

Scaling Laws for Gaussian Random Many-Access Channels

Jithin Ravi, *Member, IEEE*, and Tobias Koch, *Senior Member, IEEE*

Abstract—This paper considers a Gaussian multiple-access channel with random user activity where the total number of users ℓ_n and the average number of active users k_n may grow with the blocklength n . For this channel, it studies the maximum number of bits that can be transmitted reliably per unit-energy as a function of ℓ_n and k_n . When all users are active with probability one, i.e., $\ell_n = k_n$, it is demonstrated that, if k_n is of an order strictly below $n/\log n$, then each user can achieve the single-user capacity per unit-energy $(\log e)/N_0$ (where $N_0/2$ is the noise power) by using an orthogonal-access scheme. In contrast, if k_n is of an order strictly above $n/\log n$, then the users cannot achieve any positive rate per unit-energy. Consequently, there is a sharp transition between orders of growth where interference-free communication is feasible and orders of growth where reliable communication at a positive rate per unit-energy is infeasible. It is further demonstrated that orthogonal-access schemes in combination with orthogonal codebooks, which achieve the capacity per unit-energy when the number of users is bounded, can be strictly suboptimal.

When the user activity is random, i.e., when ℓ_n and k_n are different, it is demonstrated that, if $k_n \log \ell_n$ is sublinear in n , then each user can achieve the single-user capacity per unit-energy $(\log e)/N_0$. Conversely, if $k_n \log \ell_n$ is superlinear in n , then the users cannot achieve any positive rate per unit-energy. Consequently, there is again a sharp transition between orders of growth where interference-free communication is feasible and orders of growth where reliable communication at a positive rate is infeasible that depends on the asymptotic behaviors of both ℓ_n and k_n . It is further demonstrated that orthogonal-access schemes, which are optimal when all users are active with probability one, can be strictly suboptimal in general.

Index Terms—Capacity per unit-energy, many-access channel, multiple access, random access.

I. INTRODUCTION

CHEN *et al.* [1] introduced the many-access channel (MnAC) as a multiple-access channel (MAC) where the number of users grows with the blocklength and each user is active with a given probability. This model is motivated by

J. Ravi and T. Koch have received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (Grant No. 714161). T. Koch has further received funding from the Spanish Ministerio de Ciencia e Innovación under Grants RYC-2014-16332, TEC2016-78434-C3-3-R (AEI/FEDER, EU), and PID2020-116683GB-C21 / AEI / 10.13039/501100011033. The material in this paper was presented in part at the IEEE International Symposium on Information Theory, Paris, France, July 2019, at the International Zurich Seminar on Information and Communication, Zurich, Switzerland, February 2020, and at the IEEE International Symposium on Information Theory, Los Angeles, CA, USA, June 2020.

J. Ravi and T. Koch are with the Signal Theory and Communications Department, Universidad Carlos III de Madrid, Spain, and with the Gregorio Marañón Health Research Institute, Madrid, Spain (emails: rjithin@tsc.uc3m.es, koch@tsc.uc3m.es).

Copyright (c) 2021 IEEE. Personal use of this material is permitted. However, permission to use this material for any other purposes must be obtained from the IEEE by sending a request to pubs-permissions@ieee.org.

systems consisting of a single receiver and many transmitters, the number of which is comparable or even larger than the blocklength. This situation may occur, e.g., in a machine-to-machine communication scenario with many thousands of devices in a given cell that are active only sporadically. In [1], Chen *et al.* considered a Gaussian MnAC with ℓ_n users, each of which is active with probability α_n , and determined the number of messages M_n each user can transmit reliably with a codebook of average power not exceeding P . Since then, MnACs have been studied in various papers under different settings.

An example of a MAC is the uplink connection in a cellular network. Current cellular networks follow a *grant-based* access protocols, i.e., an active device has to obtain permission from the base station to transmit data. In MnACs, this will lead to a large signalling overhead. *Grant-free* access protocols, where active devices can access the network without a permission, were proposed to overcome this [2]. The synchronization issues arising in such scenarios have been studied by Shahi *et al.* [3]. In some of the MnACs, such as sensor networks, detecting the identity of the device that sends a particular message may not be important. This scenario was studied under the name of *unsourced* massive access by Polyanskiy [4], who further introduced the notion of *per-user probability of error*. Specifically, [4] analyzed the minimum *energy-per-bit* required to reliably transmit a message over an unsourced Gaussian MnAC where the number of active users grows linearly in the blocklength and each user's payload is fixed. Low-complexity schemes for this setting were studied in many works [5]–[9]. Generalizations to quasi-static fading MnACs can be found in [10]–[12]. Zadik *et al.* [13] presented improved bounds on the tradeoff between user density and energy-per-bit for the many-access channel introduced in [4].

Related to energy per-bit is the *capacity per unit-energy* \dot{C} , which is defined as the largest number of bits per unit-energy that can be transmitted reliably over a channel. Verdú [14] showed that \dot{C} can be obtained from the capacity-cost function $C(P)$, defined as the largest number of bits per channel use that can be transmitted reliably with average power per symbol not exceeding P , as

$$\dot{C} = \sup_{P>0} \frac{C(P)}{P}.$$

For the Gaussian channel with noise power $N_0/2$, this is equal to $\frac{\log e}{N_0}$. Verdú further showed that the capacity per unit-energy can be achieved by a codebook that is orthogonal in the sense that the nonzero components of different codewords do not overlap. Such a codebook corresponds to pulse position modulation (PPM) either in time or frequency domain. In

general, we shall say that a codebook is orthogonal if the inner product between different codewords is zero. The two-user Gaussian multiple access channel (MAC) was also studied in [14], and it was demonstrated that both users can achieve the single-user capacity per unit-energy by timesharing the channel between the users, i.e., while one user transmits the other user remains silent. This is an *orthogonal-access scheme* in the sense that the inner product between codewords of different users is zero.¹ To summarize, in a two-user Gaussian MAC, both users can achieve the rate per unit-energy $\frac{\log e}{N_0}$ by combining an orthogonal-access scheme with orthogonal codebooks. This result can be directly generalized to any finite number of users.

The picture changes when the number of users grows without bound with the blocklength n . In this paper, we consider a setting where the total number of users ℓ_n may grow as an arbitrary function of the blocklength and the probability α_n that a user is active may be a function of the blocklength, too. The contributions of this paper are as follows:

- 1) We consider the capacity per unit-energy of the Gaussian MnAC as a function of the order of growth of users when all users are active with probability one. In Theorem 1, we show that, if the order of growth is above $n/\log n$, then the capacity per unit-energy is zero, and if the order of growth is below $n/\log n$, then each user can achieve the single-user capacity per unit-energy $\frac{\log e}{N_0}$. Thus, there is a sharp transition between orders of growth where interference-free communication is feasible and orders of growth where reliable communication at a positive rate is infeasible. We further show that, if the order of growth is proportional to $n/\log n$, then the capacity per unit-energy is strictly between zero and $\frac{\log e}{N_0}$. Finally, we show that the capacity per unit-energy can be achieved by an orthogonal-access scheme.
- 2) Since an orthogonal-access scheme in combination with orthogonal codebooks is optimal in achieving the capacity per unit-energy for a finite number of users, we study the performance of such a scheme for an unbounded number of users. In particular, we characterize in Theorem 2 the largest rate per unit-energy that can be achieved with an orthogonal-access scheme and orthogonal codebooks. Our characterization shows that this scheme is only optimal if the number of users grows more slowly than any positive power of n .
- 3) We analyze the behavior of the capacity per unit-energy of the Gaussian MnAC as a function of the order of growth of the number of users for the per-user probability of error which, in this paper, we shall refer to as *average probability of error* (APE). In contrast, we refer to the classical probability of error as *joint probability of error* (JPE). We demonstrate that, if the growth is sublinear, then each user can achieve the capacity per unit-energy $\frac{\log e}{N_0}$ of the single-user Gaussian channel. Conversely, if the growth is linear or superlinear, then the capacity per unit-

energy is zero (Theorem 3). Comparing with the results in Theorem 1, we observe that relaxing the error probability from JPE to APE shifts the transition threshold separating the two regimes of interference-free communication and no reliable communication from $n/\log n$ to n .

- 4) We consider MnACs with random user activity. As before, we consider a setting where the total number of users ℓ_n may grow as an arbitrary function of the blocklength. Furthermore, the probability α_n that a user is active may be a function of the blocklength, too. Let $k_n = \alpha_n \ell_n$ denote the average number of active users. We demonstrate in Theorem 7 that, if $k_n \log \ell_n$ is sublinear in n , then each user can achieve the single-user capacity per unit-energy. Conversely, if $k_n \log \ell_n$ is superlinear in n , then the capacity per unit-energy is zero. We also demonstrate that, if $k_n \log \ell_n$ is linear in n , then the capacity per unit-energy is strictly between zero and $\frac{\log e}{N_0}$.
- 5) We show in Theorem 8 that orthogonal-access schemes, which are optimal when $\alpha_n = 1$, are strictly suboptimal when $\alpha_n \rightarrow 0$. In Theorem 9, we then characterize the behavior of the random MnAC under APE.
- 6) We conclude the paper with a comparison of the setting considered in this paper and the setting proposed by Polyanskiy in [4]. Since an important aspect of the Polyanskiy setting is that the probability of error does not vanish as the blocklength tends to infinity, we briefly discuss the behavior of the ϵ -capacity per unit-energy, i.e., the largest rate per unit-energy for which the error probability does not exceed a given ϵ . For the case where the users are active with probability one, we show that, for JPE and an unbounded number of users, the ϵ -capacity per unit energy coincides with \dot{C} . In other words, the strong converse holds in this case. In contrast, for APE, the ϵ -capacity per unit-energy can be strictly larger than \dot{C} , so the strong converse does not hold.

The rest of the paper is organized as follows. Section II introduces the system model and the different notions of probability of error. Section III presents our results for the case where all users are active with probability one (“non-random MnAC”). Section IV presents our results for the case where the user activity is random (“random MnAC”). Section V briefly compares our results with those obtained in [4] under non-vanishing probability of error. Section VI concludes the paper with a summary and discussion of our results.

II. PROBLEM FORMULATION AND PRELIMINARIES

A. Model and Definitions

Consider a network with ℓ users that, if they are active, wish to transmit their messages $W_i, i = 1, \dots, \ell$ to one common receiver, see Fig. 1. The messages are assumed to be independent and uniformly distributed on $\mathcal{M}_n^{(i)} \triangleq \{1, \dots, M_n^{(i)}\}$. To transmit their messages, the users send a codeword of n symbols over the channel, where n is referred to as the *blocklength*. We consider a many-access scenario where the number of users ℓ may grow with n , hence, we denote it as ℓ_n . We assume that a user is active with probability α_n . We

¹Note, however, that in an orthogonal-access scheme the codebooks are not required to be orthogonal. That is, codewords of different codebooks are orthogonal to each other, but codewords of the same codebook need not be.

denote the average number of active users at blocklength n by k_n , i.e., $k_n = \alpha_n \ell_n$.

Let \mathcal{U}_n denote the set of active users at blocklength n , defined as

$$\mathcal{U}_n \triangleq \{i = 1, \dots, \ell_n : \text{user } i \text{ is active}\}.$$

We consider a Gaussian channel model where the received vector \mathbf{Y} is given by

$$\mathbf{Y} = \sum_{i \in \mathcal{U}_n} \mathbf{x}_i(W_i) + \mathbf{Z}. \quad (1)$$

Here, $\mathbf{x}_i(W_i)$ is the length- n transmitted codeword from user i for message W_i , and \mathbf{Z} is a vector of n i.i.d. Gaussian components $Z_j \sim \mathcal{N}(0, N_0/2)$ (where $\mathcal{N}(\mu, \sigma^2)$ denotes the Gaussian distribution with mean μ and variance σ^2) independent of $\mathbf{X}_i \triangleq \mathbf{x}_i(W_i)$. The decoder produces an estimate of the users that are active and estimates their transmitted messages.

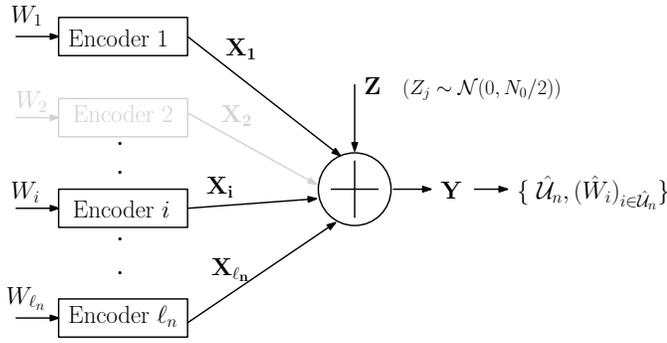


Fig. 1. Many-access channel with ℓ_n users at blocklength n .

There are different ways to define the overall probability of error. Let $\hat{\mathcal{U}}_n$ and \hat{W}_i denote the decoder's estimates of the set of active users and the message transmitted by user i , respectively. Further let \mathcal{D}_E denote the event that the set of active users was detected erroneously, i.e., that $\hat{\mathcal{U}}_n \neq \mathcal{U}_n$, and let \mathcal{M}_E denote the event that $\hat{W}_i \neq W_i$ for some $i \in \mathcal{U}_n$ (where we set $\hat{W}_i = 0$ for every $i \notin \hat{\mathcal{U}}_n$). One possibility to measure the likelihood of these two events is via the probability of error

$$P_e^{(n)} = \Pr(\mathcal{D}_E \cup \mathcal{M}_E). \quad (2)$$

Another possibility is to consider

$$P_{\max}^{(n)} = \max(\Pr(\mathcal{D}_E), \Pr(\mathcal{M}_E)). \quad (3)$$

These probabilities are related through the inequality $P_{\max}^{(n)} \leq P_e^{(n)} \leq 2P_{\max}^{(n)}$. Indeed, the first inequality follows since $\Pr(\mathcal{D}_E \cup \mathcal{M}_E) \geq \Pr(\mathcal{D}_E)$ and $\Pr(\mathcal{M}_E \cup \mathcal{M}_E) \geq \Pr(\mathcal{M}_E)$. The second inequality follows because, by the union bound, $P_e^{(n)} \leq \Pr(\mathcal{D}_E) + \Pr(\mathcal{M}_E) \leq 2P_{\max}^{(n)}$. So, in general, $P_{\max}^{(n)}$ is more optimistic than $P_e^{(n)}$. However, if we wish the probability of error to vanish as $n \rightarrow \infty$, then the two definitions are equivalent since $P_e^{(n)}$ vanishes if, and only if, $P_{\max}^{(n)}$ vanishes.

