H|U=u}}{dP_{V,H|U=0}}(v, h). \tag{80}$$

By Theorem 2, there exists an (E, M, ϵ'')-code for which the maximal probability of error ϵ'' is upper-bounded as follows:

$$\begin{aligned}\epsilon'' &\le \mathbb{E}\Big[\min\Big\{1, (M-1)\mathbb{P}\Big[\imath(x_0; V, H) \le \imath(x_0; \hat{V}, H) \mid V, H\Big]\Big\}\Big] &(81)\\ &\le \epsilon' + (1-\epsilon')\mathbb{E}\Big[\min\Big\{1, (M-1)\cdot\mathbb{P}\Big[\imath(x_0; V, H) \le \imath(x_0; \hat{V}, H)\Big| V, |H|^2 = \frac{1}{1-\epsilon'}\Big]\Big\}\Big] &(82)\\ &\le \epsilon' + (1-\epsilon')\left(\frac{\epsilon-\epsilon'}{1-\epsilon'} - \sqrt{\frac{2(1-\epsilon')}{E}} + \sqrt{\frac{(1-\epsilon')}{E}}(1+o(1))\right), \quad E \to \infty. &(83)\end{aligned}$$

Here, in (81) and (82), $P_{HV\hat{V}}(h, v, \hat{v}) = P_H(h)P_{V|H,U}(v|h, x_0)P_{V|H,U}(\hat{v}|h, 0)$, and (83) follows from [8, Eqs. (33)–(40)]. For sufficiently large E, the RHS of (83) is less than ϵ. This implies that $M^*(E, \epsilon) \ge M$ for sufficiently large E. Furthermore, by [8, Eqs. (47)–(49)], we have

$$\log M^*(E, \epsilon) \ge \log M \ge \frac{E \log e}{1-\epsilon'} + \mathcal{O}(\sqrt{E}), \quad E \to \infty. \tag{84}$$

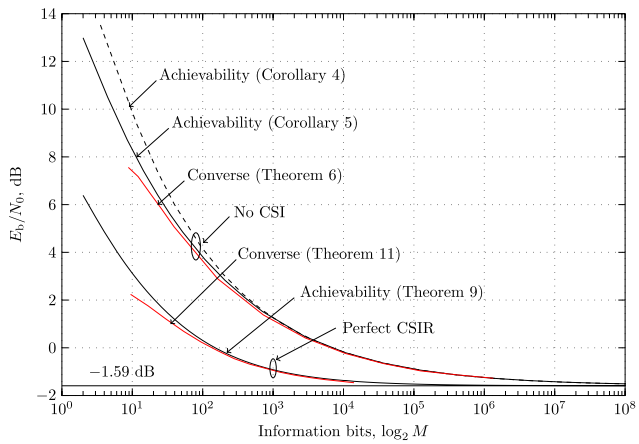

Fig. 1. Minimum energy per bit versus number of information bits; here $\epsilon = 10^{-3}$ and $m_r = 1$.

TABLE I

MINIMUM ENERGY E AND OPTIMAL NUMBER OF CHANNEL USES N^* VS. NUMBER OF INFORMATION BITS k FOR THE CASE $\epsilon = 10^{-3}$.

	Cor. 4		Cor. 5		Asymptotics	
k	E/N_0	N^*	E/N_0	N^*	E/N_0	N^*
10^1	98	25	67	18	120	50
10^2	2.6×10^2	39	2.4×10^2	38	2.9×10^2	63
10^3	1.3×10^3	96	1.3×10^3	96	1.4×10^3	124
10^4	9.6×10^3	304	9.6×10^3	304	9.7×10^3	336
10^5	8.2×10^4	1089	8.2×10^4	1090	8.2×10^4	1137

Clearly, the RHS of (84) is greater than the RHS of (77) (computed for $m_r = 1$) for large E.

In Theorem 11 below, we present a nonasymptotic converse bound, which we shall evaluate numerically in Section III-E.

Theorem 11: Fix $\eta > 6$, $E > 0$, and $0 < \epsilon < 1/2$. Let $x_1(\eta) > \eta$ be the unique solution of

$$\frac{1}{4\sqrt{\pi}} e^{-(x_1-\eta)^2/(4x_1)} \left(\frac{\eta}{\sqrt{x_1}} + \sqrt{x_1} \right) = Q\left(\frac{\eta - x_1}{\sqrt{2x_1}} \right). \quad (85)$$

Furthermore, let

$$g_\eta(x) \triangleq \begin{cases} Q\left((x-\eta)/\sqrt{2x} \right), & x > x_1(\eta), \\ 1 - \dfrac{x}{x_1(\eta)} Q\left(\dfrac{\eta - x_1(\eta)}{\sqrt{2x_1(\eta)}} \right), & x \le x_1(\eta). \end{cases} \quad (86)$$

Every (E, M, ϵ)-code for the MIMO Rayleigh block-fading channel (12) for the case of perfect CSIR satisfies

$$\log M \le \eta \log e - \log \left| g_\eta(m_r E) - \epsilon \right|^+. \quad (87)$$

Proof: See Appendix V. ■

E. Numerical Results

Fig. 1 shows[5] the achievability bounds (Corollary 4 and Corollary 5) and the converse bound (Theorem 6) for the channel (12) for the no-CSI case and when $\epsilon = 10^{-3}$ and $m_r = 1$. Specifically, the energy per bit $E_b = E/\log_2 M^*(E, \epsilon)$ is plotted against the number of information bits $\log_2 M^*(E, \epsilon)$. For the perfect-CSIR case, we plot the converse bound (Theorem 11) together with the achievability bound provided in [8, Eq. (15)] for the AWGN case. As proved in Theorem 9, this bound is also achievable in the perfect-CSIR case. As expected, as the number of information bits increases, the minimum energy per bit converges to -1.59 dB regardless of whether CSIR is available or not. However, for a fixed number of information bits, it is more costly to communicate in the no-CSI case than in the perfect-CSIR case. For example, it takes 2 dB more of energy to transmit 1000 information bits in the no-CSI case compared to the perfect-CSIR case. Additionally, to achieve an energy per bit of -1.5 dB, we need to transmit 7×10^7 information bits in the no-CSI case, but only 6×10^4 bits when perfect CSIR is available.

The codebook used in both Corollary 4 and Corollary 5 uses only one symbol x_0^* of the input alphabet in addition to 0. In Table I we list the number of channel uses $N^* = E/x_0^*$ over which the optimal input symbol x_0^* is repeated, as a function of the number of information bits k. For comparison, we also list the number of repetitions $N^* \approx \left(\frac{3}{2} Q^{-1}(\epsilon) \frac{E \log e}{\log E} \right)^{2/3}$ predicted by the asymptotic analysis (see (195)).

IV. CONCLUSIONS

In this paper, we established nonasymptotic bounds on the minimum energy per bit $E_b^*(k, \epsilon)$ required to transmit k information bits with error probability ϵ over a MIMO Rayleigh block-fading channel. As the number of information bits k goes to infinity, the ratio between $E_b^*(k, \epsilon)$ and the noise level converges to -1.59 dB, regardless of whether CSIR is available or not. However, in the nonasymptotic regime of finite k and nonzero error probability ϵ, the minimum energy per bit required in the no-CSI case is larger than that in the perfect-CSIR case (see Fig. 1). Specifically, as $k \to \infty$ the gap to -1.59 dB is proportional to $((\log k)/k)^{1/3}$ in the no-CSI case, and to $1/\sqrt{k}$ in the perfect-CSIR case.

The optimal signalling strategies for the two cases are different: in the no-CSI case, the transmitted codewords must have sufficient peakiness in order to overcome the lack of channel knowledge; in the perfect-CSIR case, the energy of each codeword must be spread uniformly over sufficiently many fading blocks in order to mitigate the stochastic variations on the received-signal energy caused by the fading process.

Throughout the paper, we have focused on the scenario where the blocklength of the code is unlimited, i.e., the spectral efficiency is zero. From a practical perspective, generalizing our analysis to the case of low but nonzero spectral efficiency is of interest. In the asymptotic regime $k \to \infty$, this can be done by approximating the spectral efficiency by an affine function of the energy per bit, and by characterizing the slope of the spectral efficiency versus energy per bit function at -1.59 dB (wideband slope) [2]. A generalization of Verdú's wideband-slope analysis to the finite-k case seems to require more sophisticated tools than the one used in the present paper (see [29, Sec. V.C] for some preliminary results in this direction).

[5]The numerical routines used to obtain these results are available at https://github.com/yp-mit/spectre

APPENDIX I
PROOF OF LEMMA 7

The proof relies on [22]. In particular, we shall make repeated use of [22, Corollary 1 and Lemma 2], which are restated below for convenience. For a continuous random variable A, let f_A denote its probability density function (pdf), and let f'_A and f''_A denote the first and the second derivatives of f_A, respectively. Furthermore, let S_1 and S_2 be independent Exp(1)-distributed random variables, which are also independent of A. Then, for every $x, q_1, q_2 \in \mathbb{R}$ [22, Lemma 2]:

$$f_{A+q_1S_1}(x) - f_{A+q_2S_2}(x) = (q_2 - q_1) f'_{A+q_1S_1+q_2S_2}(x). \tag{88}$$

This identity can be readily verified by computing the Fourier transform of both sides. Setting $q_2 = 0$ in (88), we obtain [22, Corollary 1]

$$f_{A+q_1S_1}(x) - f_A(x) = -q_1 f'_{A+q_1S_1}(x). \tag{89}$$

The proof of Lemma 7 consists of four steps.

1) We first restrict ourselves to the finite-dimensional setup, i.e., we assume that $\boldsymbol{x} \in \mathbb{R}_+^m$ for some $m \in \mathbb{N}$. We shall derive a necessary condition a minimizer $\boldsymbol{x}^* \in \mathbb{R}_+^m$ must satisfy, by deriving the Karush-Kuhn-Tucker (KKT) optimality conditions (see, e.g., [30, Sec. 5.5.3]).
2) Building upon these conditions, we show that the entries of $\boldsymbol{x}^*$ can take at most three distinct nonzero values.
3) We prove that if the entries of $\boldsymbol{x}^*$ take exactly three distinct nonzero values, then the maximum and the minimum nonzero value must appear only once, i.e., $\boldsymbol{x}^*$ is of the form (51). If the entries of $\boldsymbol{x}^*$ take less than three distinct nonzero values, then $\boldsymbol{x}^*$ satisfies (52) trivially.
4) Finally, we take m to infinity to complete the proof.

Departing from our convention, in this appendix we shall use log to denote the natural logarithm.

A. The KKT conditions

Let

$$\varphi(\boldsymbol{x}, \boldsymbol{s}) \triangleq \sum_{i=1}^{m} \Big(x_i s_i - \log(1 + x_i) \Big). \tag{90}$$

Using (90), we can express (62) for the case $\boldsymbol{x} \in \mathbb{R}_+^m$ as

$$\inf_{\boldsymbol{x} \in \mathbb{R}_+^m : \|\boldsymbol{x}\|_1 = E} \mathbb{P}[\varphi(\boldsymbol{x}, \boldsymbol{S}) \le \eta]. \tag{91}$$

By the KKT optimality conditions, if $\boldsymbol{x}^*$ is a minimizer of (62), then there must exist a $\lambda \in \mathbb{R}$ such that for all $k = 1, \ldots, m$,

$$\left. \frac{\partial \mathbb{P}[\varphi(\boldsymbol{x}, \boldsymbol{S}) \le \eta]}{\partial x_k} \right|_{\boldsymbol{x} = \boldsymbol{x}^*} \begin{cases} = \lambda, & \text{if } x_k^* > 0 \\ \ge \lambda, & \text{otherwise.} \end{cases} \tag{92}$$

Let $\hat{S}_k$ be an Exp(1)-distributed random variable that is independent of $\boldsymbol{S}$. Let $\langle \boldsymbol{x}, \boldsymbol{S} \rangle \triangleq \sum_{i=1}^m x_i S_i$, and let $\tilde{\eta} \triangleq \eta + \sum_{j=1}^m \log(1 + x_j)$. The partial derivative in (92) can be computed through a Fourier analysis as in the proof of [22, Lemma 1]. This yields

$$\frac{\partial \mathbb{P}[\varphi(\boldsymbol{x}, \boldsymbol{S}) \le \eta]}{\partial x_k} = \frac{f_{\langle \boldsymbol{x}, \boldsymbol{S} \rangle}(\tilde{\eta})}{1 + x_k} - f_{\langle \boldsymbol{x}, \boldsymbol{S} \rangle + x_k \hat{S}_k}(\tilde{\eta}). \tag{93}$$

From (93), it follows that

$$\begin{aligned} &\frac{\partial \mathbb{P}[\varphi(\boldsymbol{x}, \boldsymbol{S}) \le \eta]}{\partial x_j} - \frac{\partial \mathbb{P}[\varphi(\boldsymbol{x}, \boldsymbol{S}) \le \eta]}{\partial x_k} \\ &= f_{\langle \boldsymbol{x}, \boldsymbol{S} \rangle + x_k \hat{S}_k}(\tilde{\eta}) - f_{\langle \boldsymbol{x}, \boldsymbol{S} \rangle + x_j \hat{S}_j}(\tilde{\eta}) \\ &\quad + \frac{(x_k - x_j) f_{\langle \boldsymbol{x}, \boldsymbol{S} \rangle}(\tilde{\eta})}{(1 + x_k)(1 + x_j)} \qquad (94) \\ &= (x_j - x_k) \left(f'_{\langle \boldsymbol{x}, \boldsymbol{S} \rangle + x_k \hat{S}_k + x_j \hat{S}_j}(\tilde{\eta}) - \frac{f_{\langle \boldsymbol{x}, \boldsymbol{S} \rangle}(\tilde{\eta})}{(1 + x_k)(1 + x_j)} \right) \qquad (95) \end{aligned}$$

where in the last step we used (88).