In this paper, we will mainly consider the more pessimistic definition of probability of error $P_e^{(n)}$. For this definition, one can model an inactive user by an active user that transmits message $W_i = 0$ and an encoder that maps the zero message

to the all-zero codeword. The decoder then simply guesses the transmitted message, and the error probability $P_e^{(n)}$ is given by the probability that the decoder's guess \hat{W}_i is different from W_i . Mathematically, this can be described as follows. We enhance the message set to

$$\overline{\mathcal{M}}_n^{(i)} \triangleq \mathcal{M}_n^{(i)} \cup \{0\}$$

and define the distribution of the i -th user's message as

$$\Pr\{W_i = w\} = \begin{cases} 1 - \alpha_n, & w = 0 \\ \frac{\alpha_n}{M_n^{(i)}}, & w \in \{1, \dots, M_n^{(i)}\}. \end{cases} \quad (4)$$

We assume that the codebook is such that message 0 is mapped to the all-zero codeword. Then, the channel model (1) can be written as

$$\mathbf{Y} = \sum_{i=1}^{\ell_n} \mathbf{x}_i(W_i) + \mathbf{Z}.$$

We next introduce the notion of an $(n, \{M_n^{(\cdot)}\}, \{E_n^{(\cdot)}\}, \epsilon)$ code.

Definition 1: For $0 \leq \epsilon \leq 1$, an $(n, \{M_n^{(\cdot)}\}, \{E_n^{(\cdot)}\}, \epsilon)$ code for the Gaussian MnAC consists of:

- 1) Encoding functions $f_i : \{0, 1, \dots, M_n^{(i)}\} \rightarrow \mathbb{R}^n$, $i = 1, \dots, \ell_n$ which map user i 's message to the codeword $\mathbf{x}_i(W_i)$, satisfying the energy constraint

$$\sum_{j=1}^n x_{ij}^2(W_i) \leq E_n^{(i)}, \quad \text{with probability one} \quad (5)$$

where $x_{ij}(W_i)$ is the j -th symbol of the transmitted codeword. We set $x_{ij}(0) = 0$, $j = 1, \dots, n$ for all users $i = 1, \dots, \ell_n$.

- 2) Decoding function $g : \mathbb{R}^n \rightarrow \{0, 1, \dots, M_n^{(1)}\} \times \dots \times \{0, 1, \dots, M_n^{(\ell_n)}\}$ which maps the received vector \mathbf{Y} to the messages of all users and whose probability of error $P_e^{(n)}$ satisfies

$$P_e^{(n)} \triangleq \Pr\{g(\mathbf{Y}) \neq (W_1, \dots, W_{\ell_n})\} \leq \epsilon. \quad (6)$$

Note that the probability of error in (6) is equal to $P_e^{(n)}$ defined in (2). Indeed, the event $g(\mathbf{Y}) \neq (W_1, \dots, W_{\ell_n})$ occurs if, and only if, there exists at least one index $i = 1, \dots, \ell_n$ for which $\hat{W}_i \neq W_i$. This in turn implies that either event \mathcal{D}_E occurs (if $W_i = 0$) or event \mathcal{M}_E occurs (if $W_i \neq 0$). Conversely, if the event $\mathcal{D}_E \cup \mathcal{M}_E$ occurs, then there exists either some $i \notin \mathcal{U}_n$ for which $\hat{W}_i \neq 0$ or some $i \in \mathcal{U}_n$ for which $\hat{W}_i \neq W_i$. Consequently, there exists at least one index $i = 1, \dots, \ell_n$ for which $\hat{W}_i \neq W_i$. It follows that the events $g(\mathbf{Y}) \neq (W_1, \dots, W_{\ell_n})$ and $\mathcal{D}_E \cup \mathcal{M}_E$ are equivalent.

We shall say that the *codebook of user i is orthogonal* if the inner product between $\mathbf{x}_i(w)$ and $\mathbf{x}_i(w')$ is zero for every $w \neq w'$, where $w, w' = 1, \dots, M_n^{(i)}$. Similarly, we shall say that an *access scheme is orthogonal* if, for any two users i and j , the inner product between $\mathbf{x}_i(w)$ and $\mathbf{x}_j(w')$ is zero for every $w = 1, \dots, M_n^{(i)}$ and $w' = 1, \dots, M_n^{(j)}$. An $(n, \{M_n^{(\cdot)}\}, \{E_n^{(\cdot)}\}, \epsilon)$ code is said to be *symmetric* if $M_n^{(i)} = M_n$ and $E_n^{(i)} = E_n$ for all $i = 1, \dots, \ell_n$. For compactness, we denote such a code by (n, M_n, E_n, ϵ) . In this paper, we restrict ourselves to symmetric codes.

Definition 2: For a symmetric code, the rate per unit-energy \dot{R} is said to be ϵ -achievable if for every $\delta > 0$ there exists an n_0 such that, if $n \geq n_0$, then an (n, M_n, E_n, ϵ) code can be found whose rate per unit-energy satisfies $\frac{\log M_n}{E_n} > \dot{R} - \delta$. Furthermore, \dot{R} is said to be achievable if it is ϵ -achievable for all $0 < \epsilon < 1$. The capacity per unit-energy \dot{C} is the supremum of all achievable rates per unit-energy. The ϵ -capacity per unit-energy \dot{C}_ϵ is the supremum of all ϵ -achievable rates per unit-energy.

Remark 1: In [14, Def. 2], a rate per unit-energy \dot{R} is said to be ϵ -achievable if for every $\alpha > 0$ there exists an E_0 such that, if $E \geq E_0$, then an (n, M, E, ϵ) code can be found whose rate per unit-energy satisfies $\frac{\log M}{E} > \dot{R} - \alpha$. Thus, in contrast to Definition 2, the energy E is required to be larger than some threshold, rather than the blocklength n . For the MnAC, where the number of users grows with the blocklength, we believe it is more natural to impose a threshold on n . Definition 2 is also consistent with the definition of energy-per-bit in [4], [13]. Further note that, for the capacity per unit-energy, where a vanishing error probability is required, Definition 2 is in fact equivalent to [14, Def. 2], since $P_e^{(n)} \rightarrow 0$ only if $E_n \rightarrow \infty$ (see Lemma 4 ahead).

Remark 2: Many works in the literature on many-access channels, including [4], [5], [10]–[13], consider a *per-user probability of error*

$$P_{e,A}^{(n)} \triangleq \frac{1}{\ell_n} \sum_{i=1}^{\ell_n} \Pr\{\hat{W}_i \neq W_i\} \quad (7)$$

rather than the probability of error in (6). In this paper, we shall refer to (6) as *joint error probability (JPE)* and to (7) as *average error probability (APE)*. While we mainly consider the JPE, we also discuss the capacity per unit-energy for APE. To this end, we define an $(n, \{M_n^{(\cdot)}\}, \{E_n^{(\cdot)}\}, \epsilon)$ code for APE with the same encoding and decoding functions described in Definition 1, but with the probability of error (6) replaced with (7). The capacity per unit-energy and the ϵ -capacity per unit-energy for APE, denoted by \dot{C}^A and \dot{C}_ϵ^A respectively, are then defined as in Definition 2.

B. Order Notation

Let $\{a_n\}$ and $\{b_n\}$ be two sequences of nonnegative real numbers. We write $a_n = O(b_n)$ if $\limsup_{n \rightarrow \infty} \frac{a_n}{b_n} < \infty$. Similarly, we write $a_n = o(b_n)$ if $\lim_{n \rightarrow \infty} \frac{a_n}{b_n} = 0$, and $a_n = \Omega(b_n)$ if $\liminf_{n \rightarrow \infty} \frac{a_n}{b_n} > 0$. The notation $a_n = \Theta(b_n)$ indicates that $a_n = O(b_n)$ and $a_n = \Omega(b_n)$. Finally, we write $a_n = \omega(b_n)$ if $\lim_{n \rightarrow \infty} \frac{a_n}{b_n} = \infty$.

III. CAPACITY PER UNIT-ENERGY OF NON-RANDOM MANY-ACCESS CHANNELS

In this section, we study the Gaussian MnAC under the assumption that all users are active, i.e., $\alpha_n = 1$ and $k_n = \ell_n$. We present our results on the non-random MnACs in Subsection III-A. In particular, in Theorem 1, we characterize the capacity per unit-energy as a function of the order of k_n . Then, in Theorem 2, we give a characterization of the largest rate per unit-energy achievable using an orthogonal-access

scheme with orthogonal codebooks. Finally, in Theorem 3, we present our results on the capacity per unit-energy for APE. The proofs of Theorems 1–3 are given in Subsections III-B, III-C, and III-D, respectively.

A. Main Results

Theorem 1: The capacity per unit-energy of the Gaussian non-random MnAC has the following behavior:

- 1) If $k_n = o(n/\log n)$, then $\dot{C} = \frac{\log e}{N_0}$. Moreover, the capacity per unit-energy can be achieved by an orthogonal-access scheme.
- 2) If $k_n = \omega(n/\log n)$, then $\dot{C} = 0$.
- 3) If $k_n = \Theta(\frac{n}{\log n})$, then $0 < \dot{C} < \frac{\log e}{N_0}$.

Proof: See Section III-B. ■

Theorem 1 demonstrates that there is a sharp transition between orders of growth of k_n where each user can achieve the single-user capacity per unit-energy $\frac{\log e}{N_0}$, i.e., where users can communicate as if free of interference, and orders of growth where no positive rate per unit-energy is feasible. The transition threshold separating these two regimes is at the order of growth $n/\log n$. The capacity per unit-energy can be achieved using an orthogonal-access scheme where each user is assigned an exclusive time slot. As we shall show in Section IV, such an access scheme is wasteful in terms of resources and strictly suboptimal when users are active only sporadically. The theorem also demonstrates that, when the order of growth of k_n is exactly equal to $n/\log n$, the capacity per unit-energy is strictly positive, but also strictly less than $\frac{\log e}{N_0}$.

As mentioned in the introduction, when the number of users is finite, all users can achieve the single-user capacity per unit-energy $\frac{\log e}{N_0}$ by an orthogonal-access scheme where each user uses an orthogonal codebook. In the following theorem, we show that this is not necessarily the case anymore when the number of users grows with the blocklength.

Theorem 2: The largest rate per unit-energy $\dot{C}_{\perp\perp}$ achievable with an orthogonal-access scheme and orthogonal codebooks has the following behavior:

- 1) If $k_n = o(n^c)$ for every $c > 0$, then $\dot{C}_{\perp\perp} = \frac{\log e}{N_0}$.
- 2) If $k_n = \Theta(n^c)$, then

$$\dot{C}_{\perp\perp} = \begin{cases} \frac{\log e}{N_0} \frac{1}{(1 + \sqrt{1-c})^2}, & \text{if } 0 < c \leq 1/2 \\ \frac{\log e}{2N_0} (1-c), & \text{if } 1/2 < c < 1. \end{cases}$$

Proof: See Section III-C. ■

Theorem 2 shows that an orthogonal-access scheme in combination with orthogonal codebooks is optimal only if k_n grows more slowly than any positive power of n . Part 2) of Theorem 2 gives the largest rate per unit-energy achievable when the order of k_n is a positive power of n .

Remark 3: Observe that the behavior of $\dot{C}_{\perp\perp}$ as a function of c can be divided into two regimes: if $1/2 < c < 1$, then $\dot{C}_{\perp\perp}$ decays linearly in c ; if $0 < c \leq 1/2$, then the dependence of $\dot{C}_{\perp\perp}$ on c is nonlinear. This is a consequence of the behavior of the error exponent achievable with orthogonal codebooks. More specifically, Theorem 2 follows from lower and upper

bounds on the probability of error that become asymptotically tight as $E \rightarrow \infty$; see Lemma 6. The lower bound follows from the sphere-packing bound [15]. The upper bound is obtained by applying Gallager's ρ -trick to improve upon the union bound [16, Sec. 2.5], followed by an optimization over the parameter $0 \leq \rho \leq 1$. When the rate per unit-energy is smaller than $\frac{1}{4} \frac{\log e}{N_0}$, the optimal value of ρ is 1, and the exponent of the upper bound depends linearly on the rate per unit-energy. For rates per unit-energy above $\frac{1}{4} \frac{\log e}{N_0}$, the optimal value of ρ depends on the rate per unit-energy, which results in a nonlinear dependence of the exponent on the rate per unit-energy. This behavior of the error exponent as a function of the rate per unit-energy translates to the two regimes of $\dot{C}_{\perp\perp}$ observed in Theorem 2.

Next we discuss the behavior of the capacity per unit-energy for APE. We show that, if the order of growth of k_n is sublinear, then each user can achieve the single-user capacity per unit-energy $\frac{\log e}{N_0}$. Conversely, if the growth of k_n is linear or above, then the capacity per unit-energy is zero. We have the following theorem.

Theorem 3: The capacity per unit-energy \dot{C}^A for APE has the following behavior:

- 1) If $k_n = o(n)$, then $\dot{C}^A = \frac{\log e}{N_0}$. Furthermore, the capacity per unit-energy can be achieved by an orthogonal-access scheme where each user uses an orthogonal codebook.
- 2) If $k_n = \Omega(n)$, then $\dot{C}^A = 0$.