B. The Entries of a Minimizer Can Take at Most Three Distinct Nonzero Values

As in [22], our proof is by contradiction. We shall assume without loss of generality that $m \ge 4$. Let $\boldsymbol{x}^*$ be a minimizer of (91), and assume that the entries of $\boldsymbol{x}^*$ take more than three distinct nonzero values, the smallest four of them being $0 < x_1^* < x_2^* < x_3^* < x_4^*$. Then, by (92) and (95),

$$(1 + x_j^*) f'_{\langle \boldsymbol{x}^*, \boldsymbol{S} \rangle + x_1^* \hat{S}_1 + x_j^* \hat{S}_j}(\tilde{\eta}) = \frac{f_{\langle \boldsymbol{x}^*, \boldsymbol{S} \rangle}(\tilde{\eta})}{(1 + x_1^*)}, \quad j = 2, 3, 4. \tag{96}$$

By (89), the left-hand side (LHS) of (96) can be expressed as follows:

$$\begin{aligned} &(1 + x_j^*) f'_{\langle \boldsymbol{x}^*, \boldsymbol{S} \rangle + x_1^* \hat{S}_1 + x_j^* \hat{S}_j}(\tilde{\eta}) \\ &\quad = f'_{\langle \boldsymbol{x}^*, \boldsymbol{S} \rangle + x_1^* \hat{S}_1 + x_j^* \hat{S}_j}(\tilde{\eta}) + f_{\langle \boldsymbol{x}^*, \boldsymbol{S} \rangle + x_1^* \hat{S}_1}(\tilde{\eta}) \\ &\qquad - f_{\langle \boldsymbol{x}^*, \boldsymbol{S} \rangle + x_1^* \hat{S}_1 + x_j^* \hat{S}_j}(\tilde{\eta}). \end{aligned} \tag{97}$$

Since the RHS of (96) does not depend on j, by substituting (97) into (96) and by taking the difference between the case $j = 2$ and the case $j = 3$, we obtain

$$\begin{aligned} 0 &= f'_{\langle \boldsymbol{x}^*, \boldsymbol{S} \rangle + x_1^* \hat{S}_1 + x_2^* \hat{S}_2}(\tilde{\eta}) - f'_{\langle \boldsymbol{x}^*, \boldsymbol{S} \rangle + x_1^* \hat{S}_1 + x_3^* \hat{S}_3}(\tilde{\eta}) \\ &\quad - \Big(f_{\langle \boldsymbol{x}^*, \boldsymbol{S} \rangle + x_1^* \hat{S}_1 + x_2^* \hat{S}_2}(\tilde{\eta}) - f_{\langle \boldsymbol{x}^*, \boldsymbol{S} \rangle + x_1^* \hat{S}_1 + x_3^* \hat{S}_3}(\tilde{\eta}) \Big) \qquad (98) \\ &= (x_3^* - x_2^*) \Big(f''_{\langle \boldsymbol{x}^*, \boldsymbol{S} \rangle + x_1^* \hat{S}_1 + x_2^* \hat{S}_2 + x_3^* \hat{S}_3}(\tilde{\eta}) \\ &\qquad - f'_{\langle \boldsymbol{x}^*, \boldsymbol{S} \rangle + x_1^* \hat{S}_1 + x_2^* \hat{S}_2 + x_3^* \hat{S}_3}(\tilde{\eta}) \Big). \qquad (99) \end{aligned}$$

Here, (99) follows by (88). Set

$$A \triangleq \langle \boldsymbol{x}^*, \boldsymbol{S} \rangle + x_1^* \hat{S}_1 + x_2^* \hat{S}_2. \tag{100}$$

Since $x_2^* \ne x_3^*$ by assumption, (99) can be rewritten as

$$f''_{A + x_3^* \hat{S}_3}(\tilde{\eta}) - f'_{A + x_3^* \hat{S}_3}(\tilde{\eta}) = 0. \tag{101}$$

Following the same steps as in (98)–(101), we also have that

$$f''_{A + x_4^* \hat{S}_4}(\tilde{\eta}) - f'_{A + x_4^* \hat{S}_4}(\tilde{\eta}) = 0. \tag{102}$$

Next, we show that (101) and (102) cannot hold simultaneously. This in turn implies that the entries of $\boldsymbol{x}^*$ must take at most three distinct nonzero values. Let

$$g(t) \triangleq f''_{A+t\hat{S}}(\tilde{\eta}) - f'_{A+t\hat{S}}(\tilde{\eta}) \tag{103}$$

where $\hat{S} \sim \text{Exp}(1)$. Since (101) and (102) imply that $g(x_3^*) = g(x_4^*) = 0$, to establish a contradiction between (101) and (102), it suffices to show that the function $g(t)$ has at most one zero on $(0, \infty)$. Observe that $g(t)$ can be rewritten as

$$\begin{aligned} g(t) &= f''_{A+t\hat{S}}(\tilde{\eta}) - f'_{A+t\hat{S}}(\tilde{\eta}) && (104)\\ &= \left(f''_A \star f_{t\hat{S}}\right)(\tilde{\eta}) - \left(f'_A \star f_{t\hat{S}}\right)(\tilde{\eta}) && (105)\\ &= \frac{1}{t}\int_0^{\tilde{\eta}} \left(f''_A(\tilde{\eta}-z) - f'_A(\tilde{\eta}-z)\right)e^{-z/t}dz. && (106) \end{aligned}$$

Since the kernel $e^{-z/t}$ is *strictly totally positive* [31, p. 11] on $[0, \tilde{\eta}] \times [0, \infty)$, it follows from [31, Th. 3.1(b)] that the number of zeros of $g(t)$ on $(0, \infty)$ cannot exceed the number of sign changes of $z \mapsto f''_A(z) - f'_A(z)$ on $(0, \tilde{\eta})$, provided that the latter number is finite. Thus, to prove that $g(t)$ has at most one zero over $(0, \infty)$, it suffices to show that $f''_A(z) - f'_A(z)$ changes sign at most once on $(0, \tilde{\eta})$. In fact, we shall prove that it changes sign at most once over an interval that contains $(0, \tilde{\eta})$. By [22, Lemma 3], $f'_A(z)$ is continuous on $\mathbb{R}$, and there exists a $\hat{z} > 0$ such that $f'_A(z) > 0$ for all $z \in (0, \hat{z})$. Let $\bar{z} = \arg\max_{z\in[0,1]} f'_A(z)$. Since $f'_A(0) = 0$ (which follows because $f'_A(z) = 0$ for all $z < 0$ and because $f'_A(z)$ is continuous) and since $f'_A(z) > 0$ for all $z \in (0, \hat{z})$, we have that $0 < \bar{z} \leq 1$. This implies that

$$\begin{aligned} f'_A(\bar{z}) - f_A(\bar{z}) &= f'_A(\bar{z}) - \int_0^{\bar{z}} f'_A(z)dz && (107)\\ &\geq f'_A(\bar{z}) - \bar{z}f'_A(\bar{z}) \geq 0. && (108) \end{aligned}$$

By Lemma 12 in Appendix II, f_A is strictly log-concave on $(0, \infty)$, which implies that $z \mapsto f'_A(z)/f_A(z)$ is strictly decreasing on $(0, \infty)$. This in turn implies that there exists a unique $z_0 > 0$ such that $f'_A(z_0) - f_A(z_0) = 0$. It also implies that $f'_A(z) - f_A(z) > 0$ if $z \in (0, z_0)$ and $f'_A(z) - f_A(z) < 0$ if $z > z_0$. We shall now prove that

1) $f''_A(z) - f'_A(z)$ changes sign at most once on $(0, z_0)$;
2) $(0, \tilde{\eta}) \subset (0, z_0)$, i.e.,

$$\tilde{\eta} < z_0. \tag{109}$$

1) The function $f''_A(z) - f'_A(z)$ changes sign at most once on $(0, z_0)$: It suffices to prove that $f'_A(z) - f_A(z)$ is unimodal on $(0, z_0)$. This is done by induction. Recall that f_A is the convolution of exponential pdfs (see (100)), i.e., A can be written as $\sum_{i=1}^{m'} a_i S_i$ for some $a_i > 0$, $i = 1, \ldots, m'$, and $2 \leq m' \leq m + 2$. Let B_k, $k = 1, \ldots, m'$, denote the partial sum $\sum_{i=1}^{k} a_i S_i$ and let z_k, $k = 2, \ldots$, denote the solution of $f'_{B_k}(z_k) - f_{B_k}(z_k) = 0$. Recall that, by the strict log-concavity of f_{B_k}, we have that z_k is unique and that $f'_{B_k}(z) - f_{B_k}(z) > 0$ if $z \in (0, z_k)$ and $f'_{B_k}(z) - f_{B_k}(z) < 0$ if $z > z_k$. It can be verified that $f'_{B_2} - f_{B_2}$ is unimodal on $(0, z_2)$. Assume now that $f'_{B_k} - f_{B_k}$ is unimodal on $(0, z_k)$ for some $k > 2$. We next show that $f'_{B_{k+1}} - f_{B_{k+1}}$ is unimodal on $(0, z_{k+1})$. Note that

$$f'_{B_{k+1}} - f_{B_{k+1}} = (f'_{B_k} - f_{B_k}) \star f_{a_{k+1}S_{k+1}}. \tag{110}$$

Since $f'_{B_k} - f_{B_k}$ and $f_{a_{k+1}S_{k+1}}$ are smooth and strictly positive on $(0, z_k)$, it follows that $(f'_{B_{k+1}} - f_{B_{k+1}})(z_k) > 0$. This implies that $z_{k+1} > z_k$. Since $f'_{B_k} - f_{B_k}$ is positive and unimodal on $(0, z_k)$, and since $f_{a_{k+1}S_{k+1}}$ is log-concave, it follows that $f'_{B_{k+1}} - f_{B_{k+1}}$ is positive and unimodal on $(0, z_k)$ [32]. Furthermore, the strict log-concavity of f_{B_k} and the definitions of z_k and z_{k+1} imply that, for every $z \in [z_k, z_{k+1})$,

$$\begin{aligned} &(f''_{B_{k+1}} - f'_{B_{k+1}})(z)\\ &\quad= \frac{1}{a_{k+1}}\Big(\underbrace{f'_{B_k}(z) - f_{B_k}(z)}_{\leq 0} - \big(\underbrace{f'_{B_{k+1}}(z) - f_{B_{k+1}}(z)}_{>0}\big)\Big) && (111)\\ &\quad< 0. && (112) \end{aligned}$$

The first step follows by applying (89) twice. The inequality (112) implies that $f'_{B_{k+1}} - f_{B_{k+1}}$ is unimodal on $(0, z_{k+1})$. Hence, by induction, $f'_A - f_A$ is unimodal on $(0, z_0)$.

2) Proof of (109)*:* It follows from (96) that $f'_A(\tilde{\eta}) > 0$, which implies by [22, Lemma 3] that $f'_A(t) > 0$ for all $t \in (0, \tilde{\eta})$. Therefore, we have

$$f'_{A+x_3^*\hat{S}_3}(\tilde{\eta}) = \left(f'_A \star f_{x_3^*\hat{S}_3}\right)(\tilde{\eta}) > 0. \tag{113}$$

By the strict log-concavity of $f_{A+x_3^*\hat{S}}(\cdot)$ and by (101),

$$\frac{f'_{A+x_3^*\hat{S}}(\tilde{\eta})}{f_{A+x_3^*\hat{S}}(\tilde{\eta})} > \frac{f''_{A+x_3^*\hat{S}}(\tilde{\eta})}{f'_{A+x_3^*\hat{S}}(\tilde{\eta})} = 1. \tag{114}$$

Moreover, by (89) and (101),

$$f_A(\tilde{\eta}) - f_{A+x_3^*\hat{S}_3}(\tilde{\eta}) = f'_A(\tilde{\eta}) - f'_{A+x_3^*\hat{S}_3}(\tilde{\eta}). \tag{115}$$

Using (114) in (115), we conclude that

$$f'_A(\tilde{\eta}) - f_A(\tilde{\eta}) > 0. \tag{116}$$

This implies (109).

C. The Minimum and Maximum Nonzero Values Must Each Appear Only Once

We focus on the case when the entries of $\boldsymbol{x}^*$ take exactly three distinct nonzero values. Assume without loss of generality that $\boldsymbol{x}^*$ has the following form

$$\boldsymbol{x}^* = [\underbrace{x_1^*, \ldots, x_1^*}_{N_1}, \underbrace{x_2^*, \ldots, x_2^*}_{N_2}, \underbrace{x_3^*, \ldots, x_3^*}_{N_3}, 0, \ldots, 0] \tag{117}$$

where $x_1^*N_1 + x_2^*N_2 + x_3^*N_3 = E$, $0 < x_1^* < x_2^* < x_3^*$, and $N_1, N_2, N_3 > 0$. We shall prove that if $N_1 > 1$, then

$$\left.\frac{\partial^2 \mathbb{P}[\varphi(\boldsymbol{x}_\delta^*, \boldsymbol{S}) \leq \eta]}{\partial \delta^2}\right|_{\delta=0} < 0 \tag{118}$$

where $\boldsymbol{x}_\delta^* \triangleq \boldsymbol{x}^* + \delta\boldsymbol{e}_1 - \delta\boldsymbol{e}_2$. Since this contradicts the assumption that $\boldsymbol{x}^*$ is a minimizer, we conclude that $N_1 = 1$. Using a similar argument, one can show that $N_3 = 1$.

We first compute the LHS of (118). Assume $N_1 > 1$, so that $[\boldsymbol{x}^*]_1 = [\boldsymbol{x}^*]_2 = x_1^*$. Set $\tilde{\eta}_\delta \triangleq \eta + \sum_{i=1}^{m} \log(1 + [\boldsymbol{x}_\delta^*]_i)$. Proceeding similarly as in the proof of (93), we obtain

$$\begin{aligned}
&\frac{\partial \mathbb{P}[\varphi(\boldsymbol{x}_\delta^*, \boldsymbol{S}) \le \eta]}{\partial \delta} \\
&= -\Big(f_{\langle \boldsymbol{x}_\delta^*, \boldsymbol{S}\rangle + (x_1^*+\delta)\hat{S}_1}(\tilde{\eta}) - f_{\langle \boldsymbol{x}_\delta, \boldsymbol{S}\rangle + (x_1^*-\delta)\hat{S}_2}(\tilde{\eta}_\delta)\Big) \\
&\quad + \frac{f_{\langle \boldsymbol{x}_\delta^*, \boldsymbol{S}\rangle}(\tilde{\eta}_\delta)}{1 + x_1^* + \delta} - \frac{f_{\langle \boldsymbol{x}_\delta^*, \boldsymbol{S}\rangle}(\tilde{\eta}_\delta)}{1 + x_1^* - \delta} \qquad (119) \\
&= 2\delta f'_{\langle \boldsymbol{x}_\delta^*, \boldsymbol{S}\rangle + (x_1^*+\delta)\hat{S}_1 + (x_1^*-\delta)\hat{S}_2}(\tilde{\eta}_\delta) - \frac{2\delta f_{\langle \boldsymbol{x}_\delta^*, \boldsymbol{S}\rangle}(\tilde{\eta}_\delta)}{(1 + x_1^*)^2 - \delta^2}. \qquad (120)
\end{aligned}$$

Here, (120) follows from (88). Taking the derivative of the RHS of (120) with respect to δ and then setting $\delta = 0$, we obtain (recall that $\tilde{\eta} = \eta + \sum_{i=1}^{m} \log(1 + [\boldsymbol{x}^*]_i)$)

$$\begin{aligned}
&\frac{\partial^2 \mathbb{P}[\varphi(\boldsymbol{x}_\delta^*, \boldsymbol{S}) \le \eta]}{\partial \delta^2}\bigg|_{\delta=0} \\
&\quad = 2\left(f'_{\langle \boldsymbol{x}^*, \boldsymbol{S}\rangle + x_1^*\hat{S}_1 + x_1^*\hat{S}_2}(\tilde{\eta}) - \frac{f_{\langle \boldsymbol{x}^*, \boldsymbol{S}\rangle}(\tilde{\eta})}{(1 + x_1^*)^2}\right). \qquad (121)
\end{aligned}$$

From the KKT condition (96), we know that

$$f'_{\langle \boldsymbol{x}^*, \boldsymbol{S}\rangle + x_1^*\hat{S}_1 + x_2^*\hat{S}}(\tilde{\eta}) - \frac{f_{\langle \boldsymbol{x}^*, \boldsymbol{S}\rangle}(\tilde{\eta})}{(1 + x_1^*)(1 + x_2^*)} = 0 \qquad (122)$$

where $\hat{S} \sim \mathrm{Exp}(1)$ is independent of all other random variables. Let $T \triangleq \hat{S}_1 + \hat{S}_2$. Subtracting the LHS of (122) from (121), we obtain

$$\begin{aligned}
&\frac{1}{2}\frac{\partial^2 \mathbb{P}[\varphi(\boldsymbol{x}_\delta^*, \boldsymbol{S}) \le \eta]}{\partial \delta^2}\bigg|_{\delta=0} \\
&\quad = (x_2^* - x_1^*)\left(f''_{\langle \boldsymbol{x}^*, \boldsymbol{S}\rangle + x_1^*T + x_2^*\hat{S}}(\tilde{\eta}) - \frac{f_{\langle \boldsymbol{x}^*, \boldsymbol{S}\rangle}(\tilde{\eta})}{(1 + x_1^*)^2(1 + x_2^*)}\right) \qquad (123) \\
&\quad = (x_2^* - x_1^*)\left(f''_{\langle \boldsymbol{x}^*, \boldsymbol{S}\rangle + x_1^*T + x_2^*\hat{S}}(\tilde{\eta}) - \frac{f'_{\langle \boldsymbol{x}^*, \boldsymbol{S}\rangle + x_1^*\hat{S}_1 + x_2^*\hat{S}}(\tilde{\eta})}{1 + x_1^*}\right) \qquad (124) \\
&\quad = \frac{x_2^* - x_1^*}{1 + x_1^*}\left(f''_{\langle \boldsymbol{x}^*, \boldsymbol{S}\rangle + x_1^*T + x_2^*\hat{S}}(\tilde{\eta}) - f'_{\langle \boldsymbol{x}^*, \boldsymbol{S}\rangle + x_1^*T + x_2^*\hat{S}}(\tilde{\eta})\right). \qquad (125)
\end{aligned}$$

Here, in (123) we used (88); (124) follows from (122); and in (125) we used (89).

We shall next make (125) depend on x_3^*. Note first that by (89),

$$\begin{aligned}
&f''_{\langle \boldsymbol{x}^*, \boldsymbol{S}\rangle + x_1^*T + x_2^*\hat{S}}(\tilde{\eta}) - f'_{\langle \boldsymbol{x}^*, \boldsymbol{S}\rangle + x_1^*T + x_2^*\hat{S}}(\tilde{\eta}) \\
&\quad + f'_{\langle \boldsymbol{x}^*, \boldsymbol{S}\rangle + x_1^*T + x_2^*\hat{S} + x_3^*\hat{S}_3}(\tilde{\eta}) - f''_{\langle \boldsymbol{x}^*, \boldsymbol{S}\rangle + x_1^*T + x_2^*\hat{S} + x_3^*\hat{S}_3}(\tilde{\eta}) \\
&\quad = x_3^*\Big(f'''_{\langle \boldsymbol{x}^*, \boldsymbol{S}\rangle + x_1^*T + x_2^*\hat{S} + x_3^*\hat{S}_3}(\tilde{\eta}) - f''_{\langle \boldsymbol{x}^*, \boldsymbol{S}\rangle + x_1^*T + x_2^*\hat{S} + x_3^*\hat{S}_3}(\tilde{\eta})\Big). \qquad (126)
\end{aligned}$$

Also by (89) and (101),

$$\begin{aligned}
&f'''_{\langle \boldsymbol{x}^*, \boldsymbol{S}\rangle + x_1^*T + x_2^*\hat{S} + x_3^*\hat{S}_3}(\tilde{\eta}) - f''_{\langle \boldsymbol{x}^*, \boldsymbol{S}\rangle + x_1^*T + x_2^*\hat{S} + x_3^*\hat{S}_3}(\tilde{\eta}) \\
&\quad = \frac{1}{x_1^*}\Big(f'_{\langle \boldsymbol{x}^*, \boldsymbol{S}\rangle + x_1^*T + x_2^*\hat{S} + x_3^*\hat{S}_3}(\tilde{\eta}) - f''_{\langle \boldsymbol{x}^*, \boldsymbol{S}\rangle + x_1^*T + x_2^*\hat{S} + x_3^*\hat{S}_3}(\tilde{\eta})\Big). \qquad (127)
\end{aligned}$$

Combining (126) and (127), we conclude that

$$\begin{aligned}
&f''_{\langle \boldsymbol{x}^*, \boldsymbol{S}\rangle + x_1^*T + x_2^*\hat{S}}(\tilde{\eta}) - f'_{\langle \boldsymbol{x}^*, \boldsymbol{S}\rangle + x_1^*T + x_2^*\hat{S}}(\tilde{\eta}) \\
&\quad = \frac{x_3^* - x_1^*}{x_1^*}\Big(f'_{\langle \boldsymbol{x}^*, \boldsymbol{S}\rangle + x_1^*T + x_2^*\hat{S} + x_3^*\hat{S}_3}(\tilde{\eta}) \\
&\qquad\qquad - f''_{\langle \boldsymbol{x}^*, \boldsymbol{S}\rangle + x_1^*T + x_2^*\hat{S} + x_3^*\hat{S}_3}(\tilde{\eta})\Big). \qquad (128)
\end{aligned}$$

Substituting (128) in (125), we obtain

$$\begin{aligned}
&\frac{1}{2}\frac{\partial^2 \mathbb{P}[\varphi(\boldsymbol{x}_\delta^*, \boldsymbol{S}) \le \eta]}{\partial \delta^2}\bigg|_{\delta=0} \\
&\quad = \frac{(x_2^* - x_1^*)(x_3^* - x_1^*)}{x_1^*(1 + x_1^*)}\Big(f'_{\langle \boldsymbol{x}^*, \boldsymbol{S}\rangle + x_1^*T + x_2^*\hat{S} + x_3^*\hat{S}_3}(\tilde{\eta}) \\
&\qquad\qquad - f''_{\langle \boldsymbol{x}^*, \boldsymbol{S}\rangle + x_1^*T + x_2^*\hat{S} + x_3^*\hat{S}_3}(\tilde{\eta})\Big). \qquad (129)
\end{aligned}$$

Since $(x_2^* - x_1^*)(x_3^* - x_1^*) > 0$, to establish (118), it remains to prove that

$$f'_{\langle \boldsymbol{x}^*, \boldsymbol{S}\rangle + x_1^*T + x_2^*\hat{S} + x_3^*\hat{S}_3}(\tilde{\eta}) - f''_{\langle \boldsymbol{x}^*, \boldsymbol{S}\rangle + x_1^*T + x_2^*\hat{S} + x_3^*\hat{S}_3}(\tilde{\eta}) < 0. \qquad (130)$$

Let $\widetilde{A} \triangleq \langle \boldsymbol{x}^*, \boldsymbol{S}\rangle + x_2^*\hat{S} + x_3^*\hat{S}_3$. The LHS of (130) can be rewritten as

$$\begin{aligned}
&f'_{\widetilde{A} + x_1^*T}(\tilde{\eta}) - f''_{\widetilde{A} + x_1^*T}(\tilde{\eta}) \\
&\quad = \left(f'_{\widetilde{A} + x_1^*\hat{S}_1} - f''_{\widetilde{A} + x_1^*\hat{S}_1}\right) \star f_{x_1^*\hat{S}_2}(\tilde{\eta}) \qquad (131) \\
&\quad = \frac{1}{x_1^*}\int_0^{\tilde{\eta}}\Big(f'_{\widetilde{A} + x_1^*\hat{S}_1}(\tilde{\eta} - z) - f''_{\widetilde{A} + x_1^*\hat{S}_1}(\tilde{\eta} - z)\Big)e^{-z/x_1^*}dz. \qquad (132)
\end{aligned}$$

Since $A + x_3^*\hat{S}_3 \sim \widetilde{A} + x_1^*\hat{S}_1$, by (101),

$$f'_{\widetilde{A} + x_1^*\hat{S}_1}(\tilde{\eta}) - f''_{\widetilde{A} + x_1^*\hat{S}_1}(\tilde{\eta}) = 0. \qquad (133)$$

Note that, for every $t \in (0, \tilde{\eta})$, we have

$$\begin{aligned}
&f'_{\widetilde{A} + x_1^*\hat{S}_1}(t) - f''_{\widetilde{A} + x_1^*\hat{S}_1}(t) \\
&\quad = \int_0^t (f'_{\widetilde{A}}(z) - f''_{\widetilde{A}}(z))e^{-(t-z)/x_1^*}dz \qquad (134) \\
&\quad = e^{-t/x_1^*}\underbrace{\int_0^t (f'_{\widetilde{A}}(z) - f''_{\widetilde{A}}(z))e^{z/x_1^*}dz}_{\triangleq h(t)}. \qquad (135)
\end{aligned}$$

In Appendix I-B1, we have shown that the function $f'_{\widetilde{A}} - f''_{\widetilde{A}}$ changes sign at most once over the interval $(0, \tilde{\eta})$. Therefore, $h'(t) = (f'_{\widetilde{A}}(t) - f''_{\widetilde{A}}(t))e^{t/x_1^*}$ changes sign at most once over the interval $(0, \tilde{\eta})$. But since $h(\tilde{\eta}) = e^{\tilde{\eta}/x_1^*}\left(f'_{\widetilde{A} + x_1^*\hat{S}_1}(\tilde{\eta}) - f''_{\widetilde{A} + x_1^*\hat{S}_1}(\tilde{\eta})\right) = 0 = h(0)$, the function h does not change sign on $(0, \tilde{\eta})$. Indeed, there are three possible cases:

1) $h'(t) = 0$ for all $t \in (0, \tilde{\eta})$; in this case $h(t) = 0$ for all $t \in (0, \tilde{\eta})$.
2) there exists a $t_0 \in (0, \tilde{\eta})$ such that $h'(t) \leq 0$ on $(0, t_0)$, $h'(t_0) = 0$, and $h'(t) \geq 0$ on $(t_0, \tilde{\eta})$; in this case $h(t) \leq 0$ for all $t \in (0, \tilde{\eta})$.
3) there exists a $t_0 \in (0, \tilde{\eta})$ such that $h'(t) \geq 0$ on $(0, t_0)$, $h'(t_0) = 0$, and $h'(t) \leq 0$ on $(t_0, \tilde{\eta})$; in this case $h(t) \geq 0$ for all $t \in (0, \tilde{\eta})$.

In all three scenarios, $h(t)$ does not change sign on $(0, \tilde{\eta})$. This implies that $f'_{\widetilde{A}+x_1^*\hat{S}_1} - f''_{\widetilde{A}+x_1^*\hat{S}_1}$ does not change sign on $(0, \tilde{\eta})$ either. Furthermore,

$$\begin{aligned}\int_0^{\tilde{\eta}} & f'_{\widetilde{A}+x_1^*\hat{S}_1}(z) - f''_{\widetilde{A}+x_1^*\hat{S}_1}(z)dz \\ &= f_{\widetilde{A}+x_1^*\hat{S}_1}(\tilde{\eta}) - f'_{\widetilde{A}+x_1^*\hat{S}_1}(\tilde{\eta}) \\ &\quad + \underbrace{f'_{\widetilde{A}+x_1^*\hat{S}_1}(0) - f_{\widetilde{A}+x_1^*\hat{S}_1}(0)}_{=0} \qquad (136)\\ &< 0. \qquad (137)\end{aligned}$$

Here, the first step follows because $f'_{\widetilde{A}+x_1^*\hat{S}_1}(0) = f''_{\widetilde{A}+x_1^*\hat{S}_1}(0) = 0$ [22, Lemma 3], and the second step follows from (114). We establish (130) by using the following chain of inequalities

$$\begin{aligned} & f'_{\widetilde{A}+x_1^*T}(\tilde{\eta}) - f''_{\widetilde{A}+x_1^*T}(\tilde{\eta}) \\ & \leq \frac{e^{-\tilde{\eta}/x_1^*}}{x_1^*}\int_0^{\tilde{\eta}}\Big(f'_{\widetilde{A}+x_1^*\hat{S}_1}(\tilde{\eta}-z) - f''_{\widetilde{A}+x_1^*\hat{S}_1}(\tilde{\eta}-z)\Big)dz \qquad (138)\\ & < 0. \qquad (139)\end{aligned}$$

Here, (138) follows from (132) and because $e^{-z/x_1^*} \geq e^{-\tilde{\eta}/x_1^*} > 0$ for all $z \in (0, \tilde{\eta})$; (139) follows from (137).

D. Extension to $\mathbb{R}_+^\infty$

Consider the following chain of equalities:

$$\begin{aligned} & \inf_{\boldsymbol{x}\in\mathbb{R}_+^\infty:\|\boldsymbol{x}\|_1=m_{\mathrm{r}}E} \mathbb{P}\left[\sum_{i=1}^{\infty}\Big(x_iS_i - \log(1+x_i)\Big) \leq \eta\right] \\ & = \lim_{m\to\infty}\inf_{\boldsymbol{x}\in\mathbb{R}_+^m:\|\boldsymbol{x}\|_1=m_{\mathrm{r}}E} \mathbb{P}\left[\sum_{i=1}^{m}\Big(x_iS_i - \log(1+x_i)\Big) \leq \eta\right] \qquad (140)\\ & = \lim_{m\to\infty}\inf \mathbb{P}\left[\sum_{i=1}^{m}\Big(x_iS_i - \log(1+x_i)\Big) \leq \eta\right] \qquad (141)\\ & = \inf \mathbb{P}\left[\sum_{i=1}^{\infty}\Big(x_iS_i - \log(1+x_i)\Big) \leq \eta\right]. \qquad (142)\end{aligned}$$

Here, both (140) and (142) follow from the monotone convergence theorem [25, Th. 2.14]; the infimum in (141) and (142) is over all $\boldsymbol{x}$ (in $\mathbb{R}_+^m$ and $\mathbb{R}_+^\infty$, respectively) of the form (51) or (52). This concludes the proof of Lemma 7.

Appendix II
Convolution of Exponential Distributions

In this appendix, we summarize some results about the convolution of exponential distributions that are needed in Appendices I, III, and IV.

The first lemma deals with the log-concavity of the convolution of exponential distributions. Recall that a function f is called log-concave if $\log f$ is concave, and it is called *strictly* log-concave if $\log f$ is strictly concave. Since the exponential distribution is log-concave, and log-concavity is preserved under convolution [32], it follows that the convolution of exponential distributions is also log-concave. Lemma 12 below shows that this distribution is in fact *strictly* log-concave.

Lemma 12: Fix an integer $m \geq 2$. Let $S_1, \ldots, S_m$ be i.i.d. Exp(1)-distributed random variables, and let $a_1, \ldots, a_m$ be positive real numbers. Furthermore, let $B \triangleq \sum_{i=1}^m a_iS_i$. Then, the pdf f_B of B is strictly log-concave on $(0, \infty)$.

Proof: The proof is based on induction. Through algebraic manipulations, it can be verified that $f_{a_1S_1+a_1S_2}$ is strictly log-concave on $(0, \infty)$ for every $a_1, a_2 > 0$. Suppose now that the pdf of $B_k \triangleq \sum_{i=1}^k a_iS_i$ is strictly log-concave for some $k \geq 2$. We have

$$f_{B_{k+1}}(t) = \int \underbrace{f_{B_k}(t-s)f_{a_{k+1}S_{k+1}}(s)}_{\triangleq g(s,t)}ds, \quad t > 0. \qquad (143)$$

It follows that the integrand $g(s, t)$ in (143) is (jointly) log-concave in (s, t) on $\mathbb{R}_+^2$ and it is strictly log-concave on the subspace $\{(s, t) \in \mathbb{R}_+^2 : s \leq t\}$. Note that by the Prékopa Theorem [33], [34, Sec. 3] for each $a, b > 0$,

$$\begin{aligned} f_{B_{k+1}}\left(\frac{a+b}{2}\right) &= \int g\left(s, \frac{a+b}{2}\right)ds \qquad (144)\\ &\geq \left(\int g(s,a)ds\right)^{1/2}\left(\int g(s,b)ds\right)^{1/2} \qquad (145)\\ &= \sqrt{f_{B_{k+1}}(a)f_{B_{k+1}}(b)}. \qquad (146)\end{aligned}$$

This implies that $f_{B_{k+1}}$ is log-concave. Following the proof of the Prékopa Theorem in [34, Sec. 3], and using that the function $(s, t) \mapsto f_{B_k}(t-s)f_{a_{k+1}S_{k+1}}(s)$ is strictly positive, smooth [22, Lemma 3], and strictly log-concave for $0 < s < t$, we can verify that the inequality in (145) is strict for every $a, b > 0$. This in turn implies that $f_{B_{k+1}}$ is *strictly* log-concave on $(0, \infty)$. By induction, f_B is strictly log-concave on $(0, \infty)$ for every $m \geq 2$. ■

The next lemma characterizes the optimal convex combination of exponential random variables that minimizes the probability that such combination does not exceed a given threshold.