Proof: See Section III-D. ■

Theorem 3 demonstrates that, under APE, the capacity per unit-energy has a similar behavior as under JPE. Again, there is a sharp transition between orders of growth of k_n where interference-free communication is possible and orders of growth where no positive rate per unit-energy is feasible. The main difference is that the transition threshold is shifted from $n/\log n$ to n . Such an improvement on the order of growth is possible because, for the probability of error to vanish as $n \rightarrow \infty$, the energy E_n needs to satisfy different necessary constraints under JPE and APE. Indeed, we show in the proof of Theorem 1 that the JPE vanishes only if the energy E_n scales logarithmically in the number of users (Lemma 5), and a positive rate per unit-energy is feasible only if the total power $k_n E_n/n$ is bounded in n . No sequence $\{E_n\}$ can satisfy both these conditions if $k_n = \omega(n/\log n)$. In contrast, for the APE to vanish asymptotically, the energy E_n does not need to grow logarithmically in the number of users, it suffices that it tends to infinity as $n \rightarrow \infty$. We can then find sequences $\{E_n\}$ that tend to infinity and for which $k_n E_n/n$ is bounded if, and only if, k_n is sublinear in n . Also note that, for APE, an orthogonal-access scheme with orthogonal codebooks is optimal for all orders of k_n , whereas for JPE it is only optimal if k_n grows more slowly than any positive power of n .

B. Proof of Theorem 1

We first give an outline of the proof of Theorem 1. To prove Part 1), we use an orthogonal-access scheme where the total number of channel uses is divided equally among all users. Each user uses the same single-user code in the assigned channel uses. The receiver decodes the message of each user separately, which is possible because the access scheme is

orthogonal. We next express the overall probability of error in terms of the number of users k_n and the probability of error achieved by the single-user code in an AWGN channel, which we then show vanishes as $n \rightarrow \infty$ if $k_n = o(n/\log n)$. The proof of Part 2) hinges mainly on two facts. The first one is that the probability of error vanishes only if the energy E_n scales at least logarithmically in the number of users, i.e., $E_n = \Omega(\log k_n)$.² The second one is that we have $\dot{R} > 0$ only if the total power $k_n E_n/n$ is bounded as $n \rightarrow \infty$, which is a direct consequence of Fano's inequality. If $k_n = \omega(n/\log n)$, then there is no sequence $\{E_n\}$ that simultaneously satisfies these two conditions. Part 3) follows by revisiting the proofs of Parts 1) and 2) for the case where $k_n = \Theta(n/\log n)$.

1) *Proof of Part 1):* The achievability uses an orthogonal-access scheme where, in each time step, only one user transmits, the other users remain silent. We first note that the probability of correct decoding of any orthogonal-access scheme is given by

$$P_c^{(n)} = \prod_{i=1}^{k_n} (1 - P_{e,i})$$

where $P_{e,i} = \Pr(\hat{W}_i \neq W_i)$ denotes the probability of error in decoding user i 's message. In addition, if each user follows the same coding scheme, then the probability of correct decoding is given by

$$P_c^{(n)} = (1 - P_{e,1})^{k_n}. \quad (8)$$

For a Gaussian point-to-point channel with blocklength N and power constraint P , i.e., $\frac{E_N}{N} \leq P$, there exists an encoding and decoding scheme whose average probability of error is upper-bounded by

$$P(\mathcal{E}) \leq M_N^\rho \exp[-NE_0(\rho, P)], \quad \text{for every } 0 < \rho \leq 1 \quad (9)$$

where

$$E_0(\rho, P) \triangleq \frac{\rho}{2} \ln \left(1 + \frac{2P}{(1+\rho)N_0} \right).$$

This bound is due to Gallager and can be found in [18, Sec. 7.4].

Now let us consider an orthogonal-access scheme in which each user gets n/k_n channel uses and we timeshare between users. Each user follows the coding scheme that achieves (9) with power constraint $P_n = \frac{E_n}{n/k_n}$. Note that this coding scheme satisfies also the energy constraint (5). Then, we obtain the following upper bound $P_{e,1}$ for a fixed rate per unit-energy $\dot{R} = \frac{\log M_n}{\frac{E_n}{n/k_n}}$ by substituting in (9) N by n/k_n and P by $P_n = \frac{E_n}{n/k_n}$:

$$\begin{aligned} P_{e,1} &\leq M_n^\rho \exp \left[-\frac{n}{k_n} E_0(\rho, P_n) \right] \\ &= \exp \left[\rho \ln M_n - \frac{n}{k_n} \frac{\rho}{2} \ln \left(1 + \frac{2E_n k_n/n}{(1+\rho)N_0} \right) \right] \\ &= \exp \left[-E_n \rho \left(\frac{\ln \left(1 + \frac{2E_n k_n/n}{(1+\rho)N_0} \right)}{2E_n k_n/n} - \frac{\dot{R}}{\log e} \right) \right]. \quad (10) \end{aligned}$$

²A similar bound was presented in [17, p. 82] for the case where $M_n = 2$.

Combining (10) with (8), we obtain that the probability of correct decoding can be lower-bounded as

$$1 - P_e^{(n)} \geq \left(1 - \exp \left[-E_n \rho \left(\frac{\ln(1 + \frac{2E_n k_n/n}{(1+\rho)N_0})}{2E_n k_n/n} - \frac{\dot{R}}{\log e} \right) \right] \right)^{k_n}. \quad (11)$$

We next choose $E_n = c_n \ln n$ with $c_n \triangleq \ln(\frac{n}{k_n \ln n})$. Since, by assumption, $k_n = o(n/\log n)$, this implies that $\frac{k_n E_n}{n} \rightarrow 0$ as $n \rightarrow \infty$. Consequently, the first term in the inner-most bracket in (11) tends to $1/((1+\rho)N_0)$ as $n \rightarrow \infty$. It follows that for $\dot{R} < \frac{\log e}{N_0}$, there exists a sufficiently large n_0 , a $0 < \rho \leq 1$, and a $\delta > 0$ such that, for all $n \geq n_0$, the right-hand side (RHS) of (11) is lower-bounded by $(1 - \exp[-E_n \rho \delta])^{k_n}$. Since $c_n \delta \rho \rightarrow \infty$ as $n \rightarrow \infty$, we have

$$\begin{aligned} (1 - \exp[-E_n \rho \delta])^{k_n} &\geq \left(1 - \frac{1}{n^2} \right)^{k_n} \\ &\geq \left(1 - \frac{1}{n^2} \right)^{\frac{n}{\log n}} \\ &= \left[\left(1 - \frac{1}{n^2} \right)^{n^2} \right]^{\frac{1}{n \log n}} \end{aligned} \quad (12)$$

for $n \geq n_0$ and sufficiently large n_0 such that $c_n \delta \rho \geq 2$ and $k_n \leq \frac{n}{\log n}$. Noting that $(1 - \frac{1}{n^2})^{n^2} \rightarrow 1/e$ and $\frac{1}{n \log n} \rightarrow 0$ as $n \rightarrow \infty$, we obtain that the RHS of (12) tends to one as $n \rightarrow \infty$. This implies that, if $k_n = o(n/\log n)$, then any rate per unit-energy $\dot{R} < \frac{\log e}{N_0}$ is achievable.

2) *Proof of Part 2):* Let \mathbf{W} and $\hat{\mathbf{W}}$ denote the vectors (W_1, \dots, W_{k_n}) and $(\hat{W}_1, \dots, \hat{W}_{k_n})$, respectively. Then

$$\begin{aligned} k_n \log M_n &= H(\mathbf{W}) \\ &= H(\mathbf{W} | \hat{\mathbf{W}}) + I(\mathbf{W}; \hat{\mathbf{W}}) \\ &\leq 1 + P_e^{(n)} k_n \log M_n + I(\mathbf{X}; \mathbf{Y}) \end{aligned}$$

by Fano's inequality and the data processing inequality. By following [19, Sec. 15.3], it can be shown that $I(\mathbf{X}; \mathbf{Y}) \leq \frac{n}{2} \log \left(1 + \frac{2k_n E_n}{nN_0} \right)$. Consequently,

$$\frac{\log M_n}{E_n} \leq \frac{1}{k_n E_n} + \frac{P_e^{(n)} \log M_n}{E_n} + \frac{n}{2k_n E_n} \log \left(1 + \frac{2k_n E_n}{nN_0} \right).$$

This implies that the rate per unit-energy $\dot{R} = (\log M_n)/E_n$ is upper-bounded by

$$\dot{R} \leq \frac{\frac{1}{k_n E_n} + \frac{n}{2k_n E_n} \log \left(1 + \frac{2k_n E_n}{nN_0} \right)}{1 - P_e^{(n)}}. \quad (13)$$

We next show by contradiction that, if $k_n = \omega(n/\log n)$, then $P_e^{(n)} \rightarrow 0$ as $n \rightarrow \infty$ only if $\dot{C} = 0$. Thus, assume that $k_n = \omega(n/\log n)$ and that there exists a code with rate per unit-energy $\dot{R} > 0$ such that $P_e^{(n)} \rightarrow 0$ as $n \rightarrow \infty$. To prove that there is a contradiction we need the following lemma.

Lemma 4: If $M_n \geq 2$, then $P_e^{(n)} \rightarrow 0$ only if $E_n \rightarrow \infty$.

Proof: See Appendix I. ■

By the assumption $\dot{R} > 0$, we have that $M_n \geq 2$. Since we further assumed that $P_e^{(n)} \rightarrow 0$, Lemma 4 implies that

$E_n \rightarrow \infty$. Together with (13), this in turn implies that $\dot{R} > 0$ is only possible if $k_n E_n/n$ is bounded in n . Thus,

$$E_n = O(n/k_n). \quad (14)$$

The next lemma presents another necessary condition on the order of E_n which contradicts (14).

Lemma 5: If $\dot{R} > 0$ and $k_n \geq 5$, then $P_e^{(n)} \rightarrow 0$ only if $E_n = \Omega(\log k_n)$.

Proof: This lemma is a special case of Lemma 12 stated in the proof of Theorem 7 in Section IV-B and proven in Appendix IV. ■

We finish the proof by showing that, if $k_n = \omega(n/\log n)$, then there exists no sequence $\{E_n\}$ of order $\Omega(\log k_n)$ that satisfies (14). Indeed, $E_n = \Omega(\log k_n)$ and $k_n = \omega(n/\log n)$ imply that

$$E_n = \Omega(\log n) \quad (15)$$

because the order of E_n is lower-bounded by the order of $\log n - \log \log n$, and $\log n - \log \log n = \Theta(\log n)$. Furthermore, (14) and $k_n = \omega(n/\log n)$ imply that

$$E_n = o(\log n). \quad (16)$$

Since no sequence $\{E_n\}$ can simultaneously satisfy (15) and (16), this contradicts the assumption that there exists a code with a positive rate per unit-energy such that the probability of error vanishes as n tends to infinity. Consequently, if $k_n = \omega(n/\log n)$, then no positive rate per unit-energy is achievable. This proves Part 2) of Theorem 1.

3) *Proof of Part 3):* To show that $\dot{C} > 0$, we use the same orthogonal-access scheme as in the proof of Part 1) of Theorem 1. Thus, each user is assigned n/k_n channel uses, and only one user transmits at a time. We further assume that each user uses energy $E_n = c \log n$, where c is some positive constant to be determined later. By the assumption $k_n = \Theta(n/\log n)$, there exist $n_0 > 0$ and $0 < a_1 \leq a_2$ such that, for all $n \geq n_0$, we have

$$a_1 \frac{n}{\log n} \leq k_n \leq a_2 \frac{n}{\log n}. \quad (17)$$

The probability of error in decoding the first user's message is then given by (10), namely,

$$\begin{aligned} P_{e,1} &\leq \exp \left[-E_n \rho \left(\frac{\ln(1 + \frac{2E_n k_n/n}{(1+\rho)N_0})}{2E_n k_n/n} - \frac{\dot{R}}{\log e} \right) \right] \\ &\leq \exp \left[-c \log n \rho \left(\frac{\ln(1 + \frac{2a_2 c}{(1+\rho)N_0})}{2a_2 c} - \frac{\dot{R}}{\log e} \right) \right] \end{aligned} \quad (18)$$

for every $0 < \rho \leq 1$, $n \geq n_0$, where the last inequality follows since $k_n E_n/n \leq a_2 c$ for $n \geq n_0$.

We next set

$$\dot{R} = \frac{\log e}{2} \frac{\ln(1 + \frac{2a_2 c}{(1+\rho)N_0})}{2a_2 c}$$

which is clearly positive for fixed a_2 , c , and ρ . The upper bound (18) then becomes

$$P_{e,1} \leq \exp \left[-\log n \frac{\rho}{2} c \frac{\ln(1 + \frac{2a_2 c}{(1+\rho)N_0})}{2a_2 c} \right], \quad n \geq n_0. \quad (19)$$

For every fixed a_2 and ρ , the term

$$\frac{\rho}{2} c \frac{\ln\left(1 + \frac{2a_2 c}{(1+\rho)N_0}\right)}{2a_2 c} = \frac{\rho}{2} \frac{\ln\left(1 + \frac{2a_2 c}{(1+\rho)N_0}\right)}{2a_2}$$

is a continuous, monotonically increasing, function of c that is independent of n and ranges from zero to infinity. We can therefore find a c such that (19) simplifies to

$$P_{e,1} \leq \exp[-\ln n] = \frac{1}{n}, \quad n \geq n_0.$$

The above scheme has a positive rate per unit-energy. It remains to show that this rate per unit-energy is also achievable, i.e., that the overall probability of correct decoding tends to one as $n \rightarrow \infty$. To this end, we use (8) to obtain that

$$\begin{aligned} 1 - P_e^{(n)} &= (1 - P_{e,1})^{k_n} \\ &\geq \left(1 - \frac{1}{n}\right)^{a_2 n / \log n}, \quad n \geq n_0. \end{aligned} \quad (20)$$

Since $(1 - \frac{1}{n})^n \rightarrow 1/e$ and $\frac{a_2 n}{\log n} \rightarrow 0$ as $n \rightarrow \infty$, the RHS of (20) tends to one as $n \rightarrow \infty$, hence so does the probability of correct decoding.

We next show that $\dot{C} < \frac{\log e}{N_0}$. Lemma 5 implies that, if $k_n = \Theta(n/\log n)$, then $P_e^{(n)}$ vanishes only if $E_n = \Omega(\log n)$. Furthermore, if $E_n = \omega(\log n)$, then it follows from (13) that $\dot{C} = 0$ since, in this case, $k_n E_n/n$ tends to infinity as $n \rightarrow \infty$. Without loss of generality, we can thus assume that E_n must satisfy $E_n = \Theta(\log n)$. Thus, there exist $n'_0 > 0$ and $0 < l_1 \leq l_2$ such that, for all $n \geq n'_0$, we have $l_1 \log n \leq E_n \leq l_2 \log n$. Together with (17), this implies that $\frac{k_n E_n}{N_0} \geq a_1 l_1$ for all $n \geq \max(n_0, n'_0)$. The claim that $\dot{C} < \frac{\log e}{N_0}$ follows then directly from (13). Indeed, using that $\frac{\log(1+x)}{x} < \log e$ for every $x > 0$, we obtain that

$$\begin{aligned} \frac{n}{2k_n E_n} \log\left(1 + \frac{2k_n E_n}{nN_0}\right) &\leq \frac{1}{2a_1 l_1} \log\left(1 + \frac{2a_1 l_1}{N_0}\right) \\ &< \frac{\log e}{N_0}, \quad n \geq \max(n_0, n'_0). \end{aligned} \quad (21)$$

By (13), in the limit as $P_e^{(n)} \rightarrow 0$ and $E_n \rightarrow \infty$, the rate per unit-energy is upper-bounded by (21). It thus follows that $\dot{C} < \frac{\log e}{N_0}$, which concludes the proof of Part 3) of Theorem 1.

C. Proof of Theorem 2

The proof of Theorem 2 is based on the following lemma, which presents bounds on the probability of error achievable over a Gaussian point-to-point channel with an orthogonal codebook.

Lemma 6: The probability of error $P_{e,1} = \Pr(\hat{W} \neq W)$ achievable over a Gaussian point-to-point channel with an orthogonal codebook with M codewords and energy less than or equal to E satisfies the following bounds:

$$\begin{aligned} 1) \text{ For } 0 < \dot{R} \leq \frac{1}{4} \frac{\log e}{N_0}, \\ e^{-\frac{\ln M}{\dot{R}} \left(\frac{\log e}{2N_0} - \dot{R} + \beta_E\right)} \leq P_{e,1} \leq e^{-\frac{\ln M}{\dot{R}} \left(\frac{\log e}{2N_0} - \dot{R}\right)}. \end{aligned} \quad (22)$$

$$\begin{aligned} 2) \text{ For } \frac{1}{4} \frac{\log e}{N_0} \leq \dot{R} \leq \frac{\log e}{N_0}, \\ e^{-\frac{\ln M}{\dot{R}} \left(\left(\sqrt{\frac{\log e}{N_0}} - \sqrt{\dot{R}}\right)^2 + \beta'_E\right)} \\ \leq P_{e,1} \leq e^{-\frac{\ln M}{\dot{R}} \left(\sqrt{\frac{\log e}{N_0}} - \sqrt{\dot{R}}\right)^2}. \end{aligned} \quad (23)$$

In (22) and (23), β_E and β'_E are some functions of E that are of order $O(\frac{1}{\sqrt{E}})$.

Proof: The upper bounds in (22) and (23) are obtained by upper-bounding the probability of error using Gallager's ρ -trick to improve upon the union bound [16, Sec. 2.5], followed by a maximization over ρ . For $0 < \dot{R} \leq \frac{1}{4} \frac{\log e}{N_0}$, the optimal ρ is equal to 1; for $\frac{1}{4} \frac{\log e}{N_0} \leq \dot{R} \leq \frac{\log e}{N_0}$, the optimal ρ is a function of \dot{R} . Hence, the upper bounds in (22) and (23) have different dependencies on \dot{R} . The lower bounds in (22) and (23) follow from the sphere-packing bound by Shannon, Gallager, and Berlekamp [15]. However, their approach to improve the sphere-packing bound at low rates by writing codewords as concatenations of subcodewords and lower-bounding the error exponent by the convex combination of the error exponents of these subcodewords does not directly apply to our setting where $\log M/E$ is held fixed and $E \rightarrow \infty$ (rather than $\log M/n$ is held fixed and $n \rightarrow \infty$). The reason is that, for some orthogonal codebooks, the energy of one of the subcodebooks is always zero, resulting in a trivial case where the Shannon-Gallager-Berlekamp approach cannot improve upon the original sphere-packing bound. To sidestep this problem, we lower-bound the probability of error by first rotating the orthogonal codebook in such a way that the energy of each subcodeword is proportional to its blocklength, after which the Shannon-Gallager-Berlekamp approach can be applied. For a full proof of Lemma 6, see Appendix II. ■

Next, we define

$$a \triangleq \begin{cases} \frac{\left(\frac{\log e}{2N_0} - \dot{R}\right)}{\dot{R}}, & \text{if } 0 < \dot{R} \leq \frac{1}{4} \frac{\log e}{N_0} \\ \frac{\left(\sqrt{\frac{\log e}{N_0}} - \sqrt{\dot{R}}\right)^2}{\dot{R}}, & \text{if } \frac{1}{4} \frac{\log e}{N_0} \leq \dot{R} \leq \frac{\log e}{N_0} \end{cases} \quad (24)$$

and let $a_E \triangleq a + \max\{\beta_E, \beta'_E\}$. Then, the bounds in Lemma 6 can be written as

$$1/M^{a_E} \leq P_{e,1} \leq 1/M^a. \quad (25)$$

Next, let us consider the case where the users apply an orthogonal-access scheme together with orthogonal codebooks. For such a scheme, the collection of codewords from all users is orthogonal, hence there are at most n codewords of length n . Since, with a symmetric code, each user transmits the same number of messages, it follows that each user transmits $M_n = n/k_n$ messages with codewords of energy less than or equal to E_n . In this case, we obtain from (8) and (25) that

$$\left(1 - \left(\frac{k_n}{n}\right)^a\right)^{k_n} \leq (1 - P_{e,1})^{k_n} \leq \left(1 - \left(\frac{k_n}{n}\right)^{a_{E_n}}\right)^{k_n}$$

which, denoting $a_n \triangleq a_{E_n}$, can be written as

$$\left[\left(1 - \left(\frac{k_n}{n} \right)^a \right)^{\left(\frac{n}{k_n} \right)^a} \right]^{\frac{k_n^{1+a}}{n^a}} \leq (1 - P_{e,1})^{k_n} \leq \left[\left(1 - \left(\frac{k_n}{n} \right)^{a_n} \right)^{\left(\frac{n}{k_n} \right)^{a_n}} \right]^{\frac{k_n^{1+a_n}}{n^{a_n}}}. \quad (26)$$

Since Theorem 2 only concerns a sublinear number of users, we have

$$\lim_{n \rightarrow \infty} \left(1 - \left(\frac{k_n}{n} \right)^a \right)^{\left(\frac{n}{k_n} \right)^a} = \frac{1}{e}.$$

Furthermore, if $P_e^{(n)} \rightarrow 0$ then, by Lemma 4, $E_n \rightarrow \infty$ as $n \rightarrow \infty$. In this case, a_n converges to the finite value a as $n \rightarrow \infty$, and we obtain

$$\lim_{n \rightarrow \infty} \left(1 - \left(\frac{k_n}{n} \right)^{a_n} \right)^{\left(\frac{n}{k_n} \right)^{a_n}} = \frac{1}{e}.$$

So (26) implies that $P_e^{(n)} \rightarrow 0$ as $n \rightarrow \infty$ if

$$\lim_{n \rightarrow \infty} \frac{k_n^{1+a}}{n^a} = 0 \quad (27)$$

and only if

$$\lim_{n \rightarrow \infty} \frac{k_n^{1+a_n}}{n^{a_n}} = 0. \quad (28)$$

We next use these observations to prove Parts 1) and 2) of Theorem 2. We begin with Part 1). Let $\dot{R} < \frac{\log e}{N_0}$. In this case we have $a > 0$, which implies that we can find a constant $\eta < a/(1+a)$ such that $n^{\eta(1+a)}/n^a \rightarrow 0$ as $n \rightarrow \infty$. Since, by assumption, $k_n = o(n^c)$ for every $c > 0$, it follows that there exists an n_0 such that, for all $n \geq n_0$, we have $k_n \leq n^{\eta(1+a)}$. This implies that (27) is satisfied, from which Part 1) follows.

We next prove Part 2) of Theorem 2. Indeed, if $k_n = \Theta(n^c)$, $0 < c < 1$, then there exist $0 < l_1 \leq l_2$ and n_0 such that, for all $n \geq n_0$, we have $(l_1 n)^c \leq k_n \leq (l_2 n)^c$. Consequently,

$$\frac{(l_1 n)^{c(1+a_n)}}{n^{a_n}} \leq \frac{k_n^{1+a_n}}{n^{a_n}} \leq \frac{(l_2 n)^{c(1+a_n)}}{n^{a_n}}. \quad (29)$$

If $P_e^{(n)} \rightarrow 0$, then from (28) we have $\frac{k_n^{1+a_n}}{n^{a_n}} \rightarrow 0$. Thus, (29) implies that $c(1+a_n) - a_n$ converges to a negative value. Since $c(1+a_n) - a_n$ tends to $c(1+a) - a$ as $n \rightarrow \infty$, it follows that $P_e^{(n)} \rightarrow 0$ only if $c(1+a) - a < 0$, which is the same as $a > c/(1-c)$. Using similar arguments, it follows from (27) that if $a > c/(1-c)$, then $P_e^{(n)} \rightarrow 0$. Hence, $P_e^{(n)} \rightarrow 0$ if, and only if, $a > c/(1-c)$. It can be observed from (24) that a is a monotonically decreasing function of \dot{R} . So, for $k_n = \Theta(n^c)$, $0 < c < 1$, the capacity per unit-energy $\dot{C}_{\perp\perp}$ is given by

$$\dot{C}_{\perp\perp} = \sup\{\dot{R} \geq 0 : a(\dot{R}) > c/(1-c)\}$$

where we write $a(\dot{R})$ to make it clear that a as defined in (24) is a function of \dot{R} . This supremum can be computed as

$$\dot{C}_{\perp\perp} = \begin{cases} \frac{\log e}{N_0} \left(\frac{1}{1 + \sqrt{1-c}} \right)^2, & \text{if } 0 < c \leq 1/2 \\ \frac{\log e}{2N_0} (1-c), & \text{if } 1/2 < c < 1 \end{cases}$$

which proves Part 2) of Theorem 2.

D. Proof of Theorem 3

1) *Proof of Part 1):* We first argue that $P_{e,A}^{(n)} \rightarrow 0$ only if $E_n \rightarrow \infty$, and that in this case, $\dot{C}^A \leq \frac{\log e}{N_0}$. Indeed, let $P_{e,i} \triangleq \Pr\{\hat{W}_i \neq W_i\}$ denote the probability that message W_i is decoded erroneously. We then have that $P_{e,A}^{(n)} \geq \min_i P_{e,i}$. Furthermore, $P_{e,i}$ is lower-bounded by the error probability of the Gaussian single-user channel, since a single-user channel can be obtained from the MnAC if a genie informs the receiver about the codewords transmitted by users $j \neq i$. By applying the lower bound [20, Eq. (30)] on the error probability of the Gaussian single-user channel, we thus obtain

$$P_{e,A}^{(n)} \geq Q \left(\sqrt{\frac{2E_n}{N_0}} \right), \quad M_n \geq 2 \quad (30)$$

where Q denotes the tail distribution function of the standard Gaussian distribution. Hence, $P_{e,A}^{(n)} \rightarrow 0$ only if $E_n \rightarrow \infty$. As mentioned in Remark 1, when E_n tends to infinity as $n \rightarrow \infty$, the capacity per unit-energy \dot{C}^A coincides with the capacity per unit-energy defined in [14], which for the Gaussian single-user channel is given by $\frac{\log e}{N_0}$ [14, Ex. 3]. Furthermore, if $P_{e,A}^{(n)} \rightarrow 0$ as $n \rightarrow \infty$, then there exists at least one user i for which $P_{e,i} \rightarrow 0$ as $n \rightarrow \infty$. By the above genie argument, this user's rate per unit-energy is upper-bounded by the capacity per unit-energy of the Gaussian single-user channel. Since, for the class of symmetric codes considered in this paper, each user transmits at the same rate per unit-energy, we conclude that $\dot{C}^A \leq \frac{\log e}{N_0}$.

We next show that any rate per unit-energy $\dot{R} < \frac{\log e}{N_0}$ is achievable by an orthogonal-access scheme where each user uses an orthogonal codebook of blocklength n/k_n . To transmit message w_i , user i sends in his assigned slot the codeword $\mathbf{x}(w_i) = (x_1(w_i), \dots, x_{n/k_n}(w_i))$, which is given by

$$x_j(w_i) = \begin{cases} \sqrt{E_n}, & \text{if } j = w_i \\ 0, & \text{otherwise.} \end{cases}$$

To show that the probability of error vanishes, we use the following bound from Lemma 6:

$$P_{e,i} \leq \begin{cases} e^{-\frac{\ln M_n}{\dot{R}} \left(\frac{\log e}{2N_0} - \dot{R} \right)}, & \text{if } 0 < \dot{R} \leq \frac{1}{4} \frac{\log e}{N_0} \\ e^{-\frac{\ln M_n}{\dot{R}} \left(\sqrt{\frac{\log e}{N_0}} - \sqrt{\dot{R}} \right)^2}, & \text{if } \frac{1}{4} \frac{\log e}{N_0} \leq \dot{R} \leq \frac{\log e}{N_0}. \end{cases} \quad (31)$$

It follows from (31) that, if $\dot{R} < \frac{\log e}{N_0}$ and $M_n \rightarrow \infty$ as $n \rightarrow \infty$, then $P_{e,i}, i = 1, \dots, k_n$ tends to zero as $n \rightarrow \infty$. Since $k_n = o(n)$, it follows that $M_n = n/k_n$ tends to ∞ , as $n \rightarrow \infty$. Thus, for any $\dot{R} < \frac{\log e}{N_0}$, the probability of error $P_{e,i}$ vanishes. This implies that also $P_{e,A}^{(n)}$ vanishes as $n \rightarrow \infty$, thus proving Part 1).