Lemma 13: Let $n \in \mathbb{N}$, let $S_1, \ldots, S_n$ be i.i.d. Exp(1)-distributed random variables, and let $\mathcal{A}_n \triangleq \{\boldsymbol{x} \in \mathbb{R}_+^n : \|\boldsymbol{x}\|_1 \leq 1, x_1 \geq x_2 \geq \ldots \geq x_n\}$. Then, for every $t \in \mathbb{R}_+$, there exists a $k \in \{1, \ldots, n\}$ such that

$$\arg\min_{\boldsymbol{x}\in\mathcal{A}_n} \mathbb{P}\left[\sum_{i=1}^n x_iS_i \leq t\right] = \Big[\underbrace{\frac{1}{k}, \ldots, \frac{1}{k}}_{k}, 0, \ldots, 0\Big]. \qquad (147)$$

In particular, if $t \in (0, 1]$, then

$$\arg\min_{\boldsymbol{x}\in\mathcal{A}_n} \mathbb{P}\left[\sum_{i=1}^n x_iS_i \leq t\right] = \Big[\frac{1}{n}, \ldots, \frac{1}{n}\Big]. \qquad (148)$$

Proof: The equality (147) follows directly from [22, p. 2597]. To prove (148), it is sufficient to

show that for every $k \in \mathbb{N}$ and every $t \in (0, 1]$, the following inequality holds:

$$\mathbb{P}\left[\sum_{i=1}^{k} S_i \le tk\right] \ge \mathbb{P}\left[\sum_{i=1}^{k+1} S_i \le t(k+1)\right]. \tag{149}$$

Let $f_k(x) \triangleq x^k e^{-x}$. Consider the following chain of (in)equalities

$$\begin{aligned}
&\mathbb{P}\left[\sum_{i=1}^{k} S_i \le tk\right] - \mathbb{P}\left[\sum_{i=1}^{k+1} S_i \le t(k+1)\right] \\
&= \int_0^{tk} \frac{f_{k-1}(x)}{(k-1)!}dx - \int_0^{t(k+1)} \frac{f_k(x)}{k!}dx && (150)\\
&= \frac{1}{k!}\left(\int_0^{tk} k f_{k-1}(x)dx - \int_0^{t(k+1)} f_k(x)dx\right) && (151)\\
&= \frac{1}{k!}\left(f_k(tk) - \int_{tk}^{t(k+1)} f_k(x)dx\right) && (152)\\
&\ge \frac{1}{k!}\Bigg(f_k(tk) \\
&\quad - \int_{tk}^{t(k+1)} \exp\Big(\log f(tk) + \frac{f_k'(tk)}{f_k(tk)}(x-tk)\log e\Big)dx\Bigg) && (153)\\
&= \frac{f_k(tk)}{k!}\frac{1-te^{1-t}}{1-t} && (154)\\
&\ge 0. && (155)
\end{aligned}$$

Here, (150) follows because the random variable $\sum_{i=1}^{k} S_i$ is chi-squared distributed with pdf $f_{k-1}(x)/(k-1)!$; in (152) we used integration by parts; (153) follows because $f_k(x)$ is log-concave, which implies that for every $x \ge 0$

$$\log f_k(x) \le \log f_k(tk) + \frac{f_k'(tk)}{f_k(tk)}(x-tk)\log e; \tag{156}$$

finally, (155) follows because $t \mapsto te^{1-t}$ is monotonically increasing on $(0, 1]$, and because $te^{1-t}\big|_{t=1} = 1$. This proves (149). ■

The following lemma provides a uniform lower bound on the cdf of the weighted sum of exponential distributions.

Lemma 14: Let $\{S_i\}$ be i.i.d. Exp(1)-distributed random variables. Let $\boldsymbol{x} = [x_1, x_2, \ldots] \in \mathbb{R}_+^\infty$ satisfy $0 < \|\boldsymbol{x}\|_1 < \infty$. Furthermore, let

$$L(\boldsymbol{x}) \triangleq \frac{1}{\|\boldsymbol{x}\|_2}\left(\sum_{i=1}^{\infty} x_i S_i - \|\boldsymbol{x}\|_1\right) \tag{157}$$

and denote the cdf of $L(\boldsymbol{x})$ by $F_{L(\boldsymbol{x})}(t)$. Then, for every $t \in (-\infty, 0]$,

$$F_{L(\boldsymbol{x})}(t) \ge \left|\frac{1}{2} + t\right|^+. \tag{158}$$

Equivalently,

$$F_{L(\boldsymbol{x})}^{-1}(\epsilon) \le \epsilon - \frac{1}{2}, \quad \text{for all } 0 < \epsilon < \frac{1}{2}. \tag{159}$$

Proof: Since $\|\boldsymbol{x}\|_1 > 0$, we can assume without loss of generality that $x_1 > 0$. Let $\boldsymbol{x}_n$ denote the vector that contains the first n entries of $\boldsymbol{x}$, let

$$L_n(\boldsymbol{x}) \triangleq \frac{1}{\|\boldsymbol{x}_n\|_2}\left(\sum_{i=1}^{n} x_i S_i - \|\boldsymbol{x}_n\|_1\right) \tag{160}$$

and let $F_{L_n(\boldsymbol{x})}(t)$ denote the cdf of $L_n(\boldsymbol{x})$. Through algebraic manipulations, it can be shown that $F_{L_n(\boldsymbol{x})}(t)$ converges pointwise to $F_{L(\boldsymbol{x})}(t)$ as $n \to \infty$. Hence, to prove (158), it suffices to show that for every $n \in \mathbb{N}$ and every $t \in (-\infty, 0]$

$$F_{L_n(\boldsymbol{x})}(t) \ge \left|\frac{1}{2} + t\right|^+. \tag{161}$$

We first show that (161) holds when $t = 0$. Indeed, we have that

$$\begin{aligned}
F_{L_n(\boldsymbol{x})}(0) &= \mathbb{P}\left[\sum_{i=1}^{n} x_i S_i \le \|\boldsymbol{x}_n\|_1\right] && (162)\\
&\ge \inf_{\boldsymbol{y}\in\mathbb{R}_+^n : \|\boldsymbol{y}\|_1 = \|\boldsymbol{x}_n\|_1} \mathbb{P}\left[\sum_{i=1}^{n} y_i S_i \le \|\boldsymbol{x}_n\|_1\right] && (163)\\
&= \mathbb{P}\left[n^{-1}\|\boldsymbol{x}_n\|_1 \sum_{i=1}^{n} S_i \le \|\boldsymbol{x}_n\|_1\right] && (164)\\
&> \frac{1}{2}. && (165)
\end{aligned}$$

Here, (164) follows from (148); (165) follows because $\sum_{i=1}^{n} S_i$ is chi-squared distributed, and because the median of a chi-squared distribution is smaller than its mean [24, Ch. 17].

We next prove (161) for the case $t < 0$. By definition, $L_n(\boldsymbol{x})$ has zero mean and unit variance. Moreover, by Lemma 12 the pdf $f_{L_n(\boldsymbol{x})}$ of $L_n(\boldsymbol{x})$ is log-concave. Hence, we have that [35, Lemma 5.5] [36, Proposition 2.1]

$$\sup_{t\in\mathbb{R}} f_{L_n(\boldsymbol{x})}(t) \le 1. \tag{166}$$

Then, the bound (161) holds because

$$\begin{aligned}
F_{L_n(\boldsymbol{x})}(t) &= \underbrace{\int_{-\infty}^{0} f_{L_n(\boldsymbol{x})}(y)dy}_{\ge 1/2} - \int_t^0 \underbrace{f_{L_n(\boldsymbol{x})}(y)}_{\le 1} dy && (167)\\
&\ge \frac{1}{2} + t\,. && (168)
\end{aligned}$$

The last step follows from (165) and (166). ■

Consider the random variable obtained by summing finitely many independent but not necessarily identically distributed exponential random variables. The next lemma establishes that the derivative of the pdf of the resulting random variable, computed at the mean value, is negative. Since the convolution of exponential distributions is unimodal, this implies that the mode of this random variable is smaller than its mean, i.e., its probability distribution is right skewed.

Lemma 15: Let $m \in \mathbb{N}$, let $a_1, \ldots, a_m$ be positive real numbers, and let $S_1, \ldots, S_m$ be i.i.d. Exp(1)-distributed random variables. Furthermore, let $\mu \triangleq \sum_{i=1}^{m} a_i$, $a_{\min} \triangleq \min_i\{a_i\}$, $a_{\max} \triangleq \max_i\{a_i\}$, and $A \triangleq \sum_{i=1}^{m} a_i S_i$. Then,

$$f_A'(\mu) \le -\frac{a_{\min}}{a_{\max}}\frac{f_A(\mu)}{\mu} < 0 \tag{169}$$

where f'_A denotes the derivative of the pdf of A. Moreover, the first inequality in (169) holds with equality if and only if $a_1 = \cdots = a_m$.

Proof: Note that the $\{S_i\}$, $i = 1, \ldots, m$, have the same distribution as $\{X_i^2 + X_{m+i}^2\}$, $i = 1, \ldots, m$, where $\{X_i\}$, $i = 1, \ldots, 2m$, are i.i.d. $\mathcal{N}(0, 1/2)$-distributed. Let $a_{m+i} \triangleq a_i$, $i = 1, \ldots, m$. Then, A has the same distribution as

$$\widetilde{A} \triangleq \sum_{i=1}^{2m} a_i X_i^2. \tag{170}$$

Next, we prove that $f'_{\widetilde{A}}(\mu) < 0$ by using [18, Lemma 22], which provides expressions for the pdf and the derivative of the pdf of functions of random variables. We first give some definitions. Let $\boldsymbol{X} \triangleq [X_1, \ldots, X_{2m}]$, and let $f_{\boldsymbol{X}}$ denote the joint pdf of $X_1, \ldots, X_{2m}$. Let $\varphi(\boldsymbol{x}) : \mathbb{R}^{2m} \to \mathbb{R}_+$ be defined as

$$\varphi(\boldsymbol{x}) \triangleq \sum_{i=1}^{2m} a_i x_i^2. \tag{171}$$

Let $\nabla\varphi$ and $\Delta\varphi$ be the gradient and Laplacian of φ, namely,

$$\nabla\varphi(\boldsymbol{x}) \triangleq \left[\frac{\partial}{\partial x_1}\varphi(\boldsymbol{x}), \ldots, \frac{\partial}{\partial x_{2m}}\varphi(\boldsymbol{x})\right] \tag{172}$$

and

$$\Delta\varphi(\boldsymbol{x}) \triangleq \sum_{i=1}^{2m} \frac{\partial^2}{\partial x_i^2}\varphi(\boldsymbol{x}). \tag{173}$$

Finally, let $\varphi^{-1}(\mu)$ denote the preimage $\{\boldsymbol{x} \in \mathbb{R}^{2m} : \varphi(\boldsymbol{x}) = \mu\}$, and let $\mathrm{d}S$ be the surface area form on $\varphi^{-1}(\mu)$, chosen so that $\mathrm{d}S(\nabla\varphi) > 0$. Note that $f_{\boldsymbol{X}}$ is smooth and that the set $\varphi^{-1}(\mu)$ is bounded. Moreover, for every $\boldsymbol{x} \in \varphi^{-1}(\mu)$

$$\|\nabla\varphi(\boldsymbol{x})\|_2^2 = \sum_{i=1}^{2m} 4a_i^2 x_i^2 \geq 4\mu \min_{i=1,\ldots,m}\{a_i\} > 0. \tag{174}$$

Then, by [18, Eq. (407)],

$$f'_{\widetilde{A}}(\mu) = \int_{\varphi^{-1}(\mu)} \psi \frac{\mathrm{d}S}{\|\nabla\varphi\|_2} \tag{175}$$

where [18, Eq. (422)]

$$\psi \triangleq \frac{\langle \nabla f_{\boldsymbol{X}}, \nabla\varphi\rangle + f_{\boldsymbol{X}} \cdot \Delta\varphi}{\|\nabla\varphi\|_2^2} - \frac{f_{\boldsymbol{X}}\langle \nabla\|\nabla\varphi\|_2^2, \nabla\varphi\rangle}{\|\nabla\varphi\|_2^4}. \tag{176}$$

The first term on the RHS of (176) is equal to zero. Indeed,

$$\begin{aligned}
&\langle \nabla f_{\boldsymbol{X}}, \nabla\varphi\rangle + f_{\boldsymbol{X}} \cdot \Delta\varphi \\
&= \sum_{i=1}^{2m} -2x_i f_{\boldsymbol{X}} \cdot (2a_i x_i) + f_{\boldsymbol{X}} \cdot \sum_{i=1}^{2m} 2a_i && (177)\\
&= 4 f_{\boldsymbol{X}} \left(\sum_{i=1}^{m} a_i - \sum_{i=1}^{2m} a_i x_i^2\right) && (178)\\
&= 0. && (179)
\end{aligned}$$

Here, the last step follows because for every $\boldsymbol{x} \in \varphi^{-1}(\mu)$

$$\sum_{i=1}^{2m} a_i x_i^2 = \mu = \sum_{i=1}^{m} a_i. \tag{180}$$

The second term on the RHS of (176) can be computed as follows:

$$\begin{aligned}
\frac{f_{\boldsymbol{X}}\langle \nabla\|\nabla\varphi\|_2^2, \nabla\varphi\rangle}{\|\nabla\varphi\|_2^4} &= f_{\boldsymbol{X}} \frac{16\sum_{i=1}^{2m} a_i^3 x_i^2}{\left(\sum_{i=1}^{2m} 4a_i^2 x_i^2\right)^2} && (181)\\
&\geq f_{\boldsymbol{X}} \frac{a_{\min}\sum_{i=1}^{2m} a_i^2 x_i^2}{a_{\max}\mu \sum_{i=1}^{2m} a_i^2 x_i^2} && (182)\\
&= \frac{a_{\min}}{a_{\max}} \frac{f_{\boldsymbol{X}}}{\mu}. && (183)
\end{aligned}$$

Note that the inequality on the RHS of (182) holds with equality if and only if $a_1 = \cdots = a_m$. Finally, using (179) and (183) in (175) we conclude that

$$f'_{\widetilde{A}}(\mu) \leq -\int_{\varphi^{-1}(\mu)} \frac{a_{\min}}{a_{\max}} \frac{f_{\boldsymbol{X}}}{\mu} \frac{\mathrm{d}S}{\|\nabla\varphi\|_2} = -\frac{a_{\min}}{a_{\max}} \frac{f_{\widetilde{A}}(\mu)}{\mu}. \tag{184}$$

Here, the last step follows from [18, Lemma 22]. The second inequality in (169) follows because $f_{\widetilde{A}}(\mu) > 0$ (see [22, Lemma 3]). ■