2) *Proof of Part 2):* Fano's inequality yields that

$$\log M_n \leq 1 + P_{e,i} \log M_n + I(W_i; \hat{W}_i), \quad \text{for } i = 1, \dots, k_n.$$

Averaging over all i 's then gives

$$\begin{aligned} \log M_n &\leq 1 + \frac{1}{k_n} \sum_{i=1}^{k_n} P_{e,i} \log M_n + \frac{1}{k_n} I(\mathbf{W}; \hat{\mathbf{W}}) \\ &\leq 1 + P_{e,A}^{(n)} \log M_n + \frac{1}{k_n} I(\mathbf{W}; \mathbf{Y}) \\ &\leq 1 + P_{e,A}^{(n)} \log M_n + \frac{n}{2k_n} \log \left(1 + \frac{2k_n E_n}{nN_0} \right) \end{aligned} \quad (32)$$

where the first inequality follows because the messages $W_i, i = 1, \dots, k_n$ are independent and because conditioning reduces entropy, the second inequality follows from the definition of $P_{e,A}^{(n)}$ and the data processing inequality, and the third inequality follows by upper-bounding $I(\mathbf{W}; \mathbf{Y})$ by $\frac{n}{2} \log \left(1 + \frac{2k_n E_n}{nN_0} \right)$.

Dividing both sides of (32) by E_n , and solving the inequality for R^A , we obtain the upper bound

$$R^A \leq \frac{\frac{1}{E_n} + \frac{n}{2k_n E_n} \log \left(1 + \frac{2k_n E_n}{nN_0} \right)}{1 - P_{e,A}^{(n)}}. \quad (33)$$

As argued at the beginning of the proof of Part 1), we have $P_{e,A}^{(n)} \rightarrow 0$ only if $E_n \rightarrow \infty$. If $k_n = \Omega(n)$, then this implies that $k_n E_n/n \rightarrow \infty$ as $n \rightarrow \infty$. It thus follows from (33) that, if $k_n = \Omega(n)$, then $\dot{C}^A = 0$, which is Part 2) of Theorem 3.

IV. CAPACITY PER UNIT-ENERGY OF RANDOM MANY-ACCESS CHANNELS

In this section, we consider the case where the users' activation probability can be strictly smaller than 1. In Subsection IV-A, we discuss the capacity per unit-energy of random MnACs. In particular, we present our main result in Theorem 7, which characterizes the capacity per unit-energy in terms of ℓ_n and k_n . Then, in Theorem 8, we analyze the largest rate per unit-energy achievable using an orthogonal-access scheme. Finally, in Theorem 9, we briefly discuss the behavior of the capacity per unit-energy of random MnAC for APE. The proofs of Theorems 7–9 are presented in Subsections IV-B, IV-C, and IV-D, respectively.

A. Capacity per Unit-Energy of Random MnAC

Before presenting our results, we first note that the case where k_n vanishes as $n \rightarrow \infty$ is uninteresting. Indeed, this case only happens if $\alpha_n \rightarrow 0$. Then, the probability that all the users are inactive, given by $((1 - \alpha_n)^{\frac{1}{\alpha_n}})^{k_n}$, tends to one since $(1 - \alpha_n)^{\frac{1}{\alpha_n}} \rightarrow 1/e$ and $k_n \rightarrow 0$. Consequently, if each user employs a code with $M_n = 2$ and $E_n = 0$ for all n , and if the decoder always declares that all users are inactive, then the probability of error $P_e^{(n)}$ vanishes as $n \rightarrow \infty$. This implies that $\dot{C} = \infty$. In the following, we avoid this trivial case and assume that ℓ_n and α_n are such that $k_n = \Omega(1)$. This implies that the inverse of α_n is upper-bounded by the order of ℓ_n , i.e., $\frac{1}{\alpha_n} = O(\ell_n)$. We have the following theorem.

Theorem 7: Assume that $k_n = \Omega(1)$. Then the capacity per unit-energy of the Gaussian random MnAC has the following behavior:

- 1) If $k_n \log \ell_n = o(n)$, then $\dot{C} = \frac{\log e}{N_0}$.

- 2) If $k_n \log \ell_n = \omega(n)$, then $\dot{C} = 0$.
- 3) If $k_n \log \ell_n = \Theta(n)$, then $0 < \dot{C} < \frac{\log e}{N_0}$.

Proof: See Section IV-B. ■

Theorem 7 demonstrates that there is a sharp transition between orders of growth of k_n and ℓ_n where interference-free communication is feasible and orders of growth where no positive rate per unit-energy is feasible. Recall that the same behavior was observed for the non-random-access case ($\alpha_n = 1$), where the transition threshold separating these two regimes is at the order of growth $n/\log n$, as shown in Theorem 1. For a general α_n , this transition threshold depends both on ℓ_n and k_n . However, if $\liminf_{n \rightarrow \infty} \alpha_n > 0$, then $k_n = \Theta(\ell_n)$ and the order of growth of $k_n \log \ell_n$ coincides with that of both $k_n \log k_n$ and $\ell_n \log \ell_n$. It follows that, in this case, the transition thresholds for both k_n and ℓ_n are also at $n/\log n$, since $k_n \log k_n = \Theta(n)$ is equivalent to $k_n = \Theta(n/\log n)$.

When $\alpha_n \rightarrow 0$, the orders of growth of k_n and ℓ_n are different and the transition threshold for ℓ_n is in general larger than $n/\log n$. For example, when $\ell_n = n$ and $\alpha_n = \frac{1}{\sqrt{n}}$, then $k_n \log \ell_n = \sqrt{n} \log n = o(n)$, so all users can communicate without interference. Thus, random user-activity enables interference-free communication at an order of growth above the limit $n/\log n$. Similarly, when $\alpha_n \rightarrow 0$, the transition threshold for k_n may be smaller than $n/\log n$, even though this is only the case if ℓ_n is superpolynomial in n . For example, when $\ell_n = 2^n$ and $\alpha_n = \frac{\sqrt{n}}{2^n \log n}$, then $k_n = \frac{\sqrt{n}}{\log n} = o(n/\log n)$ and $k_n \log \ell_n = \frac{n^{3/2}}{\log n} = \omega(n)$, so no positive rate per unit-energy is feasible. This implies that treating a random MnAC with ℓ_n users as a non-random MnAC with k_n users may be overly-optimistic, since it suggests that interference-free communication is feasible at orders of growth of k_n where actually no positive rate per unit-energy is feasible.

In the proof of Part 1) of Theorem 1, we have shown that, when $k_n = o(n/\log n)$ and $\alpha_n = 1$, an orthogonal-access scheme achieves the capacity per unit-energy. It turns out that this is not necessarily the case anymore when $\alpha_n \rightarrow 0$, as we show in the following theorem.

Theorem 8: Assume that $k_n = \Omega(1)$. The largest rate per unit-energy \dot{C}_\perp achievable with an orthogonal-access scheme satisfies the following:

- 1) If $\ell_n = o(n/\log n)$, then $\dot{C}_\perp = \frac{\log e}{N_0}$.
- 2) If $\ell_n = \omega(n/\log n)$, then $\dot{C}_\perp = 0$.
- 3) If $\ell_n = \Theta(\frac{n}{\log n})$, then $0 < \dot{C}_\perp < \frac{\log e}{N_0}$.

Proof: See Section IV-C. ■

Observe that there is again a sharp transition between the orders of growth of ℓ_n where interference-free communication is feasible and orders of growth where no positive rate per unit-energy is feasible. In contrast to the optimal transmission scheme, the transition threshold for the orthogonal-access scheme is located at $n/\log n$, irrespective of the behavior of α_n . Thus, by using an orthogonal-access scheme, we treat the random MnAC as if it were a non-random MnAC. This also implies that there are orders of growth of ℓ_n and k_n where non-orthogonal-access schemes are necessary to achieve the capacity per unit-energy.

Next we present our results on the behavior of capacity per unit-energy for APE. To this end, we first note that, if $\alpha_n \rightarrow 0$

as $n \rightarrow \infty$, then $\Pr\{W_i = 0\} \rightarrow 1$ for all $i = 1, \dots, \ell_n$. Consequently, if each user employs a code with $M_n = 2$ and $E_n = 0$ for all n , and if the decoder always declares that all users are inactive, then the APE vanishes as $n \rightarrow \infty$. This implies that $\dot{C}^A = \infty$. In the following, we avoid this trivial case and assume that α_n is bounded away from zero. For $\alpha_n = 1$ ("non-random-access case") and APE, we showed in Theorem 3 that if the number of users grows sublinearly in n , then each user can achieve the single-user capacity per unit-energy, and if the growth is linear or superlinear, then the capacity per unit-energy is zero. Perhaps not surprisingly, the same result holds in the random-access case since, when α_n is bounded away from zero, k_n is of the same order as ℓ_n . We have the following theorem.

Theorem 9: If $\liminf_{n \rightarrow \infty} \alpha_n > 0$, then \dot{C}^A has the following behavior:

- 1) If $\ell_n = o(n)$, then $\dot{C}^A = \frac{\log e}{N_0}$.
- 2) If $\ell_n = \Omega(n)$, then $\dot{C}^A = 0$.

Proof: See Section IV-D. ■

B. Proof of Theorem 7

We first give an outline of the proof. The achievability scheme to show Part 1) is a non-orthogonal-access scheme where the codewords of all users are of length n and the codebooks of different users may be different. In each codebook, the codewords consist of two parts: The first n'' symbols are a signature part that is used to convey to the receiver that the user is active. The remaining $n - n''$ symbols are used to send the message. The decoder follows a two-step decoding process. First, it determines which users are active, then it decodes the messages of all users that are estimated as active. For this decoding process, we analyze two types of errors: the detection error and the decoding error. We show that, if $k_n \log \ell_n$ is sublinear in n , then both the probability of a detection error and the probability of a decoding error tend to zero as $n \rightarrow \infty$. The proof of Part 2) follows along similar lines as that of Part 2) of Theorem 1. We first show that the probability of error vanishes only if the energy E_n scales at least logarithmically in the total number of users, i.e., $E_n = \Omega(\log \ell_n)$. We then show that a positive rate per unit-energy is achievable only if the total power of the active users, given by $k_n E_n / n$, is bounded as $n \rightarrow \infty$. The proof of Part 2) concludes by noting that, if $k_n \log \ell_n$ is superlinear in n , then there is no E_n that can simultaneously satisfy these two conditions. Part 3) follows by revisiting the proofs of Parts 1) and 2) for the case where $k_n \log \ell_n = \Theta(n)$.

1) *Proof of Part 1):* We use an achievability scheme with a decoding process consisting of two steps: First, the receiver determines which users are active. It then fixes an arbitrary positive integer ξ , based on which it decides whether it will decode the messages of all active users, or whether it will declare an error. Specifically, if the number of estimated active users is less than or equal to ξk_n , then the receiver decodes the messages of all active users. If the number of estimated

active users is greater than ξk_n , then it declares an error.³ By the union bound, the total error probability of this scheme can be upper-bounded by

$$P(\mathcal{D}) + \sum_{k'_n=1}^{\xi k_n} \Pr\{K'_n = k'_n\} P_m(k'_n) + \Pr\{K'_n > \xi k_n\}$$

where K'_n is a random variable describing the number of active users, $P(\mathcal{D})$ is the probability of a detection error, and $P_m(k'_n)$ is the probability of a decoding error given that the receiver has correctly detected that there are k'_n active users. In the following, we show that $P(\mathcal{D})$ and $P_m(k'_n)$ vanish as $n \rightarrow \infty$ for any fixed, positive integer ξ . Furthermore, by Markov's inequality, we have that $\Pr\{K'_n > \xi k_n\} \leq 1/\xi$. Consequently, the total probability of error vanishes as we let first $n \rightarrow \infty$ and then $\xi \rightarrow \infty$.

To enable user detection at the receiver, each user sends in the first n'' channel uses to its signature and in the remaining $n' = n - n''$ channel uses its message. The signature uses energy E'_n out of E_n , while the energy used for sending the message is given by $E''_n = E_n - E'_n$.

Let \mathbf{s}_i denote the signature of user i and $\tilde{\mathbf{x}}_i(w_i)$ denote the codeword of length n' for sending message w_i , where $w_i = 1, \dots, M_n$. Then, the codeword $\mathbf{x}_i(w_i)$ is given by the concatenation of \mathbf{s}_i and $\tilde{\mathbf{x}}_i(w_i)$, i.e.,

$$\mathbf{x}_i(w_i) = (\mathbf{s}_i, \tilde{\mathbf{x}}_i(w_i)).$$

For a given arbitrary $0 < b < 1$, we let

$$n'' = bn \tag{34}$$

$$E''_n = bE_n, \quad E_n = c_n \ln \ell_n \tag{35}$$

with $c_n = \ln\left(\frac{n}{k_n \ln \ell_n}\right)$.⁴ Based on the first n'' received symbols, the receiver detects which users are active. We need the following lemma to show that the detection error probability vanishes as $n \rightarrow \infty$.

Lemma 10: Assume that $k_n = \Omega(1)$ and $k_n \log \ell_n = O(n)$, and let $E_n = c_n \ln \ell_n$, where

$$c_n = \begin{cases} \ln\left(\frac{n}{k_n \log \ell_n}\right), & \text{if } k_n \log \ell_n = o(n) \\ c', & \text{if } k_n \log \ell_n = \Theta(n) \end{cases}$$

for some positive constant c' that is independent of n . If c' is sufficiently large, then there exist signatures $\mathbf{s}_i, i = 1, \dots, \ell_n$ with $n'' = bn$ channel uses and energy $E''_n = bE_n$ such that $P(\mathcal{D})$ vanishes as $n \rightarrow \infty$.

Proof: The proof of Lemma 10 follows along similar lines as that of [1, Th. 2]. However, there are some differences in the settings considered. Here, the goal is to achieve user

³The threshold ξk_n becomes inactive when α_n is bounded away from zero. Indeed, the number of estimated active users is a random variable taking value in $\{0, \dots, \ell_n\}$. When α_n is bounded away from zero, $\ell_n = k_n / \alpha_n$ is bounded by ξk_n for some positive integer ξ . Hence, in this case we can find a threshold ξ such that the receiver will never have to declare an error.