Appendix III
Proof of Theorem 8

A. Achievability

To prove that (63) is achievable, we start from the inequality

$$M - 1 \geq \frac{\tau}{\beta_{1-\epsilon+\tau}(P_{\mathbb{Y}\,|\,\boldsymbol{X}=\boldsymbol{c}_1}, P_{\mathbb{Y}\,|\,\boldsymbol{X}=\boldsymbol{0}})} \tag{185}$$

which is equivalent to Theorem 1 (see (25) for a definition of $\boldsymbol{c}_1$). First, we upper-bound $\beta_{1-\epsilon+\tau}(P_{\mathbb{Y}\,|\,\boldsymbol{X}=\boldsymbol{c}_1}, P_{\mathbb{Y}\,|\,\boldsymbol{X}=\boldsymbol{0}})$ as [7, Eq. (103)]

$$\beta_{1-\epsilon+\tau}(P_{\mathbb{Y}\,|\,\boldsymbol{X}=\boldsymbol{c}_1}, P_{\mathbb{Y}\,|\,\boldsymbol{X}=\boldsymbol{0}}) \leq \xi^{-1} \tag{186}$$

where $\xi > 0$ satisfies

$$P_{\mathbb{Y}\,|\,\boldsymbol{X}=\boldsymbol{c}_1}[\imath(\boldsymbol{c}_1, \mathbb{Y}) \leq \log\xi] = \epsilon - \tau \tag{187}$$

and $\imath(\cdot,\cdot)$ was defined in (38). The LHS of (187) can be lower-bounded as follows:

$$\begin{aligned}
&P_{\mathbb{Y}\,|\,\boldsymbol{X}=\boldsymbol{c}_1}[\imath_{\boldsymbol{X},\mathbb{Y}}(\boldsymbol{c}_1, \mathbb{Y}) \leq \log\xi] && (188)\\
&= \mathbb{P}\left[-m_{\mathrm{r}}N\log\left(1 + \frac{E}{N}\right) + \frac{E}{N}\sum_{i=1}^{m_{\mathrm{r}}N} S_i \log e \leq \log\xi\right] && (189)\\
&\geq Q\left(-\frac{\log\xi + m_{\mathrm{r}}N\log(1 + E/N) - m_{\mathrm{r}}E\log e}{\sqrt{m_{\mathrm{r}}N}\cdot(E/N)\log e}\right) - \frac{\mathrm{const}}{\sqrt{N}}. && (190)
\end{aligned}$$

Here, const denotes a positive constant[6] independent of E and N, (189) follows from (47), and (190) follows from the Berry-Esseen Theorem (see, e.g., [23, Ch. XVI.5]).

Next, we set $\tau = 1/\sqrt{E}$ in (187) and consider the asymptotic regime $E \to \infty$. We shall choose N as a function of E so

[6]Throughout the remainder of the paper, we will use const to denote an arbitrary constant whose exact value is irrelevant for the analysis. Its value may change at each appearance.

that $N \to \infty$ as $E \to \infty$ with $N/E \to 0$. Substituting (190) into (187), and solving for $\log \xi$ we obtain

$$\begin{aligned}\log \xi &\geq m_{\mathrm{r}} E \log e - m_{\mathrm{r}} N \log\left(1+\frac{E}{N}\right) \\ &\quad - \frac{\sqrt{m_{\mathrm{r}}} E \log e}{\sqrt{N}} Q^{-1}\left(\epsilon - \frac{1}{\sqrt{E}} + \frac{\mathrm{const}}{\sqrt{N}}\right) \qquad (191)\\ &= m_{\mathrm{r}} E \log e - m_{\mathrm{r}} N \log\left(1+\frac{E}{N}\right) \\ &\quad - \frac{\sqrt{m_{\mathrm{r}}} E \log e}{\sqrt{N}} Q^{-1}(\epsilon) + \mathcal{O}\left(\left(\frac{-1}{\sqrt{E}} + \frac{\mathrm{const}}{\sqrt{N}}\right)\frac{E}{\sqrt{N}}\right) \qquad (192)\\ &= m_{\mathrm{r}} E \log e - m_{\mathrm{r}} N \log\left(1+\frac{E}{N}\right) \\ &\quad - \frac{\sqrt{m_{\mathrm{r}}} E \log e}{\sqrt{N}} Q^{-1}(\epsilon) + \mathcal{O}\left(\frac{E}{N}\right). \qquad (193)\end{aligned}$$

Here, (192) follows by operating a Taylor-expansion of $Q^{-1}(\cdot)$ around ϵ, and (193) follows because $N/E \to 0$.

We next maximize the dominant terms on the RHS of (193) by choosing

$$\begin{aligned}N = N^* \triangleq \arg\min_{N\in\mathbb{N}} \Bigg\{ & m_{\mathrm{r}} N \log\left(1+\frac{E}{N}\right) \\ & + \frac{\sqrt{m_{\mathrm{r}}} E \log e}{\sqrt{N}} Q^{-1}(\epsilon)\Bigg\}. \qquad (194)\end{aligned}$$

After some algebraic computations, we obtain

$$N^* = \frac{1}{m_{\mathrm{r}}}\left(\frac{3}{2} Q^{-1}(\epsilon) \frac{(m_{\mathrm{r}} E)\log e}{\log(m_{\mathrm{r}} E)}\right)^{2/3} + \mathcal{O}\left(\frac{E^{2/3}\log\log E}{(\log E)^{5/3}}\right). \qquad (195)$$

Substituting (195) into (193), then (193) into (186), and finally (186) into (32) we conclude that

$$\begin{aligned}&\log M^*(E,\epsilon) \\ &\geq m_{\mathrm{r}} E \log e - V_0 \cdot \left(m_{\mathrm{r}} E Q^{-1}(\epsilon)\right)^{2/3} \left(\log(m_{\mathrm{r}} E)\right)^{1/3} \\ &\quad + \mathcal{O}\left(\frac{E^{2/3}\log\log E}{(\log E)^{2/3}}\right) \qquad (196)\end{aligned}$$

where V_0 is given in (5).

B. Converse

It follows from (61) that for every $\eta \in \mathbb{R}$

$$\begin{aligned}&\log M^*(E,\epsilon) \leq \eta \\ &\quad - \log\left|\inf_{\boldsymbol{x}} \mathbb{P}\left[\sum_{i=1}^{\infty}\left(x_i S_i \log e - \log(1+x_i)\right) \leq \eta\right] - \epsilon\right|^+ \qquad (197)\end{aligned}$$

where the infimum is taken over all $\boldsymbol{x}$ that are of the form specified in (51) and (52).

Before proceeding to further bound (197), we introduce some notation. To every $\boldsymbol{x} \in \mathbb{R}_+^\infty$ satisfying $\|\boldsymbol{x}\|_1 = m_{\mathrm{r}} E$, we assign the random variable

$$L(\boldsymbol{x}) \triangleq \frac{1}{\|\boldsymbol{x}\|_2}\left(\sum_{i=1}^{\infty} x_i S_i - m_{\mathrm{r}} E\right). \qquad (198)$$

Let $F_{L(\boldsymbol{x})}(t)$ be the cdf of $L(\boldsymbol{x})$. By construction, $L(\boldsymbol{x})$ has zero mean and unit variance. Let $\hat{\eta}_E(\boldsymbol{x}) : \mathbb{R}_+^\infty \to \mathbb{R}$ be defined as follows:

$$\begin{aligned}\hat{\eta}_E(\boldsymbol{x}) \triangleq\ & m_{\mathrm{r}} E \log e - \sum_{i=1}^{\infty}\log(1+x_i) \\ & + F_{L(\boldsymbol{x})}^{-1}\left(\epsilon + E^{-1/2}\right)\|\boldsymbol{x}\|_2 \log e. \qquad (199)\end{aligned}$$

We shall choose η so that

$$\eta = \eta_E \triangleq \sup_{\boldsymbol{x}} \hat{\eta}_E(\boldsymbol{x}) \qquad (200)$$

where the supremum is again over all $\boldsymbol{x}$ that are of the form specified in (51) and (52). Substituting (200) into (197), we obtain

$$\begin{aligned}&\log M^*(E,\epsilon) \\ &\leq \sup_{\boldsymbol{x}} \hat{\eta}_E(\boldsymbol{x}) - \log\left|\inf_{\boldsymbol{x}} F_{L(\boldsymbol{x})}\left(F_{L(\boldsymbol{x})}^{-1}(\epsilon + E^{-1/2})\right) - \epsilon\right| \qquad (201)\\ &= \sup_{\boldsymbol{x}} \hat{\eta}_E(\boldsymbol{x}) + \frac{1}{2}\log E. \qquad (202)\end{aligned}$$

To conclude the proof, it remains to show that for every $\boldsymbol{x}$ that is of the form specified in (51) and (52)

$$\begin{aligned}\hat{\eta}_E(\boldsymbol{x}) \leq\ & m_{\mathrm{r}} E \log e - V_0 \cdot \left(m_{\mathrm{r}} E Q^{-1}(\epsilon)\right)^{2/3}\left(\log(m_{\mathrm{r}} E)\right)^{1/3} \\ & + \mathcal{O}\left(\frac{E^{2/3}\log\log E}{(\log E)^{2/3}}\right). \qquad (203)\end{aligned}$$

To this end, we consider the following three cases separately.

1) The vector $\boldsymbol{x}$ takes the form (52), and $\widetilde{N}_2 > E^{1/6}$;
2) The vector $\boldsymbol{x}$ takes the form (51);
3) The vector $\boldsymbol{x}$ takes the form (52), and $\widetilde{N}_2 \leq E^{1/6}$.

Case 1: By assumption, $\boldsymbol{x}$ has at most two distinct nonzero entries $0 \leq \tilde{q}_1 \leq \tilde{q}_2$, and $\widetilde{N}_2 \geq E^{1/6}$. Suppose that we can approximate $F_{L(\boldsymbol{x})}^{-1}\left(\epsilon + E^{-1/2}\right)$ by $-Q^{-1}(\epsilon)$ in the limit $E \to \infty$ (in a sense we shall make precise later on). The proof is then concluded by using the result in Lemma 16 below, together with (194) and (195), in (202).

Lemma 16: For every positive constant a, we have that

$$\begin{aligned}&\inf_{\boldsymbol{x}\in\mathbb{R}_+^\infty:\|\boldsymbol{x}\|_1 = m_{\mathrm{r}} E} \sum_{i=1}^{\infty}\log(1+x_i) + a\|\boldsymbol{x}\|_2 \\ &\qquad = \min_{N\in\mathbb{N}} N\log\left(1+\frac{m_{\mathrm{r}} E}{N}\right) + a\frac{m_{\mathrm{r}} E}{\sqrt{N}}. \qquad (204)\end{aligned}$$

Proof: See Appendix III-C. ■

It remains to show that we can indeed approximate $F_{L(\boldsymbol{x})}^{-1}\left(\epsilon + E^{-1/2}\right)$ by $-Q^{-1}(\epsilon)$. Since $L(\boldsymbol{x})$ is the normalized sum of $\widetilde{N}_1 + \widetilde{N}_2$ independent random variables, and $\widetilde{N}_2 \to \infty$ as $E \to \infty$, it is natural to use the central-limit theorem to establish this result. More precisely, we apply the Berry-Esseen Theorem [23, Ch. XVI.5] to $F_{L(\boldsymbol{x})}(\cdot)$ and obtain that, for an arbitrary $\xi \in \mathbb{R}$,

$$\begin{aligned}&F_{L(\boldsymbol{x})}(\xi) \\ &= \mathbb{P}\left[\frac{1}{\|\boldsymbol{x}\|_2}\left(\tilde{q}_1\sum_{i=1}^{\widetilde{N}_1} S_i + \tilde{q}_2\sum_{i=1}^{\widetilde{N}_2} S_{i+\widetilde{N}_1} - m_{\mathrm{r}} E\right) \leq \xi\right] \qquad (205)\\ &\geq Q(-\xi) - \frac{\mathrm{const}\left(\widetilde{N}_1(\tilde{q}_1)^3 + \widetilde{N}_2(\tilde{q}_2)^3\right)}{\left(\widetilde{N}_1(\tilde{q}_1)^2 + \widetilde{N}_2(\tilde{q}_2)^2\right)^{3/2}}. \qquad (206)\end{aligned}$$

The second term on the RHS of (206) can be evaluated as follows

$$\frac{\widetilde{N}_1(\tilde{q}_1)^3+\widetilde{N}_2(\tilde{q}_2)^3}{\left(\widetilde{N}_1(\tilde{q}_1)^2+\widetilde{N}_2(\tilde{q}_2)^2\right)^{3/2}} \leq \frac{\tilde{q}_2}{\left(\widetilde{N}_1(\tilde{q}_1)^2+\widetilde{N}_2(\tilde{q}_2)^2\right)^{1/2}} \tag{207}$$

$$\leq \widetilde{N}_2^{-1/2} \tag{208}$$

$$\leq E^{-1/12}. \tag{209}$$

Here, (207) follows because $(\tilde{q}_1)^3 \leq (\tilde{q}_1)^2\tilde{q}_2$, and in (209) we used that $\widetilde{N}_2 > E^{\frac{1}{6}}$. Using (209) in (206), selecting ξ such that the LHS of (205) equals $\epsilon + E^{-1/2}$, and using that the function $Q(\cdot)$ is monotonically decreasing, we conclude that

$$\xi = F^{-1}_{L(\boldsymbol{x})}\left(\epsilon + E^{-1/2}\right) \tag{210}$$

$$\leq -Q^{-1}\left(\epsilon + E^{-1/2} + \text{const}\cdot E^{-1/12}\right) \tag{211}$$

$$= -Q^{-1}(\epsilon) + \mathcal{O}\left(E^{-1/12}\right). \tag{212}$$

Here, (212) follows by applying Taylor's theorem to $Q^{-1}(\cdot)$ around ϵ.

Case 2: By assumption, $\boldsymbol{x}$ contains three distinct nonzero entries $0 < q_1 < q_2 < q_3$, and q_1 and q_3 each appear only once. For this case, we shall use a different approach from that used in Case 1. The main differences between the two cases are as follows:

- In order to use the central limit theorem, we need to show that the $\boldsymbol{x}$ that maximizes $\hat{\eta}_E(\boldsymbol{x})$ contains sufficiently many nonzero entries, and that the available energy $m_{\mathrm{r}}E$ is spread evenly over these nonzero entries as $E \to \infty$. These properties are satisfied in Case 1 by definition. In Case 2, however, we need to verify that they hold.
- Intuitively, since q_1 and q_3 appear only once in $\boldsymbol{x}$, we expect that they do not contribute to the dominant terms in (202). As a result, we can approximate the second and the third term on the RHS of (202) directly without using Lemma 16.