⁴In our scheme, a fraction of the total energy must be assigned to the signature part in order to ensure that the detection error probability vanishes as $n \rightarrow \infty$. However, this incurs a loss in rate per unit-energy, so this fraction will be made arbitrarily small at the end of the proof. Alternatively, one could consider a sequence $\{b_n\}$ that satisfies $b_n \rightarrow 0$ and $b_n c_n \rightarrow \infty$ as $n \rightarrow \infty$.

detection with minimum energy, whereas in [1] the goal is to achieve user detection with the minimum number of channel uses. Furthermore, the energy we assign to the signature part is proportional to the total energy E_n , cf. (35), whereas in [1] the energy assigned to the signature part is proportional to the number of channel uses. These differences have the positive effect that, in our proof, the condition [1, Eq. (19)], namely that

$$\lim_{n \rightarrow \infty} \ell_n e^{-\delta k_n} = 0$$

for all $\delta > 0$, is not necessary. For a full proof of Lemma 10, see Appendix III. ■

We next use the following lemma to show that $P_m(k'_n)$ vanishes as $n \rightarrow \infty$ uniformly in $k'_n \in \mathcal{K}_n$, where $\mathcal{K}_n \triangleq \{1, \dots, \xi k_n\}$.

Lemma 11: Let $A_{k'_n} \triangleq \frac{1}{k'_n} \sum_{i=1}^{k'_n} \mathbf{1}(\hat{W}_i \neq W_i)$ and $\mathcal{A}_{k'_n} \triangleq \{1/k'_n, \dots, 1\}$, where $\mathbf{1}(\cdot)$ denotes the indicator function. Then, for any arbitrary $0 < \rho \leq 1$, we have

$$\Pr\{A_{k'_n} = a\} \leq \left(\frac{1}{\mu}\right)^{2k'_n} \binom{k'_n}{ak'_n} M_n^{ak'_n \rho} e^{-n' E_{0,k'_n}(a,\rho,n)}, \quad a \in \mathcal{A}_{k'_n} \quad (36)$$

where

$$E_{0,k'_n}(a,\rho,n) \triangleq \frac{\rho}{2} \ln \left(1 + \frac{a2k'_n E'_n}{n'(\rho+1)N_0}\right) \quad (37)$$

and

$$\mu \triangleq \int \mathbf{1}(\|\mathbf{v}\|^2 \leq E'_n) \prod_{i=1}^{n'} \tilde{q}(v_i) d\mathbf{v} \quad (38)$$

is a normalizing constant. In (38), $\tilde{q}(\cdot)$ denotes the probability density function of a zero-mean Gaussian random variable with variance $E'_n/(2n')$ and $\mathbf{v} = (v_1, v_2, \dots, v_{n'})$.

Proof: The upper bound in (36) without the factor $(1/\mu)^{2k'_n}$ can be obtained using random coding with i.i.d. Gaussian inputs [21, Th. 2]. However, while i.i.d. Gaussian codebooks satisfy the energy constraint on average (averaged over all codewords), there may be some codewords in the codebook that violate it. We therefore need to adapt the proof of [21, Th. 2] as follows. Let

$$\tilde{\mathbf{q}}(\mathbf{v}) = \prod_{i=1}^{n'} \tilde{q}(v_i).$$

For random codewords $\tilde{\mathbf{X}}_i, i = 1, \dots, k'_n$ distributed according to $\tilde{\mathbf{q}}(\cdot)$, the probability $\Pr(A_{k'_n} = a)$ can be upper-bounded as [21, Th. 2]

$$\Pr(A_{k'_n} = a) \leq \binom{k'_n}{ak'_n} M_n^{ak'_n \rho} \times \int \tilde{\mathbf{q}}(\tilde{\mathbf{x}}_{ak'_n+1}) \cdots \tilde{\mathbf{q}}(\tilde{\mathbf{x}}_{k'_n}) G^{1+\rho} d\tilde{\mathbf{x}}_{ak'_n+1} \cdots d\tilde{\mathbf{x}}_{k'_n} d\tilde{\mathbf{y}} \quad (39)$$

where

$$G = \int \tilde{\mathbf{q}}(\tilde{\mathbf{x}}_1) \cdots \tilde{\mathbf{q}}(\tilde{\mathbf{x}}_{ak'_n}) \times (p(\tilde{\mathbf{y}} | \tilde{\mathbf{x}}_1, \dots, \tilde{\mathbf{x}}_{ak'_n}))^{1+\rho} d\tilde{\mathbf{x}}_1 \cdots d\tilde{\mathbf{x}}_{ak'_n}.$$

Using the fact that the channel is memoryless, the RHS of (36) without the factor $(1/\mu)^{2k'_n}$ follows from (39). The case of $k'_n = 2$ was analyzed in [21, Eq. (2.33)].

Now suppose that all codewords are generated according to the distribution

$$\mathbf{q}(\mathbf{v}) = \frac{1}{\mu} \mathbf{1}(\|\mathbf{v}\|^2 \leq E'_n) \tilde{\mathbf{q}}(\mathbf{v}).$$

Clearly, such codewords satisfy the energy constraint E'_n with probability one. Furthermore,

$$\mathbf{q}(\mathbf{v}) \leq \frac{1}{\mu} \tilde{\mathbf{q}}(\mathbf{v}). \quad (40)$$

By replacing $\tilde{\mathbf{q}}(\cdot)$ in (39) by $\mathbf{q}(\cdot)$, and upper-bounding $\mathbf{q}(\cdot)$ by (40), we obtain that

$$\Pr\{A_{k'_n} = a\} \leq \left(\frac{1}{\mu}\right)^{(1+\rho)(ak'_n)} \left(\frac{1}{\mu}\right)^{k'_n - ak'_n} \binom{k'_n}{ak'_n} \times M_n^{ak'_n \rho} e^{-n' E_{0,k'_n}(a,\rho,n)}, \quad a \in \mathcal{A}_{k'_n}. \quad (41)$$

From the definition of μ , we have that $0 < \mu \leq 1$. Since we further have $\rho \leq 1$ and $a \leq 1$, it follows that $(1/\mu)^{(1+\rho)(ak'_n)} \leq (1/\mu)^{ak'_n + k'_n}$. Using this bound in (41), we obtain (36). ■

We next show that $(1/\mu)^{2k'_n} \rightarrow 1$ as $n \rightarrow \infty$ uniformly in $k'_n \in \mathcal{K}_n$. Let \mathbf{H} be a Gaussian vector distributed according to $\tilde{\mathbf{q}}(\cdot)$. Then, by the definition of μ , we have

$$\mu = 1 - \Pr(\|\mathbf{H}_1\|_2^2 > E'_n)$$

so $(1/\mu)^{2k'_n} \geq 1$. Let us consider $\mathbf{H}_0 \triangleq \frac{2n'}{E'_n} \|\mathbf{H}_1\|_2^2$, which has a central chi-square distribution with n' degrees of freedom. Then,

$$\Pr(\|\mathbf{H}_1\|_2^2 > E'_n) = \Pr(\mathbf{H}_0 > 2n').$$

So, from the Chernoff bound we obtain that

$$\Pr(\mathbf{H}_0 > a) \leq \frac{E(e^{t\mathbf{H}_0})}{e^{ta}} = \frac{(1-2t)^{-n'/2}}{e^{ta}}$$

for every $t > 0$. By choosing $a = 2n'$ and $t = \frac{1}{4}$, this yields

$$\Pr(\mathbf{H}_0 > 2n') \leq \frac{\left(\frac{1}{2}\right)^{-n'/2}}{\exp(n'/2)} = \exp\left[-\frac{n'}{2}\tau\right]$$

where $\tau \triangleq (1 - \ln 2)$ is strictly positive. Thus,

$$\begin{aligned} 1 &\leq \left(\frac{1}{\mu}\right)^{2k'_n} \\ &\leq \left(\frac{1}{\mu}\right)^{2\xi k_n} \\ &\leq \left(1 - \exp\left[-\frac{n'}{2}\tau\right]\right)^{-(2\xi k_n)}, \quad k'_n \in \mathcal{K}_n. \end{aligned} \quad (42)$$

By assumption, we have that $k_n = o(n)$ and $n' = \Theta(n)$. For any two non-negative sequences $\{a_n\}$ and $\{b_n\}$ satisfying $a_n \rightarrow 0$ and $a_n b_n \rightarrow 0$ as $n \rightarrow \infty$, it holds that

$(1 - a_n)^{-b_n} \rightarrow 1$ as $n \rightarrow \infty$, so the RHS of (42) tends to one as $n \rightarrow \infty$ uniformly in $k'_n \in \mathcal{K}_n$. It follows that there exists a positive constant n_0 that is independent of k'_n and satisfies

$$\left(\frac{1}{\mu}\right)^{2k'_n} \leq 2, \quad k'_n \in \mathcal{K}_n, n \geq n_0. \quad (43)$$

The probability of error $P_m(k'_n)$ can be written as

$$P_m(k'_n) = \sum_{a \in \mathcal{A}_{k'_n}} \Pr\{A_{k'_n} = a\}. \quad (44)$$

From Lemma 11 and (43), we obtain

$$\begin{aligned} \Pr\{A_{k'_n} = a\} &\leq 2 \binom{k'_n}{ak'_n} M_n^{ak'_n \rho} \exp[-n' E_{0,k'_n}(a, \rho, n)] \\ &\leq 2 \exp[k'_n H_2(a) + a \rho k'_n \log M_n - n' E_{0,k'_n}(a, \rho, n)] \\ &= 2 \exp[-E'_n f_{k'_n}(a, \rho, n)], \quad n \geq n_0 \end{aligned} \quad (45)$$

where $H_2(\cdot)$ denotes the binary entropy function and

$$f_{k'_n}(a, \rho, n) \triangleq \frac{n' E_{0,k'_n}(a, \rho, n)}{E'_n} - \frac{a \rho k'_n \log M_n}{E'_n} - \frac{k'_n H_2(a)}{E'_n}. \quad (46)$$

We next show that, for sufficiently large n , we have

$$\Pr\{A_{k'_n} = a\} \leq 2 \exp[-E'_n f_{\xi k_n}(1/(\xi k_n), \rho, n)], \quad a \in \mathcal{A}_{k'_n}, k'_n \in \mathcal{K}_n. \quad (47)$$

To this end, we lower-bound

$$\begin{aligned} \frac{df_{k'_n}(a, \rho, n)}{da} &\geq \rho k'_n \left[\frac{1}{1 + \frac{2k'_n E'_n}{n'(\rho+1)N_0}} \frac{1}{(1+\rho)N_0} - \frac{\dot{R}}{(1-b)\log e} \right] \\ &\geq \rho \left[\frac{1}{1 + \frac{2\xi k_n E'_n}{n'(\rho+1)N_0}} \frac{1}{(1+\rho)N_0} - \frac{\dot{R}}{(1-b)\log e} \right] \end{aligned} \quad (48)$$

by using simple algebra. The lower bound implies that, for any fixed value of ρ and our choices of E'_n and $\dot{R} = \frac{(1-b)\log e}{(1+\rho)N_0} - \delta$ (for some arbitrary $0 < \delta < \frac{(1-b)\log e}{(1+\rho)N_0}$),

$$\liminf_{n \rightarrow \infty} \min_{k'_n \in \mathcal{K}_n} \min_{a \in \mathcal{A}_{k'_n}} \frac{df_{k'_n}(a, \rho, n)}{da} > 0.$$

Indeed, the RHS of (48) is independent of a and k'_n and tends to $\rho\delta$ as $n \rightarrow \infty$, since $\frac{k_n E'_n}{n'} \rightarrow 0$ by our choice of E'_n and because $k_n = o(n/\log n)$. Thus, for sufficiently large n and a given ρ , the function $a \mapsto f_{k'_n}(a, \rho, n)$ is monotonically increasing on $\mathcal{A}_{k'_n}$ for every $k'_n \in \mathcal{K}_n$. It follows that there exists a positive constant n'_0 that is independent of k'_n and satisfies

$$\min_{a \in \mathcal{A}_{k'_n}} f_{k'_n}(a, \rho, n) = f_{k'_n}(1/k'_n, \rho, n), \quad k'_n \in \mathcal{K}_n, n \geq n'_0.$$

It further follows from the definition of $f_{k'_n}(a, \rho, n)$ in (46) that, for $a = 1/k'_n$ and a given ρ , $f_{k'_n}(a, \rho, n')$ is decreasing

in k'_n , since in this case the first two terms on the RHS of (46) are independent of k'_n and the third term is increasing in k'_n . Hence, we can further lower-bound

$$\min_{a \in \mathcal{A}_{k'_n}} f_{k'_n}(a, \rho, n) \geq f_{\xi k_n}(1/(\xi k_n), \rho, n), \quad k'_n \in \mathcal{K}_n, n \geq n'_0.$$

Next we show that, for our choice of E'_n and \dot{R} , we have

$$\liminf_{n \rightarrow \infty} f_{\xi k_n}(1/(\xi k_n), \rho, n) > 0. \quad (49)$$

Let

$$i_n(\rho) \triangleq \frac{n' E_{0,\xi k_n}(1/(\xi k_n), \rho, n)}{E'_n} \quad (50)$$

$$j(\rho) \triangleq \frac{\rho \dot{R}}{(1-b)\log e} \quad (51)$$

$$h_n(1/(\xi k_n)) \triangleq \frac{\xi k_n H_2(1/(\xi k_n))}{E'_n} \quad (52)$$

so that

$$f_{\xi k_n}(1/(\xi k_n), \rho, n) = j(\rho) \left(\frac{i_n(\rho)}{j(\rho)} - 1 - \frac{h_n(1/(\xi k_n))}{j(\rho)} \right).$$

Note that $\frac{h_n(1/(\xi k_n))}{j(\rho)}$ vanishes as $n \rightarrow \infty$ for our choice of E'_n . Consequently,

$$\liminf_{n \rightarrow \infty} f_{\xi k_n}(1/(\xi k_n), \rho, n) = j(\rho) \left\{ \liminf_{n \rightarrow \infty} \frac{i_n(\rho)}{j(\rho)} - 1 \right\}.$$

The term $j(\rho) = \rho \dot{R}/(1-b)\log e$ is bounded away from zero for our choice of \dot{R} and $\delta < \frac{(1-b)\log e}{(1+\rho)N_0}$. Furthermore, since $E'_n/n' \rightarrow 0$, we get

$$\lim_{n \rightarrow \infty} \frac{i_n(\rho)}{j(\rho)} = \frac{(1-b)\log e}{(1+\rho)N_0 \dot{R}} \quad (53)$$

which is strictly larger than 1 for our choice of \dot{R} . So, (49) follows.