We proceed now with the proof. The idea is to upper-bound (202) using (159) (Lemma 14 in Appendix II), and then compare the resulting bound with the achievability result (196). Since $0 < \epsilon < 1/2$, and since we are interested in the asymptotic regime $E \to \infty$, we can assume without loss of generality that $\epsilon + E^{-1/2} < 1/2$. Applying (159) to (199), we obtain

$$\hat{\eta}_E(\boldsymbol{x}) \leq m_{\mathrm{r}}E\log e - \sum_{i=1}^{\infty}\log(1+x_i) - \left(1/2 - \epsilon - E^{-1/2}\right)\|\boldsymbol{x}\|_2 \log e + \mathcal{O}(\log E). \tag{213}$$

Since we are interested in upper-bounding $\sup_{\boldsymbol{x}} \hat{\eta}_E(\boldsymbol{x})$, we focus without loss of generality on the $\boldsymbol{x}$ for which $\hat{\eta}_E(\boldsymbol{x})$ is greater than the RHS of (196). By comparing (213) with (196), we conclude that such $\boldsymbol{x}$ must satisfy

$$\|\boldsymbol{x}\|_2 \leq \frac{V_0\cdot\left(Q^{-1}(\epsilon)\right)^{2/3}}{(1/2-\epsilon)\log e}\left(m_{\mathrm{r}}E\right)^{2/3}\left(\log(m_{\mathrm{r}}E)\right)^{1/3} + o\left(E^{2/3}\right) \tag{214}$$

and

$$\sum_{i=1}^{\infty}\log(1+x_i) \leq V_0\cdot\left(m_{\mathrm{r}}EQ^{-1}(\epsilon)\right)^{2/3}\left(\log(m_{\mathrm{r}}E)\right)^{1/3} + o\left(E^{2/3}\right). \tag{215}$$

We next refine the bounds (214) and (215) by exploiting that $\boldsymbol{x}$ is of the form specified in (51). By (214) and (51), we have the following estimates

$$q_3 = \|\boldsymbol{x}\|_\infty \leq \|\boldsymbol{x}\|_2 \leq \mathcal{O}\left(E^{2/3}\left(\log E\right)^{1/3}\right) \tag{216}$$

and

$$N+2 \geq \frac{\|\boldsymbol{x}\|_1^2}{\|\boldsymbol{x}\|_2^2} \tag{217}$$

$$\geq \text{const}\cdot E^{2/3}\left(\log E\right)^{-2/3}. \tag{218}$$

Here, (217) follows because $\boldsymbol{x}$ has $N+2$ nonzero entries and because $\|\boldsymbol{a}\|_1 \leq \sqrt{N+2}\|\boldsymbol{a}\|_2$ for every $(N+2)$-dimensional real vector $\boldsymbol{a}$; in (218) we used (214) and that $\|\boldsymbol{x}\|_1 = m_{\mathrm{r}}E$. Since $q_1 + q_2N + q_3 = m_{\mathrm{r}}E$, it follows from (218) that

$$q_1 \leq q_2 \leq \frac{m_{\mathrm{r}}E}{N} \leq \mathcal{O}\left(E^{1/3}\left(\log E\right)^{2/3}\right). \tag{219}$$

The bound (215) implies that

$$V_0\cdot\left(m_{\mathrm{r}}EQ^{-1}(\epsilon)\right)^{2/3}\left(\log(m_{\mathrm{r}}E)\right)^{1/3} + o\left(E^{2/3}\right) \geq \sum_{i=1}^{\infty}\log(1+x_i) \tag{220}$$

$$\geq N\log(1+q_2) \tag{221}$$

$$= N\log\left(1+\frac{m_{\mathrm{r}}E-q_1-q_3}{N}\right) \tag{222}$$

$$\geq N\log\left(1+\frac{m_{\mathrm{r}}E-\mathcal{O}\left(E^{2/3}\left(\log E\right)^{1/3}\right)}{N}\right). \tag{223}$$

Here, in (223) we used (216) and (219). Solving (223) for N, we obtain

$$N \leq \text{const}\cdot E^{2/3}\left(\log E\right)^{-2/3}. \tag{224}$$

Using (218) and (224) back in (223) we obtain

$$\sum_{i=1}^{\infty}\log(1+x_i) \geq N\log\left(1+\frac{m_{\mathrm{r}}E}{N}\right) + N\log\left(1-\mathcal{O}\left(E^{-1/3}\left(\log E\right)^{1/3}\right)\right) \tag{225}$$

$$= N\log\left(1+\frac{m_{\mathrm{r}}E}{N}\right) + \mathcal{O}\left(E^{1/3}\left(\log E\right)^{-1/3}\right). \tag{226}$$

Here, the last step follows by Taylor-expanding the log function in the second term on the RHS of (228) around 1.

We are now ready to provide a refined estimate for the term $F^{-1}_{L(\boldsymbol{x})}\left(\epsilon + E^{-1/2}\right)\|\boldsymbol{x}\|_2$ on the RHS of (202). Let

$$\boldsymbol{x}' \triangleq \Big[\underbrace{\frac{m_{\mathrm{r}}E}{N+2},\ldots,\frac{m_{\mathrm{r}}E}{N+2}}_{N+2},0,\ldots\Big]. \tag{227}$$

By Lemma 13 (see Appendix II) and by (198), the following inequality holds for every $\gamma \in (0, m_{\mathrm{r}}E]$:

$$F_{L(\boldsymbol{x})}\left(\frac{\gamma - m_{\mathrm{r}}E}{\|\boldsymbol{x}\|_2}\right) = \mathbb{P}\Big[q_1 S_1 + \sum_{i=2}^{N+1} q_2 S_i + q_3 S_{N+2} \le \gamma\Big] \tag{228}$$

$$\ge \mathbb{P}\Big[\frac{m_{\mathrm{r}}E}{N+2}\sum_{i=1}^{N+2} S_i \le \gamma\Big] \tag{229}$$

$$= F_{L(\boldsymbol{x}')}\left(\frac{\gamma - m_{\mathrm{r}}E}{\|\boldsymbol{x}'\|_2}\right). \tag{230}$$

Since $\epsilon + E^{-1/2} < 1/2$ and since, by Lemma 14 (see Appendix II), $F_{L(\boldsymbol{x}')}(0) \ge 1/2$, we have $F^{-1}_{L(\boldsymbol{x}')}\big(\epsilon + E^{-1/2}\big) < 0$. Set $\gamma = m_{\mathrm{r}}E + F^{-1}_{L(\boldsymbol{x}')}\big(\epsilon + E^{-1/2}\big)\|\boldsymbol{x}'\|_2 < m_{\mathrm{r}}E$. Then, by (230),

$$F^{-1}_{L(\boldsymbol{x})}\big(\epsilon + E^{-1/2}\big)\|\boldsymbol{x}\|_2 \le F^{-1}_{L(\boldsymbol{x}')}\big(\epsilon + E^{-1/2}\big)\|\boldsymbol{x}'\|_2. \tag{231}$$

Applying the Berry-Esseen central-limit theorem similarly as in (205)–(212), we obtain

$$F^{-1}_{L(\boldsymbol{x}')}\big(\epsilon + E^{-1/2}\big) \le -Q^{-1}(\epsilon) + \mathcal{O}\left(\frac{1}{\sqrt{N}}\right). \tag{232}$$

Furthermore,

$$\|\boldsymbol{x}'\|_2 = \frac{m_{\mathrm{r}}E}{\sqrt{N+2}} \tag{233}$$

$$= \frac{m_{\mathrm{r}}E}{\sqrt{N}}\left(1 + \mathcal{O}\left(\frac{1}{N}\right)\right). \tag{234}$$

Substituting (232) and (234) into (231) and using (218) and (224), we obtain

$$F^{-1}_{L(\boldsymbol{x})}\big(\epsilon + E^{-1/2}\big)\|\boldsymbol{x}\|_2 \le -\frac{m_{\mathrm{r}}E}{\sqrt{N}}Q^{-1}(\epsilon) + \mathcal{O}\Big(E^{1/3}\big(\log E\big)^{2/3}\Big). \tag{235}$$

Finally, substituting (226) and (235) into (202), we conclude that

$$\hat{\eta}_E(\boldsymbol{x}) \le m_{\mathrm{r}}E\log e - N\log\left(1 + \frac{m_{\mathrm{r}}E}{N}\right) - \frac{m_{\mathrm{r}}E\log e}{\sqrt{N}}Q^{-1}(\epsilon) + \mathcal{O}\Big(E^{1/3}\big(\log E\big)^{-1/3}\Big). \tag{236}$$

The proof is completed by maximizing the RHS of (236) over $N \in \mathbb{N}$ and by using (194) and (195).

Case 3: By assumption, $\boldsymbol{x}$ has at most two different nonzero entries $0 \le \tilde{q}_1 \le \tilde{q}_2$, and $\widetilde{N}_2 \le E^{1/6}$. Since the multiplicity of q_2 in $\boldsymbol{x}$ is less than $E^{1/6}$, it can be shown that all entries of $\boldsymbol{x}$ that are equal to $\tilde{q}_2$ do not contribute to the dominant terms in (202). The analysis follows steps similar to the ones for Case 2.

C. Proof of Lemma 16

Let

$$l_a(\boldsymbol{x}) \triangleq \sum_{i=1}^{\infty}\log(1 + x_i) + a\|\boldsymbol{x}\|_2 \tag{237}$$

with x_i standing for the ith entry of $\boldsymbol{x}$, and let $\boldsymbol{x}^*$ be a minimizer of

$$\inf_{\boldsymbol{x}\in\mathbb{R}_+^{\infty}:\|\boldsymbol{x}\|_1 = m_{\mathrm{r}}E} l_a(\boldsymbol{x}). \tag{238}$$

In order to prove Lemma 16, it suffices to show that all nonzero entries of $\boldsymbol{x}^*$ must take the same value. This is proved by contradiction.

Assume that there exist indices i, j for which $0 < x_i^* < x_j^*$. Let $b \triangleq x_i^* + x_j^*$, $c \triangleq \sum_{k\ne i, k\ne j}^{n}(x_k^*)^2$, and $d \triangleq \sum_{k\ne i, k\ne j}^{n}\log(1 + x_k^*)$. Consider now the function $f : [0, b] \to \mathbb{R}$ defined as

$$f(t) \triangleq \log(1+t) + \log(1+b-t) + a\sqrt{c + t^2 + (b-t)^2} + d. \tag{239}$$

Note that $f(t)$ is symmetric around $t = b/2$, and that $f(x_i^*) = f(x_j^*) = l_a(\boldsymbol{x}^*)$.

Standard computations reveal that the minimum of $f(t)$ over $[0, b/2]$ is achieved at one of the boundary points, i.e.,

$$f(t) > \min\{f(0), f(b/2)\}, \quad \text{for all } t \in (0, b/2). \tag{240}$$

Let $\boldsymbol{x}_1$ (resp. $\boldsymbol{x}_2$) be the vector obtained from $\boldsymbol{x}^*$ by replacing the ith and jth entries with 0 (resp. $b/2$) and b (resp. $b/2$), respectively. Clearly, $\|\boldsymbol{x}_1\|_1 = \|\boldsymbol{x}_2\|_1 = m_{\mathrm{r}}E$. Then, (240) implies that

$$l_a(\boldsymbol{x}^*) > \min\{l_a(\boldsymbol{x}_1), l_a(\boldsymbol{x}_2)\}. \tag{241}$$

This contradicts the assumption that $\boldsymbol{x}^*$ is a minimizer. Therefore, the entries of $\boldsymbol{x}^*$ cannot take more than one distinct nonzero values.

Appendix IV
Proof of Theorem 10

The achievability of (77) follows from Theorem 9 and [8, Th. 3]. Next, we prove a converse. As in the proof of Theorem 6, we assume without loss of generality that each codeword U^{∞} for the channel (12) satisfies the equal-energy constraint

$$\|\mathsf{U}^{\infty}\|_{\mathsf{F}}^2 = E. \tag{242}$$

Let $P_{\mathbb{V}^{\infty}\mathbb{H}^{\infty}|\mathbb{U}^{\infty}} \triangleq P_{\mathbb{H}^{\infty}}P_{\mathbb{V}^{\infty}|\mathbb{U}^{\infty}\mathbb{H}^{\infty}}$. By the meta-converse theorem [7, Th. 31] applied with $Q_{\mathbb{V}^{\infty}\mathbb{H}^{\infty}} = P_{\mathbb{V}^{\infty}\mathbb{H}^{\infty}|\mathbb{U}^{\infty}=\mathbf{0}}$, we obtain

$$\frac{1}{M^*(E,\epsilon)} \ge \inf_{\mathsf{U}^{\infty}} \beta_{1-\epsilon}(P_{\mathbb{V}^{\infty}\mathbb{H}^{\infty}|\mathbb{U}^{\infty}=\mathsf{U}^{\infty}}, Q_{\mathbb{V}^{\infty}\mathbb{H}^{\infty}}). \tag{243}$$

Here, the infimum in (243) is over all matrices $\mathsf{U}^{\infty} \in \mathbb{C}^{\infty\times m_{\mathrm{t}}}$ that satisfy $\|\mathsf{U}^{\infty}\|_{\mathsf{F}}^2 = E$. Proceeding similarly to the proof of Theorem 6, we observe that the RHS of (243) does not change if we focus on diagonal input matrices. This implies that for the purpose of evaluating (243), the MIMO Rayleigh block-fading channel (12) is equivalent to the memoryless SIMO Rayleigh-fading channel (19). Let now $\boldsymbol{u}$ and $(\mathbb{V}, \mathbb{H})$ denote the input and the output of this SIMO channel, respectively. Then, the RHS of (243) is equal to

$$\inf_{\boldsymbol{u}\in\mathbb{C}^{\infty}:\|\boldsymbol{u}\|_2^2 = E} \beta_{1-\epsilon}(P_{\mathbb{V}\mathbb{H}|\boldsymbol{U}=\boldsymbol{u}}, Q_{\mathbb{V}\mathbb{H}}) \tag{244}$$

where $P_{\mathbb{VH}\,|\,\boldsymbol{U}=\boldsymbol{u}}$ denotes the conditional probability distribution of the output of the channel (19) given the input, and $Q_{\mathbb{VH}} = P_{\mathbb{VH}\,|\,\mathbb{U}=\mathbf{0}}$. Substituting (244) into (243), and using the lower bound [7, Eq. (102)], we obtain that for every $\eta > 0$,

$$\log M^*(E,\epsilon) \le \eta \log e - \log\left|\inf_{\boldsymbol{u}} P_{\mathbb{VH}|\boldsymbol{U}=\boldsymbol{u}}\left[\log \frac{dP_{\mathbb{VH}|\boldsymbol{U}=\boldsymbol{u}}}{dQ_{\mathbb{VH}}}(\mathbb{V},\mathbb{H}) \le \eta \log e\right] - \epsilon\right|^+. \tag{245}$$

Here, the infimum on the RHS of (245) is over all $\boldsymbol{u} \in \mathbb{C}^\infty$ that satisfy $\|\boldsymbol{u}\|_2^2 = E$. Under $P_{\mathbb{VH}\,|\,\boldsymbol{U}=\boldsymbol{u}}$, the random variable $\log \frac{dP_{\mathbb{VH}\,|\,\boldsymbol{U}=\boldsymbol{u}}}{dQ_{\mathbb{VH}}}(\mathbb{V},\mathbb{H})$ in (245) has the same distribution as

$$\log e\left(\sum_{r=1}^{m_\mathrm{r}}\sum_{i=1}^{\infty}|u_i H_{r,i}|^2 + \left(2\sum_{r=1}^{m_\mathrm{r}}\sum_{i=1}^{\infty}|u_i H_{r,i}|^2\right)^{1/2} Z\right) \tag{246}$$

where $Z \sim \mathcal{N}(0,1)$.