We conclude that there exist two positive constants γ and $n''_0 \geq \max(n_0, n'_0)$ that are independent of k'_n and satisfy $f_{k'_n}(a, \rho, n) \geq \gamma$ for $a \in \mathcal{A}_{k'_n}$, $k'_n \in \mathcal{K}_n$, and $n \geq n''_0$. Consequently, it follows from (45) that, for $n \geq n''_0$,

$$\Pr\{A_{k'_n} = a\} \leq 2e^{-E'_n \gamma}, \quad a \in \mathcal{A}_{k'_n}, k'_n \in \mathcal{K}_n. \quad (54)$$

Since $|\mathcal{A}_{k'_n}| = k'_n$, (44) and (54) yield that

$$P_m(k'_n) \leq k'_n 2e^{-E'_n \gamma}, \quad k'_n \in \mathcal{K}_n, n \geq n''_0.$$

Further upper-bounding $k'_n \leq \xi k_n$, this implies that

$$\sum_{k'_n=1}^{\xi k_n} \Pr\{K'_n = k'_n\} P_m(k'_n) \leq \xi k_n 2e^{-E'_n \gamma}, \quad n \geq n''_0. \quad (55)$$

Since $E'_n = (1-b)c_n \ln \ell_n$ and $k_n = O(\ell_n)$, it follows that the RHS of (55) tends to 0 as $n \rightarrow \infty$ for our choice of $\dot{R} = \frac{(1-b)\log e}{(1+\rho)N_0} - \delta$. Using that ρ, δ , and b are arbitrary, we thus obtain that any rate $\dot{R} < \frac{\log e}{N_0}$ is achievable. This proves Part 1) of Theorem 7.

2) *Proof of Part 2*): Let \hat{W}_i denote the receiver's estimate of W_i , and denote by \mathbf{W} and $\hat{\mathbf{W}}$ the vectors (W_1, \dots, W_{ℓ_n}) and $(\hat{W}_1, \dots, \hat{W}_{\ell_n})$, respectively. The messages W_1, \dots, W_{ℓ_n} are independent, so it follows from (4) that

$$H(\mathbf{W}) = \ell_n H(\mathbf{W}_1) = \ell_n (H_2(\alpha_n) + \alpha_n \log M_n).$$

Since $H(\mathbf{W}) = H(\mathbf{W}|\mathbf{Y}) + I(\mathbf{W}; \mathbf{Y})$, we obtain

$$\ell_n (H_2(\alpha_n) + \alpha_n \log M_n) = H(\mathbf{W}|\mathbf{Y}) + I(\mathbf{W}; \mathbf{Y}). \quad (56)$$

To bound $H(\mathbf{W})$, we use the upper bounds [1, Lemma 2]

$$H(\mathbf{W}|\mathbf{Y}) \leq \log 4 + 4P_e^{(n)}(k_n \log M_n + k_n + \ell_n H_2(\alpha_n) + \log M_n) \quad (57)$$

and

$$I(\mathbf{W}; \mathbf{Y}) \leq \frac{n}{2} \log \left(1 + \frac{2k_n E_n}{nN_0} \right). \quad (58)$$

Using (57) and (58) in (56), rearranging terms, and dividing by $k_n E_n$, yields

$$\begin{aligned} \left(1 - 4P_e^{(n)}(1 + 1/k_n) \right) \dot{R} &\leq \frac{\log 4}{k_n E_n} + \frac{H_2(\alpha_n)}{\alpha_n E_n} (4P_e^{(n)} - 1) \\ &+ 4P_e^{(n)}(1/E_n + 1/k_n) + \frac{n}{2k_n E_n} \log \left(1 + \frac{2k_n E_n}{nN_0} \right). \end{aligned} \quad (59)$$

We next show that, if $k_n \log \ell_n = \omega(n)$, then the RHS of (59) tends to a non-positive value. To this end, we need the following lemma.

Lemma 12: If $\dot{R} > 0$, $\ell_n \geq 5$, and $k_n = \Omega(1)$, then $P_e^{(n)}$ vanishes as $n \rightarrow \infty$ only if $E_n = \Omega(\log \ell_n)$.

Proof: See Appendix IV. ■

Part 2) of Theorem 7 follows now by contradiction. Indeed, let us assume that $k_n \log \ell_n = \omega(n)$, $P_e^{(n)} \rightarrow 0$, and $\dot{R} > 0$. The assumption $k_n \log \ell_n = \omega(n)$ implies that $\ell_n \rightarrow \infty$ as $n \rightarrow \infty$. Then, Lemma 12 together with the assumption that $k_n = \Omega(1)$ implies that $E_n \rightarrow \infty$ and $k_n E_n = \omega(n)$. It follows that the last term on the RHS of (59) tends to zero as $n \rightarrow \infty$. Since $P_e^{(n)}$ tends to zero as $n \rightarrow \infty$, it further follows by the same argument that the first and third term on the RHS of (59) vanish as $n \rightarrow \infty$. Finally, $\frac{H_2(\alpha_n)}{\alpha_n E_n}$ is a sequence of non-negative numbers and $(4P_e^{(n)} - 1) \rightarrow -1$ as $n \rightarrow \infty$, so the second term converges to a non-positive value. Noting that, by the assumption $k_n = \Omega(1)$, the term $(1 - 4P_e^{(n)})(1 + 1/k_n)$ tends to one as $P_e^{(n)} \rightarrow 0$, we thus obtain from (59) that \dot{R} tends to a non-positive value as $n \rightarrow \infty$. This contradicts the assumption $\dot{R} > 0$, so Part 2) of Theorem 7 follows.

3) *Proof of Part 3*): To show that $\dot{C} > 0$ when $k_n \log \ell_n = \Theta(n)$, we use the same achievability scheme and follow the same analysis as in the proof of Part 1) of Theorem 7. That is, each user uses $n'' = bn$ channel uses for sending a signature and $n' = n - n''$ channel uses for sending the message. Furthermore, the decoding process consists of two steps. First, the receiver determines which users are active. If the number of estimated active users is less than or equal to ξk_n (for some arbitrary positive integer ξ), then the receiver decodes in a second step the messages of all active users. If the number of estimated active users is greater than ξk_n , then the receiver declares an error. We set $E_n = c' \ln \ell_n$ for some $c' > 0$ chosen

sufficiently large so that, by Lemma 10, the probability of a detection error vanishes as $n \rightarrow \infty$. We next show that there exists an $\dot{R} > 0$ such that the probability of a decoding error also vanishes as $n \rightarrow \infty$. To this end, we first argue that, if $k_n \log \ell_n = \Theta(n)$, then we can find an $\dot{R} > 0$ such that $f_{k'_n}(a, \rho, n)$ defined in (46) satisfies

$$\liminf_{n \rightarrow \infty} \min_{k'_n \in \mathcal{K}_n} \min_{a \in \mathcal{A}_{k'_n}} f_{k'_n}(a, \rho, n) > 0. \quad (60)$$

In Part 1) of Theorem 7, we proved (60) by first showing that there exists a positive constant n'_0 such that

$$\min_{k'_n \in \mathcal{K}_n} \min_{a \in \mathcal{A}_{k'_n}} f_{k'_n}(a, \rho, n) \geq f_{\xi k_n}(1/(\xi k_n), \rho, n), \quad n \geq n'_0 \quad (61)$$

and then

$$\liminf_{n \rightarrow \infty} f_{\xi k_n}(1/(\xi k_n), \rho, n) > 0. \quad (62)$$

We follow the same steps here, too. Since, by assumption, $k_n E_n = k_n(1-b)c' \ln \ell_n = \Theta(n)$ for every fixed $c' > 0$ and $n' = \Theta(n)$, there exist $r_1 > 0$ and $\tilde{n}_0 > 0$ such that

$$\frac{k_n E_n'}{n'} \leq r_1, \quad n \geq \tilde{n}_0.$$

It then follows from (48) that, for every

$$0 < \dot{R} < \frac{(1-b) \log e}{(\rho+1)N_0 + 2\xi r_1} \quad (63)$$

we have that

$$\liminf_{n \rightarrow \infty} \min_{k'_n \in \mathcal{K}_n} \min_{a \in \mathcal{A}_{k'_n}} \frac{df_{k'_n}(a, \rho, n)}{da} > 0.$$

Thus, for sufficiently large n and a given ρ , the function $a \mapsto f_{k'_n}(a, \rho, n)$ is monotonically increasing on $\mathcal{A}_{k'_n}$ for every $k'_n \in \mathcal{K}_n$. This gives (61).

To prove (62), we write

$$f_{\xi k_n}(1/(\xi k_n), \rho, n) = j(\rho) \left(\frac{i_n(\rho)}{j(\rho)} - 1 - \frac{h_n(1/(\xi k_n))}{j(\rho)} \right) \quad (64)$$

where $i_n(\rho)$, $j(\rho)$, and $h_n(1/(\xi k_n))$ are defined in (50), (51), and (52), respectively. We consider two cases:

Case 1— k_n is unbounded: In this case, the assumption $k_n \log \ell_n = \Theta(n)$ implies that $\Theta(\log \ell_n) = o(n)$. Since $E_n' = \Theta(\log \ell_n)$ for every fixed $c' > 0$, it follows that $E_n'/n' \rightarrow 0$. We thus get (53), namely

$$\lim_{n \rightarrow \infty} \frac{i_n(\rho)}{j(\rho)} = \frac{(1-b) \log e}{\dot{R}(\rho+1)N_0}.$$

If \dot{R} satisfies (63), then this is strictly larger than 1. Furthermore, if k_n is unbounded, then we can make $\frac{h_n(1/(\xi k_n))}{j(\rho)}$ arbitrarily small by choosing c' sufficiently large. Since $j(\rho)$ is bounded away from zero for every positive ρ and \dot{R} , we then obtain (62) from (64).

Case 2— k_n is bounded: In this case, $\Theta(\log \ell_n) = \Theta(k_n \log \ell_n) = \Theta(n)$, so for every fixed $c' > 0$ we have $E'_n = \Theta(n)$. It follows that we can find $r_2 > 0$ and \tilde{n}'_0 such that

$$\frac{2E'_n}{n'(1+\rho)N_0} \leq r_2, \quad n \geq \tilde{n}'_0.$$

If we choose

$$\dot{R} < \frac{\ln(1+r_2)}{r_2} \frac{(1-b)\log e}{(\rho+1)N_0} \quad (65)$$

then

$$\lim_{n \rightarrow \infty} \frac{i_n(\rho)}{j(\rho)} > 1. \quad (66)$$

Furthermore, if k_n is bounded, then $h_n(1/(\xi k_n))$ vanishes as $n \rightarrow \infty$, since ξk_n is bounded and $E'_n \rightarrow \infty$. Recalling that $j(\rho)$ is bounded away from zero for every positive ρ and \dot{R} , we then again obtain (62) from (64).

From (61) and (62), it follows that, for every positive \dot{R} satisfying both (63) and (65), there exist two positive constants γ and $n''_0 \geq \max(n_0, n'_0, \tilde{n}'_0)$ (where n_0 is as in (45)) that are independent of k'_n and satisfy $f_{k'_n}(a, \rho, n) \geq \gamma$ for $a \in \mathcal{A}_{k'_n}$, $k'_n \in \mathcal{K}_n$, and $n \geq n''_0$. It follows from (45) that

$$\begin{aligned} & \sum_{k'_n=1}^{\xi k_n} \Pr\{K'_n = k'_n\} P_m(k'_n) \\ & \leq \xi k_n 2e^{-E'_n \gamma} \\ & = 2\xi \exp\left[-E'_n \left(\gamma - \frac{\ln k_n}{E'_n}\right)\right], \quad n \geq n''_0. \end{aligned} \quad (67)$$

The term

$$\frac{\ln k_n}{E'_n} = \frac{\ln k_n}{(1-b)c' \ln \ell_n}$$

can be made arbitrarily small by choosing c' sufficiently large since $\ln k_n \leq \ln \ell_n$. We thus have that $\frac{\ln k_n}{E'_n} < \gamma$ for sufficiently large c' , in which case the RHS of (67) vanishes as $n \rightarrow \infty$. Since, by Markov's inequality, we further have that $\Pr\{K'_n > \xi k_n\} \leq 1/\xi$, we conclude that the probability of a decoding error vanishes as we let first $n \rightarrow \infty$ and then $\xi \rightarrow \infty$. Consequently, if $k_n \log \ell_n = \Theta(n)$, then $\dot{C} > 0$.

To prove that $\dot{C} < \frac{\log e}{N_0}$, we first note that the assumption $k_n \log \ell_n = \Theta(n)$ implies that $\ell_n \rightarrow \infty$ as $n \rightarrow \infty$. Then, Lemma 12 shows that $P_e^{(n)}$ vanishes as $n \rightarrow \infty$ only if $E_n = \Omega(\log \ell_n)$. This further implies that $P_e^{(n)} \rightarrow 0$ only if $k_n E_n = \Omega(n)$. If $k_n E_n = \omega(n)$, then it follows from the proof of Part 2) of Theorem 7 that $\dot{C} = 0$. We can thus assume without loss of optimality that $k_n E_n = \Theta(n)$. In this case, by following the arguments given in the proof of Part 2) of Theorem 7, we obtain that the first and the third term on the RHS of (59) vanish as $n \rightarrow \infty$. Furthermore, the second term tends to a non-positive value, and the factor $(1 - 4P_e^{(n)}(1 + 1/k_n))$ tends to one. It follows from (59) that

$$\dot{R} \leq \limsup_{n \rightarrow \infty} \frac{n}{2k_n E_n} \log\left(1 + \frac{2k_n E_n}{nN_0}\right). \quad (68)$$

Since $k_n E_n = \Theta(n)$, there exist $n_0 > 0$ and $l_1 > 0$ such that, for $n \geq n_0$, we have $\frac{k_n E_n}{n} \geq l_1$. By noting that

$\frac{\log(1+x)}{x} < \log e$ for every $x > 0$, we thus obtain that the RHS of (68) is strictly less than $\frac{\log e}{N_0}$ for $n \geq n_0$. Hence $\dot{C} < \frac{\log e}{N_0}$, which concludes the proof of Part 3) of Theorem 7.