Let now $\epsilon_E \triangleq \epsilon + c_1\sqrt{E^{-1}\log E}$, where $c_1 > 0$ is an arbitrary constant. Since, by assumption, $0 < \epsilon < 1/2$, and since we are interested in the asymptotic behavior of $\log M^*(E,\epsilon)$ as $E \to \infty$, we can assume without loss of generality that $\epsilon_E < 1/2$. Set

$$\eta = m_\mathrm{r}E - \sqrt{2m_\mathrm{r}E}\,Q^{-1}(\epsilon_E). \tag{247}$$

Then, we can rewrite the minimization problem on the RHS of (245) using (246) and (247) as follows

$$\inf_{\substack{\boldsymbol{u}\in\mathbb{C}^\infty:\\ \|\boldsymbol{u}\|_2^2=E}} P_{\mathbb{VH}\,|\,\boldsymbol{U}=\boldsymbol{u}}\left[\log \frac{dP_{\mathbb{VH}\,|\,\boldsymbol{U}=\boldsymbol{u}}}{dQ_{\mathbb{VH}}}(\mathbb{V},\mathbb{H}) \le \eta\log e\right]$$

$$= \inf \mathbb{E}\left[Q\left(\frac{\sum_{r=1}^{m_\mathrm{r}}\sum_{i=1}^{\infty}|u_iH_{r,i}|^2 - m_\mathrm{r}E + \sqrt{2m_\mathrm{r}E}\,Q^{-1}(\epsilon_E)}{\left(2\sum_{r=1}^{m_\mathrm{r}}\sum_{i=1}^{\infty}|u_iH_i|^2\right)^{1/2}}\right)\right] \tag{248}$$

$$\triangleq q(E). \tag{249}$$

where the infimum on the RHS of (248) is over all $\boldsymbol{u} \in \mathbb{C}^\infty$ that satisfy $\|\boldsymbol{u}\|_2^2 = E$.

We next show that $q(E)$ admits the following large-E expansion:

$$q(E) = \inf_{\substack{\boldsymbol{u}\in\mathbb{C}^\infty:\\ \|\boldsymbol{u}\|_2^2=1}} \mathbb{P}\left[\sqrt{\frac{E}{2m_\mathrm{r}}}\left(\sum_{r=1}^{m_\mathrm{r}}\sum_{i=1}^{\infty}|u_iH_{r,i}|^2 - m_\mathrm{r}\right) \le Z - Q^{-1}(\epsilon_E)\right] + \mathcal{O}\left(\sqrt{\frac{\log E}{E}}\right). \tag{250}$$

The key step is to replace the term $\left(2\sum_{r=1}^{m_\mathrm{r}}\sum_{i=1}^{\infty}|u_iH_i|^2\right)^{1/2}$ in the denominator on the RHS of (248) by $\sqrt{2m_\mathrm{r}E}$. To this end, consider the function $t \mapsto Q((t-\eta)/\sqrt{2t})$ with η given in (247). If $t \le \eta - 2\sqrt{m_\mathrm{r}E\log E}$, we have

$$1 \ge Q\left(\frac{t-\eta}{\sqrt{2t}}\right) \tag{251}$$

$$\ge Q\left(\frac{t-\eta}{\sqrt{2m_\mathrm{r}E}}\right) \tag{252}$$

$$\ge Q\left(-\frac{2\sqrt{m_\mathrm{r}E\log E}}{\sqrt{2m_\mathrm{r}E}}\right) \tag{253}$$

$$= 1 - \mathcal{O}\left(E^{-1}\right). \tag{254}$$

Here, (252) follows because $Q(\cdot)$ is monotonically decreasing. The inequality (254) implies that, if $t \le \eta - 2\sqrt{m_\mathrm{r}E\log E}$, then

$$\left|Q\left(\frac{t-\eta}{\sqrt{2t}}\right) - Q\left(\frac{t-\eta}{\sqrt{2m_\mathrm{r}E}}\right)\right| \le \mathcal{O}(E^{-1}). \tag{255}$$

Proceeding similarly as in (251)–(254), we can show that (255) holds also if $t \ge \eta + 2\sqrt{m_\mathrm{r}E\log E}$. Finally, if $|t-\eta| < 2\sqrt{m_\mathrm{r}E\log E}$, by the mean-value theorem [37, p. 107] there exists an $a_0 \in \left[(t-\eta)/\sqrt{2t}, (t-\eta)/\sqrt{2m_\mathrm{r}E}\right]$ such that

$$\left|Q\left(\frac{t-\eta}{\sqrt{2t}}\right) - Q\left(\frac{t-\eta}{\sqrt{2m_\mathrm{r}E}}\right)\right|$$

$$= |Q'(a_0)|\left|\frac{t-\eta}{\sqrt{2t}} - \frac{t-\eta}{\sqrt{2m_\mathrm{r}E}}\right| \tag{256}$$

$$= \frac{1}{\sqrt{2\pi}}e^{-a_0^2/2}\left|\frac{t-\eta}{\sqrt{2m_\mathrm{r}E}}\right|\mathcal{O}\left(\sqrt{\frac{\log E}{E}}\right) \tag{257}$$

$$= \frac{1}{\sqrt{2\pi}}\underbrace{e^{-\frac{(t-\eta)^2}{4m_\mathrm{r}E}\cdot\left(1+\mathcal{O}\left(\sqrt{\frac{\log E}{E}}\right)\right)}\left|\frac{t-\eta}{\sqrt{2m_\mathrm{r}E}}\right|}_{\le\mathrm{const}}\mathcal{O}\left(\sqrt{\frac{\log E}{E}}\right) \tag{258}$$

$$= \mathcal{O}\left(\sqrt{\frac{\log E}{E}}\right). \tag{259}$$

Here, (257) and (258) follow because

$$\left|a_0 - \frac{t-\eta}{\sqrt{2m_\mathrm{r}E}}\right| \le \left|\frac{t-\eta}{\sqrt{2t}} - \frac{t-\eta}{\sqrt{2m_\mathrm{r}E}}\right| \tag{260}$$

$$= \left|\frac{t-\eta}{\sqrt{2m_\mathrm{r}E}}\right|\mathcal{O}\left(\sqrt{\frac{\log E}{E}}\right). \tag{261}$$

Combining (255) and (259), we conclude that for every $t \in (0,\infty)$

$$Q\left(\frac{t-\eta}{\sqrt{2t}}\right) = Q\left(\frac{t-\eta}{\sqrt{2m_\mathrm{r}E}}\right) + \mathcal{O}\left(\sqrt{\frac{\log E}{E}}\right) \tag{262}$$

where the $\mathcal{O}(\sqrt{(\log E)/E})$ term is uniform in t. This means that replacing the denominator in (249) with $\sqrt{2m_\mathrm{r}E}$ affects the value of (249) only by $\mathcal{O}\left(\sqrt{(\log E)/E}\right)$. Finally, we establish (250) by using (262) in (249) and by normalizing $\boldsymbol{u}$ in (249) with respect to E.

Lemma 17 below characterizes the solution of the optimization problem in (250).

Lemma 17: Fix an arbitrary $a > 0$, $b > 0$, and $m_\mathrm{r} \in \mathbb{N}$. Let $\{H_{r,i}\}$ be i.i.d. $\mathcal{CN}(0,1)$-distributed and let $Z \sim \mathcal{N}(0,1)$ be

independent of $\{H_{r,i}\}$. Then, we have

$$\inf_{\substack{\boldsymbol{u}\in\mathbb{C}^\infty:\\ \|\boldsymbol{u}\|_2^2=1}} \mathbb{P}\left[a\left(\sum_{r=1}^{m_\mathrm{r}}\sum_{i=1}^{\infty}|u_i H_{r,i}|^2 - m_\mathrm{r}\right) \le Z-b\right] = Q(b). \tag{263}$$

Proof: See Appendix IV-A. ■

Using Lemma 17 in (250), we obtain

$$q(E) = \epsilon_E + \mathcal{O}\left(\sqrt{\frac{\log E}{E}}\right). \tag{264}$$

Finally, substituting (264) and (247) into (245), we conclude that

$$\begin{aligned}\log M &\le m_\mathrm{r} E\log e - \sqrt{2m_\mathrm{r}E}\,Q^{-1}(\epsilon_E)\log e \\ &\quad - \log\left(\epsilon_E - \epsilon + \mathcal{O}\left(\sqrt{\frac{\log E}{E}}\right)\right) &(265)\\ &= m_\mathrm{r} E\log e - \sqrt{2m_\mathrm{r}E}\,Q^{-1}\left(\epsilon + c_1\sqrt{\frac{\log E}{E}}\right)\log e \\ &\quad - \log\left(c_1\sqrt{\frac{\log E}{E}} + \mathcal{O}\left(\sqrt{\frac{\log E}{E}}\right)\right) &(266)\\ &\le m_\mathrm{r} E\log e - \sqrt{2m_\mathrm{r}E}\,Q^{-1}(\epsilon)\log e \\ &\quad + \frac{1}{2}\log E + \mathcal{O}(\sqrt{\log E}). &(267)\end{aligned}$$

Here, the last step follows by Taylor-expanding $Q^{-1}(\cdot)$ around ϵ, and by taking c_1 so that

$$c_1\sqrt{\frac{\log E}{E}} + \mathcal{O}\left(\sqrt{\frac{\log E}{E}}\right) \ge \sqrt{\frac{\log E}{E}}. \tag{268}$$

This concludes the proof.

A. Proof of Lemma 17

First, consider the following sequence of vectors indexed by N:

$$\boldsymbol{u}^{(N)} \triangleq \frac{1}{\sqrt{N}}[\underbrace{1,\dots,1}_{N},0,\dots]. \tag{269}$$

Evaluating the probability on the LHS of (263) for this sequence of vectors, we establish the following upper bound

$$\begin{aligned}&\inf_{\substack{\boldsymbol{u}\in\mathbb{C}^\infty:\\ \|\boldsymbol{u}\|_2^2=1}} \mathbb{P}\left[a\left(\sum_{r=1}^{m_\mathrm{r}}\sum_{i=1}^{\infty}|u_i H_{r,i}|^2 - m_\mathrm{r}\right) \le Z-b\right] \\ &\le \lim_{N\to\infty}\mathbb{P}\left[a\left(\frac{1}{N}\sum_{r=1}^{m_\mathrm{r}}\sum_{i=1}^{N}|H_{r,i}|^2 - m_\mathrm{r}\right) \le Z-b\right] &(270)\\ &= Q(b). &(271)\end{aligned}$$

Here, the last step follows by the law of large numbers.

Next, we prove the reverse inequality. Suppose that for every $m\in\mathbb{N}$ and every $\boldsymbol{u}\in\mathbb{C}^m$ that satisfies $\|\boldsymbol{u}\|_2^2=1$, the following equality holds:

$$\inf_{a\ge 0}\mathbb{P}\left[a\left(\sum_{i=1}^{m}|u_i H_i|^2 - 1\right) \le Z-b\right] = Q(b). \tag{272}$$

Then,

$$\begin{aligned}&\inf_{\boldsymbol{u}\in\mathbb{C}^\infty:\|\boldsymbol{u}\|_2^2=1}\mathbb{P}\left[a\left(\sum_{r=1}^{m_\mathrm{r}}\sum_{i=1}^{\infty}|u_i H_{r,i}|^2 - m_\mathrm{r}\right) \le Z-b\right] &(273)\\ &= \inf_{\boldsymbol{u}}\mathbb{P}\left[m_\mathrm{r} a\left(\sum_{i=1}^{\infty}|u_i H_i|^2 - 1\right) \le Z-b\right] &(274)\\ &\ge \inf_{\boldsymbol{u}\in\mathbb{C}^\infty:\|\boldsymbol{u}\|_2^2=1}\mathbb{P}\left[m_\mathrm{r} a\left(\sum_{i=1}^{\infty}|u_i H_i|^2 - 1\right) \le Z-b\right] &(275)\\ &\ge \inf_{a\ge 0,\boldsymbol{u}\in\mathbb{C}^\infty:\|\boldsymbol{u}\|_2^2=1}\mathbb{P}\left[a\left(\sum_{i=1}^{\infty}|u_i H_i|^2 - 1\right) \le Z-b\right] &(276)\\ &= \lim_{m\to\infty}\inf_{\substack{a\ge 0,\boldsymbol{u}\in\mathbb{C}^m:\\ \|\boldsymbol{u}\|_2^2=1}}\mathbb{P}\left[a\left(\sum_{i=1}^{m}|u_i H_i|^2 - 1\right) \le Z-b\right] &(277)\\ &= Q(b). &(278)\end{aligned}$$

Here, the infimum on the RHS of (274) is over all vectors $\boldsymbol{u}\in\mathbb{C}^\infty$ that satisfy $\|\boldsymbol{u}\|_2^2=1$ and $u_{jm_\mathrm{r}+1}=\cdots=u_{(j+1)m_\mathrm{r}}, \forall j\in\mathbb{N}$. The equality (274) follows because $\{H_{r,i}\}$ are independent and identically distributed. This allows us to merge the double summation in (273) into one summation, provided that we account for the fact that each u_i must now multiply m_r successive $\{H_i\}$ (see the additional constraint on (274)). The inequality (275) follows by enlarging the feasible region of the minimization problem on the RHS of (274).

We next prove (272). Through standard algebraic manipulations, it can be verified that (272) holds when $m=1$. Fix now an arbitrary $m\ge 2$ and an arbitrary $\boldsymbol{u}\in\mathbb{C}^m$ that satisfies $\|\boldsymbol{u}\|_2^2=1$. Assume without loss of generality that all entries of $\boldsymbol{u}$ are positive (otherwise just set m to be the number of positive entries in $\boldsymbol{u}$). Let $B\triangleq\sum_{i=1}^m|u_i H_i|^2$, and let

$$g(a)\triangleq\mathbb{P}\big[a(B-1)\le Z-b\big] = \mathbb{E}\big[Q\big(aB-a+b\big)\big]. \tag{279}$$

Since $g(0)=Q(b)$, it suffices to show that $g(a)$ is nondecreasing on $[0,\infty)$, i.e., $g'(a)\ge 0$ for all $a\in[0,\infty)$. The derivative $g'(a)$ is given by

$$\begin{aligned}g'(a) &= \frac{d}{da}\Big(\mathbb{E}_B[Q(aB-a+b)]\Big) &(280)\\ &= -\int_{-1}^{\infty}\frac{t}{\sqrt{2\pi}}e^{-\frac{(at)^2+2atb+b^2}{2}}f_{B-1}(t)dt. &(281)\end{aligned}$$

Here, in (281) we used the Leibniz's integration rule [38] and the identity $Q'(x)=-\frac{1}{\sqrt{2\pi}}e^{-x^2/2}$. The RHS of (281) is equal to zero when $a=0$ because, by definition, $\mathbb{E}[B-1]=0$. When $a>0$, we have

$$\begin{aligned}g'(a) &\ge -\frac{e^{-b^2/2}}{\sqrt{2\pi}}\int_{-1}^{\infty}te^{-\frac{(at)^2}{2}}f_{B-1}(t)dt &(282)\\ &= -\frac{e^{-b^2/2}}{a\sqrt{2\pi}}\int_{-1}^{\infty}e^{-\frac{(at)^2}{2}}f'_{B-1}(t)dt &(283)\\ &= -\frac{e^{-b^2/2}}{a^2}f'_{B+Z/a}(1). &(284)\end{aligned}$$

Here, (282) follows because $e^{-abt}t\le t$ for every $t\in\mathbb{R}$; in (283) we used integration by parts and that $f_{B-1}(-1)=0$.

It remains to show that $f'_{B+Z/a}(1) \leq 0$ for every $a > 0$. Since $Z \sim \mathcal{N}(0,1)$, by the central limit theorem for densities (see [39, Th. VII.2.7]), the pdf of Z can be approximated to an arbitrary precision by the pdf of a sum of i.i.d. Exp(1)-distributed random variables. Moreover, B is the convolution of finitely many exponential distributions and $\mathbb{E}[B + Z/a] = 1$. Hence, to prove $f'_{B+Z/a}(1) \leq 0$, it suffices to show that the derivative of the convolution of finitely many exponential pdfs computed at the mean value of the resulting distribution is nonpositive. This follows from Lemma 15 (see Appendix II).

Appendix V
Proof of Theorem 11

Let $\eta > 0$ be an arbitrary constant and let the function $q_\eta(\cdot)$ be defined as follows:

$$q_\eta(x) \triangleq Q\left(\frac{x-\eta}{\sqrt{2x}}\right), \quad x > 0. \tag{285}$$

It follows from (245), (246), and (249) that every (E, M, ϵ)-code for the MIMO Rayleigh block-fading channel (12) for the case of perfect CSIR satisfies

$$\log M \leq \eta \log e - \log\left|\inf_{\boldsymbol{u}\in\mathbb{C}^\infty:\|\boldsymbol{u}\|_2^2=E} \mathbb{E}\left[q_\eta\left(\sum_{r=1}^{m_\mathrm{r}}\sum_{i=1}^{\infty}|u_i H_{r,i}|^2\right)\right] - \epsilon\right|^+. \tag{286}$$

Suppose that the function $g_\eta(\cdot)$ defined in (86) is convex on $[0,\infty)$, and that

$$q_\eta(x) \geq g_\eta(x), \quad \text{for all } x \in [0,\infty). \tag{287}$$

In other words, suppose that $g_\eta(\cdot)$ is a convex lower bound on $q_\eta(x)$. Then, (87) follows because, for every $\boldsymbol{u} \in \mathbb{C}^\infty$ with $\|\boldsymbol{u}\|_2^2 = E$,

$$\begin{aligned}
&\mathbb{E}\left[q_\eta\left(\sum_{r=1}^{m_\mathrm{r}}\sum_{i=1}^{\infty}|u_i H_{r,i}|^2\right)\right] \\
&\quad\geq \mathbb{E}\left[g_\eta\left(\sum_{r=1}^{m_\mathrm{r}}\sum_{i=1}^{\infty}|u_i H_{r,i}|^2\right)\right] && (288)\\
&\quad\geq g_\eta\left(\mathbb{E}\left[\sum_{r=1}^{m_\mathrm{r}}\sum_{i=1}^{\infty}|u_i H_{r,i}|^2\right]\right) && (289)\\
&\quad= g_\eta(m_\mathrm{r} E). && (290)
\end{aligned}$$

Here, (289) follows from Jensen's inequality.

It remains to prove that $g_\eta(x)$ is indeed a convex lower bound on $q_\eta(x)$. Observe the following properties of $q_\eta(\cdot)$, which can be verified through standard algebraic manipulations:

- $q_\eta(\cdot)$ is monotonically decreasing;
- $\lim_{x\to 0} q_\eta(x) = 1, \quad \lim_{x\to\infty} q_\eta(x) = 0$;
- $q_\eta(\eta) = 1/2$;
- if $\eta > \pi$, then $q'_\eta(\eta) = -1/(2\sqrt{\eta\pi}) < -1/(2\eta)$;
- if $\eta > 6$, there exists an $0 < x_0 < \eta$ such that $q_\eta(\cdot)$ is concave on $(0, x_0)$ and convex on (x_0, ∞).

Assume that $\eta > 6$. Then, the above properties of $q_\eta(\cdot)$ imply that there exists a unique x_1 such that the line connecting $(0, 1)$ and $(x_1, q_\eta(x_1))$ lies below the graph of $q_\eta(x)$ and is tangent to $q_\eta(\cdot)$ at $(x_1, q_\eta(x_1))$ (see Fig. 2). Since the slope of the line connecting $(0, 1)$ and $(x_1, q_\eta(x_1))$ is

$$-\frac{1}{x_1} Q\left(\frac{\eta - x_1}{\sqrt{2x_1}}\right) \tag{291}$$

and since the derivative of $q_\eta(x)$ at $x = x_1$ is given by

$$-\frac{1}{x_1}\frac{1}{4\sqrt{\pi}} e^{-(x_1-\eta)^2/(4x_1)}\left(\frac{\eta}{\sqrt{x_1}} + \sqrt{x_1}\right) \tag{292}$$

it follows that x_1 is the solution of (85). Furthermore, since $q'_\eta(\eta) < -1/(2\eta)$, and since $-1/(2\eta)$ is the slope of the line connecting $(0, 1)$ and $(\eta, 1/2)$, we have that $x_1 > \eta$. Observe now that $g_\eta(x)$ coincides with the line connecting $(0, 1)$ and $(x_1, q_\eta(x_1))$ for $x \leq x_1$, and that it coincides with $q_\eta(x)$ if $x \geq x_1$. This proves that $g_\eta(x)$ is indeed a convex lower bound on $q_\eta(x)$.

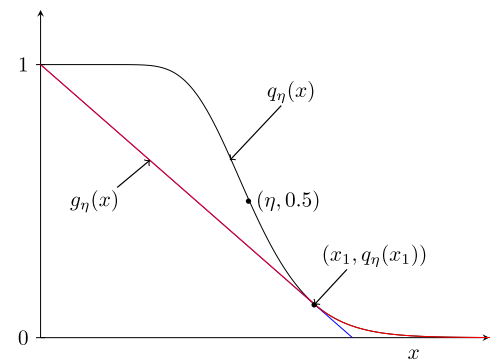

Fig. 2. A geometric illustration of $q_\eta(\cdot)$ in (285) (black curve), of the tangent line of $q_\eta(\cdot)$ (blue curve), and of $g_\eta(\cdot)$ in (86) (red curve).

References

[1] C. E. Shannon, "Communication in the presence of noise," *Proc. IRE*, vol. 37, no. 1, pp. 10–21, Jan. 1949.

[2] S. Verdú, "Spectral efficiency in the wideband regime," *IEEE Trans. Inf. Theory*, vol. 48, no. 6, pp. 1319–1343, Jun. 2002.

[3] R. S. Kennedy, *Fading Dispersive Communication Channels*. Hoboken, NJ, USA: Wiley, 1969.

[4] R. G. Gallager, "Power limited channels: Coding, multiaccess, and spread spectrum," in *Proc. Conf. Inf. Sci. Syst.*, Princeton, NJ, USA, Mar. 1988, pp. 229–257.

[5] S. Verdú, "On channel capacity per unit cost," *IEEE Trans. Inf. Theory*, vol. 36, no. 5, pp. 1019–1030, Sep. 1990.

[6] L. Zheng, D. N. C. Tse, and M. Médard, "Channel coherence in the low-SNR regime," *IEEE Trans. Inf. Theory*, vol. 53, no. 3, pp. 976–997, Mar. 2007.

[7] Y. Polyanskiy, H. V. Poor, and S. Verdú, "Channel coding rate in the finite blocklength regime," *IEEE Trans. Inf. Theory*, vol. 56, no. 5, pp. 2307–2359, May 2010.

[8] Y. Polyanskiy, H. V. Poor, and S. Verdú, "Minimum energy to send κ bits through the Gaussian channel with and without feedback," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4880–4902, Aug. 2011.

[9] V. Y. F. Tan, "Asymptotic estimates in information theory with non-vanishing error probabilities," *Found. Trends Commun. Inf. Theory*, vol. 11, nos. 1–2, pp. 1–184, Sep. 2014.

[10] V. Kostina, Y. Polyanskiy, and S. Verdú. (Jan. 2015). "Joint source-channel coding with feedback." [Online]. Available: https://arxiv.org/abs/1501.07640

[11] I. E. Telatar and D. N. C. Tse, "Capacity and mutual information of wideband multipath fading channels," *IEEE Trans. Inf. Theory*, vol. 46, no. 4, pp. 1384–1400, Jul. 2000.

[12] M. Mĕdard, "Bandwidth scaling for fading multipath channels," *IEEE Trans. Inf. Theory*, vol. 48, no. 4, pp. 840–852, Apr. 2002.

[13] V. Sethuraman and B. Hajek, "Capacity per unit energy of fading channels with a peak constraint," *IEEE Trans. Inf. Theory*, vol. 51, no. 9, pp. 3102–3120, Sep. 2005.
[14] G. Durisi, U. G. Schuster, H. Bölcskei, and S. Shamai (Shitz), "Noncoherent capacity of underspread fading channels," *IEEE Trans. Inf. Theory*, vol. 56, no. 1, pp. 367–395, Jan. 2010.
[15] Y. Polyanskiy and S. Verdú, "Scalar coherent fading channel: Dispersion analysis," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Saint Petersburg, Russia, Aug. 2011, pp. 2959–2963.
[16] W. Yang, G. Durisi, T. Koch, and Y. Polyanskiy, "Diversity versus channel knowledge at finite block-length," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Lausanne, Switzerland, Sep. 2012, pp. 577–581.
[17] J. Hoydis, R. Couillet, and P. Piantanida, "The second-order coding rate of the MIMO quasi-static Rayleigh fading channel," *IEEE Trans. Inf. Theory*, vol. 61, no. 12, pp. 6591–6622, Dec. 2015.
[18] W. Yang, G. Durisi, T. Koch, and Y. Polyanskiy, "Quasi-static multiple-antenna fading channels at finite blocklength," *IEEE Trans. Inf. Theory*, vol. 60, no. 7, pp. 4232–4265, Jun. 2014.
[19] A. Collins and Y. Polyanskiy, "Orthogonal designs optimize achievable dispersion for coherent MISO channels," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Honolulu, HI, USA, Jul. 2014, pp. 2524–2528.
[20] W. Yang, G. Caire, G. Durisi, and Y. Polyanskiy, "Optimum power control at finite blocklength," *IEEE Trans. Inf. Theory*, vol. 61, no. 9, pp. 4598–4615, Sep. 2015.
[21] G. Durisi, T. Koch, J. Östman, Y. Polyanskiy, and W. Yang, "Short-packet communications over multiple-antenna Rayleigh-fading channels," *IEEE Trans. Commun.*, vol. 64, no. 2, pp. 618–629, Feb. 2016.
[22] E. Abbe, S. L. Huang, and E. Telatar, "Proof of the outage probability conjecture for MISO channels," *IEEE Trans. Inf. Theory*, vol. 59, no. 5, pp. 2596–2602, May 2013.
[23] W. Feller, *An Introduction to Probability Theory and Its Applications*, vol. 2. New York, NY, USA: Wiley, 1970.
[24] N. Johnson, S. Kotz, and N. Balakrishnan, *Continuous Univariate Distributions*, vol. 1, 2nd ed. New York, NY, USA: Wiley, 1995.
[25] G. B. Folland, *Real Analysis: Modern Techniques and Their Applications*. New York, NY, USA: Wiley, 1999.
[26] J. Neyman and E. S. Pearson, "On the problem of the most efficient tests of statistical hypotheses," *Philos. Trans. Roy. Soc. London A*, vol. 231, nos. 694–706, pp. 289–337, 1933.
[27] A. Lapidoth and S. M. Moser, "Capacity bounds via duality with applications to multiple-antenna systems on flat-fading channels," *IEEE Trans. Inf. Theory*, vol. 49, no. 10, pp. 2426–2467, Oct. 2003.
[28] M. Medard, "The effect upon channel capacity in wireless communications of perfect and imperfect knowledge of the channel," *IEEE Trans. Inf. Theory*, vol. 46, no. 3, pp. 933–946, May 2000.
[29] W. Yang, A. Collins, G. Durisi, Y. Polyanskiy, and H. V. Poor, "A beta-beta achievability bound with applications," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Barcelona, Spain, Jul. 2016, pp. 2669–2973.
[30] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.
[31] S. Karlin, *Total Positivity*. Stanford, CA, USA: Stanford Univ. Press, 1968.
[32] I. A. Ibragimov, "On the composition of unimodal distributions," *Theory Probab. Appl.*, vol. 1, no. 2, pp. 255–260, 1956.
[33] A. Prékopa, "On logarithmic concave measures and functions," *Acta Sci. Math.*, vol. 33, pp. 335–343, 1973.
[34] K. Ball, F. Barthe, and A. Naor, "Entropy jumps in the presence of a spectral gap," *Duke Math J.*, vol. 119, no. 1, pp. 41–63, Jul. 2003.
[35] L. Lovász and S. Vempala, "The geometry of logconcave functions and sampling algorithms," *Random Struct. Algorithms*, vol. 30, no. 3, pp. 307–358, May 2007.
[36] S. G. Bobkov and G. P. Chistyakov, "On concentration functions of random variables," *J. Theor. Probab.*, vol. 28, no. 3, pp. 976–988, Sep. 2015.
[37] W. Rudin, *Principles of Mathematical Analysis*, 3rd ed. Singapore: McGraw-Hill, 1976.
[38] H. Flanders, "Differentiation under the integral sign," *Amer. Math. Monthly*, vol. 80, no. 6, pp. 615–627, Jun. 1973.
[39] V. V. Petrov, *Sums of Independent Random Variates*. New York, NY, USA: Springer-Verlag, 1975.

Wei Yang (S'09–M'15) received the B.E. and M.E. degree from the Beijing University of Posts and Telecommunications, Beijing, China, in 2008 and 2011, and the Ph.D. degree in Electrical Engineering from Chalmers University of Technology, Gothenburg, Sweden, in 2015. In 2012 (July-August) and 2014 (July-September), he was a visiting student at the Laboratory for Information and Decision Systems, Massachusetts Institute of Technology, Cambridge, MA. Since 2015, he has been with the Department of Electrical Engineering at Princeton University, where he is now a postdoctoral research associate.

Dr. Yang is the recipient of a Student Paper Award at the 2012 IEEE International Symposium on Information Theory (ISIT), Cambridge, MA, and the 2013 IEEE Sweden VT-COM-IT joint chapter best student conference paper award. His research interests are in the areas of information and communication theory.

Giuseppe Durisi (S'02–M'06–SM'12) received the Laurea degree (*summa cum laude*) and the Doctor degree both from Politecnico di Torino, Italy, in 2001 and 2006, respectively. From 2006 to 2010 he was a postdoctoral researcher at ETH Zurich, Zurich, Switzerland. In 2010, he joined Chalmers University of Technology, Gothenburg, Sweden, where he is now associate professor. He is also guest researcher at Ericsson, Sweden, and co-director of Chalmers ICT Area of Advance.

Dr. Durisi is a senior member of the IEEE. He is the recipient of the 2013 IEEE ComSoc Best Young Researcher Award for the Europe, Middle East, and Africa Region, and is co-author of a paper that won a "student paper award" at the 2012 International Symposium on Information Theory, and of a paper that won the 2013 IEEE Sweden VT-COM-IT joint chapter best student conference paper award. In 2015, he joined the editorial board of the IEEE TRANSACTIONS ON COMMUNICATIONS as associate editor. From 2011 to 2014, he served as publications editor for the IEEE TRANSACTIONS ON INFORMATION THEORY. His research interests are in the areas of communication and information theory.

Yury Polyanskiy (S'08–M'10–SM'14) is an Associate Professor of Electrical Engineering and Computer Science and a member of LIDS at MIT. Yury received M.S. degree in applied mathematics and physics from the Moscow Institute of Physics and Technology, Moscow, Russia in 2005 and Ph.D. degree in electrical engineering from Princeton University, Princeton, NJ in 2010. Currently, his research focuses on basic questions in information theory, error-correcting codes, wireless communication and fault-tolerant and defecttolerant circuits. Dr. Polyanskiy won the 2013 NSF CAREER award and 2011 IEEE Information Theory Society Paper Award.