C. Proof of Theorem 8

1) *Proof of Part 1):* To prove Part 1) of Theorem 8, we present a scheme that is similar to the one used in the proof of Part 1) of Theorem 1. Specifically, each user is assigned n/ℓ_n channel uses, out of which the first one is used for sending a pilot signal and the rest are used for sending the message. Out of the available energy E_n , tE_n (for some arbitrary $0 < t < 1$ to be determined later) is used for the pilot signal and $(1-t)E_n$ is used for sending the message. Let $\tilde{\mathbf{x}}(w)$ denote the codeword of length $\frac{n}{\ell_n} - 1$ for sending message w . Then, user i sends in his assigned slot the codeword

$$\mathbf{x}(w_i) = \left(\sqrt{tE_n}, \tilde{\mathbf{x}}(w_i)\right).$$

The receiver first detects from the pilot signal whether user i is active or not. If the user is estimated as active, then the receiver decodes the user's message. Let $P_{e,i} = \Pr\{\hat{W}_i \neq W_i\}$ denote the probability that user i 's message is decoded erroneously. Since all users follow the same coding scheme, the probability of correct decoding is given by

$$P_c^{(n)} = (1 - P_{e,1})^{\ell_n}. \quad (69)$$

By employing the transmission scheme that was used to prove Theorem 1, we get an upper bound on the probability of error $P_{e,1}$ as follows. Let \mathbf{Y}_1 denote the received vector of length n/ℓ_n corresponding to user 1 in the orthogonal-access scheme. From the pilot signal, which is the first symbol Y_{11} of \mathbf{Y}_1 , the receiver guesses whether user 1 is active or not. Specifically, the user is estimated as active if $Y_{11} > \frac{\sqrt{tE_n}}{2}$ and as inactive otherwise. If the user is declared as active, then the receiver decodes the message from the rest of \mathbf{Y}_1 . Let $\Pr(\hat{W}_1 \neq w | W_1 = w)$ denote the decoding error probability when message $w, w = 0, \dots, M_n$ was transmitted. Then, $P_{e,1}$ is given by

$$\begin{aligned} P_{e,1} &= (1 - \alpha_n) \Pr(\hat{W}_1 \neq 0 | W_1 = 0) \\ &+ \frac{\alpha_n}{M_n} \sum_{w=1}^{M_n} \Pr(\hat{W}_1 \neq w | W_1 = w) \\ &\leq \Pr(\hat{W}_1 \neq 0 | W_1 = 0) \\ &+ \frac{1}{M_n} \sum_{w=1}^{M_n} \Pr(\hat{W}_1 \neq w | W_1 = w). \end{aligned} \quad (70)$$

If $W_1 = 0$, then an error occurs if $Y_{11} > \frac{\sqrt{tE_n}}{2}$. So, we have

$$\Pr(\hat{W}_1 \neq 0 | W_1 = 0) = Q\left(\frac{\sqrt{tE_n}}{2}\right). \quad (71)$$

If $w = 1, \dots, M_n$, then an error occurs either if the user is declared as inactive or if the message is erroneously decoded. An active user is declared as inactive if $Y_{11} < \frac{\sqrt{tE_n}}{2}$. So, by the union bound,

$$\frac{1}{M_n} \sum_{w=1}^{M_n} \Pr(\hat{W}_1 \neq w | W_1 = w) \leq Q\left(\frac{\sqrt{tE_n}}{2}\right) + P_m \quad (72)$$

where P_m is the probability that the decoder correctly declares user 1 as active but erroneously decodes its message. It then follows from (70) and (71) that

$$P_{e,1} \leq 2Q\left(\frac{\sqrt{tE_n}}{2}\right) + P_m. \quad (73)$$

By choosing $E_n = c_n \ln n$ with $c_n = \ln\left(\frac{n}{\ln n}\right)$, we can upper-bound P_m by following the steps that led to (12). Thus, for every $\dot{R} < \frac{\log e}{N_0}$, there exists a sufficiently large n_0 and a $0 < t < 1$ such that

$$P_m \leq \frac{1}{n^2}, \quad n \geq n_0. \quad (74)$$

Furthermore, for the above choice of E_n , there exists a sufficiently large n'_0 such that

$$2Q\left(\frac{\sqrt{tE_n}}{2}\right) \leq \frac{1}{n^2}, \quad n \geq n'_0. \quad (75)$$

Using (74) and (75) in (73), we then obtain from (69) that

$$\begin{aligned} P_c^{(n)} &\geq \left(1 - \frac{2}{n^2}\right)^{\ell_n} \\ &\geq \left(1 - \frac{2}{n^2}\right)^{\frac{n}{\log n}}, \quad n \geq \max(n_0, n'_0) \end{aligned}$$

which tends to one as $n \rightarrow \infty$. This proves Part 1) of Theorem 8.

2) *Proof of Part 2):* Recall that we consider symmetric codes, i.e., the pair (M_n, E_n) is the same for all users. However, each user may be assigned different numbers of channel uses. Let n_i denote the number of channel uses assigned to user i . For an orthogonal-access scheme, if $\ell_n = \omega(n/\log n)$, then there exists at least one user, say $i = 1$, such that $n_i = o(\log n)$. Using that $H(W_1|W_1 \neq 0) = \log M_n$, it follows from Fano's inequality that

$$\log M_n \leq 1 + P_{e,1} \log M_n + \frac{n_1}{2} \log\left(1 + \frac{2E_n}{n_1 N_0}\right).$$

This implies that the rate per unit-energy $\dot{R} = (\log M_n)/E_n$ for user 1 is upper-bounded by

$$\dot{R} \leq \frac{\frac{1}{E_n} + \frac{n_1}{2E_n} \log\left(1 + \frac{2E_n}{n_1 N_0}\right)}{1 - P_{e,1}}. \quad (76)$$

Since $\ell_n = \omega(n/\log n)$, it follows from Lemma 12 that $P_e^{(n)}$ goes to zero only if

$$E_n = \Omega(\log n). \quad (77)$$

Furthermore, (76) implies that $\dot{R} > 0$ only if $E_n = O(n_1)$. Since $n_1 = o(\log n)$, this further implies that

$$E_n = o(\log n). \quad (78)$$

No sequence $\{E_n\}$ can satisfy both (78) and (77) simultaneously. We thus obtain that if $\ell_n = \omega(n/\log n)$, then the capacity per unit-energy is zero. This is Part 2) of Theorem 8.

3) *Proof of Part 3):* To show that $\dot{C}_\perp > 0$ when $\ell_n = \Theta(n/\log n)$, we use the same achievability scheme given in the proof of Part 1) of Theorem 8. That is, each user is assigned n/ℓ_n channel uses, out of which one is used for sending a pilot signal and the rest are used for sending the message. Out of the available energy E_n , tE_n (for some arbitrary $0 < t < 1$ to be determined later) is used for the pilot signal and $(1-t)E_n$ is used for sending the message. We choose $E_n = c' \log n$, where $c' = \frac{c}{1-t}$ and c is chosen as in the proof of Part 3) of Theorem 1. The probability of error in decoding user 1's message is then upper-bounded by (73), namely,

$$P_{e,1} \leq 2Q\left(\frac{\sqrt{tE_n}}{2}\right) + P_m \quad (79)$$

where P_m denotes the probability that the decoder correctly declares user 1 as active but makes an error in decoding its message.

By the assumption $\ell_n = \Theta(n/\log n)$, there exist $n_0 > 0$ and $0 < a_1 \leq a_2$ such that, for $n \geq n_0$, we have $a_1 \frac{n}{\log n} \leq \ell_n \leq a_2 \frac{n}{\log n}$. Since $\alpha_n \leq 1$, it follows that $k_n \leq a_2 \frac{n}{\log n}$ for $n \geq n_0$. By following the proof of Part 3) of Theorem 1, we then obtain that one can set

$$\dot{R} = (1-t) \frac{\log e}{2} \frac{\ln\left(1 + \frac{2a_2 c}{(1+\rho)N_0}\right)}{2a_2 c}$$

(for an arbitrary $0 < \rho \leq 1$) and find a c independent of n and t such that

$$P_m \leq \frac{1}{n}, \quad n \geq n_0. \quad (80)$$

Furthermore, for $E_n = c' \log n$, the upper bound $Q(x) \leq \frac{1}{2}e^{-x^2/2}$, $x \geq 0$ yields that

$$2Q\left(\frac{\sqrt{tE_n}}{2}\right) \leq \exp\left[-\log n \frac{t}{1-t} \frac{c}{8}\right].$$

For every fixed c , the term $\frac{t}{1-t} \frac{c}{8}$ is a continuous, monotonically increasing function of t that is independent of n and ranges from zero to infinity. We can therefore find a $0 < t < 1$ such that

$$2Q\left(\frac{\sqrt{tE_n}}{2}\right) \leq \frac{1}{n}.$$

Together with (79) and (80), this implies that

$$P_{e,1} \leq \frac{2}{n}, \quad n \geq n_0. \quad (81)$$

The above scheme has a positive rate per unit-energy. It remains to show that this rate per unit-energy is also achievable. To this end, we note that, for an orthogonal-access scheme, the probability of correct decoding is given by $P_c^{(n)} = (1 - P_{e,1})^{\ell_n}$. It therefore follows from (81) that

$$P_c^{(n)} \geq \left(1 - \frac{2}{n}\right)^{a_2 \frac{n}{\log n}}, \quad n \geq n_0. \quad (82)$$

Since $\left(1 - \frac{2}{n}\right)^{n/2} \rightarrow 1/e$ and $\frac{2a_2}{\log n} \rightarrow 0$ as $n \rightarrow \infty$, the RHS of (82) tends to one as $n \rightarrow \infty$. This implies that the probability of correct decoding tends to one as $n \rightarrow \infty$, hence the rate per

unit-energy is indeed achievable. Thus, if $\ell_n = \Theta(n/\log n)$, then $\dot{C}_\perp > 0$.

We next show that $\dot{C}_\perp < \frac{\log e}{N_0}$. To this end, we first note that, if $\ell_n = \Theta(\frac{n}{\log n})$, and if we employ an orthogonal-access scheme, then there exists at least one user, say $i = 1$, such that $n_1 = O(\log n)$. That is, there exist $n_0 > 0$ and $a > 0$ such that, for all $n \geq n_0$, we have $n_1 \leq a \log n$. Furthermore, Lemma 12 implies that, if $\ell_n = \Theta(n/\log n)$, then $P_e^{(n)}$ vanishes only if $E_n = \Omega(\log n)$. If $E_n = \omega(\log n)$, then it follows from (76) that a positive \dot{R} is achievable only if $n_1 = \omega(\log n)$, which contradicts the fact that $n_1 = O(\log n)$. We can thus assume without loss of optimality that $E_n = \Theta(\log n)$, i.e., there exist $n'_0 > 0$ and $0 < l_1 \leq l_2$ such that, for all $n \geq n'_0$, we have $l_1 \log n \leq E_n \leq l_2 \log n$. Consequently, $\frac{E_n}{n_1} \geq \frac{l_1}{a}$ for $n \geq \max(n_0, n'_0)$. The claim that $\dot{C}_\perp < \frac{\log e}{N_0}$ follows then directly from (76). Indeed, using that $\frac{\log(1+x)}{x} < \log e$ for every $x > 0$, we obtain that

$$\begin{aligned} \frac{n_1}{2E_n} \log \left(1 + \frac{2E_n}{n_1 N_0} \right) &\leq \frac{a}{2l_1} \log \left(1 + \frac{2l_1}{aN_0} \right) \\ &< \frac{\log e}{N_0}, \quad n \geq \max(n_0, n'_0). \end{aligned} \quad (83)$$

By (76), in the limit as $P_{e,1} \rightarrow 0$ and $E_n \rightarrow \infty$, the rate per unit-energy is upper-bounded by (83). It follows that $\dot{C}_\perp < \frac{\log e}{N_0}$, which concludes the proof of Part 3) of Theorem 8.

D. Proof of Theorem 9

The proofs of Part 1) and Part 2) follow along the similar lines as those of Part 1) and Part 2) of Theorem 3, respectively.

1) *Proof of Part 1)*: We first argue that $P_{e,A}^{(n)} \rightarrow 0$ only if $E_n \rightarrow \infty$, and that in this case $\dot{C}^A \leq \frac{\log e}{N_0}$. Indeed, we have

$$\begin{aligned} P_{e,A}^{(n)} &\geq \min_i \Pr\{\hat{W}_i \neq W_i\} \\ &\geq \alpha_n \Pr(\hat{W}_i \neq W_i | W_i \neq 0) \text{ for some } i. \end{aligned}$$

Since $\liminf_{n \rightarrow \infty} \alpha_n > 0$, this implies that $P_{e,A}^{(n)}$ vanishes only if $\Pr(\hat{W}_i \neq W_i | W_i \neq 0)$ vanishes. We next note that $\Pr(\hat{W}_i \neq W_i | W_i \neq 0)$ is lower-bounded by the error probability of the Gaussian single-user channel. By following the arguments presented at the beginning of the proof of Theorem 3, we obtain that $P_{e,A}^{(n)} \rightarrow 0$ only if $E_n \rightarrow \infty$, which also implies that $\dot{C}^A \leq \frac{\log e}{N_0}$.

For the achievability in Part 1), we use an orthogonal-access scheme where each user uses an orthogonal codebook of blocklength n/ℓ_n . Out of these n/ℓ_n channel uses, the first one is used for sending a pilot signal to convey that the user is active, and the remaining channel uses are used to send the message. Specifically, the codeword $\mathbf{x}_i(j)$ sent by user i to convey message j is given by

$$x_{ik}(j) = \begin{cases} \sqrt{tE_n}, & \text{if } k = 1 \\ \sqrt{(1-t)E_n}, & \text{if } k = j + 1 \\ 0, & \text{otherwise} \end{cases}$$

for some arbitrary $0 < t < 1$. From the pilot signal, the receiver first detects whether the user is active or not by checking whether the corresponding output exceeds $\frac{\sqrt{tE_n}}{2}$. As noted in

the proof of Part 1) of Theorem 8, the probability of a detection error is then given by $2Q\left(\frac{\sqrt{tE_n}}{2}\right)$. Since

$$E_n = \frac{\log M_n}{\dot{R}} = \frac{\log(\frac{n}{\ell_n} - 1)}{\dot{R}}$$

and since ℓ_n is sublinear in n , E_n tends to infinity as $n \rightarrow \infty$. This implies that the detection error vanishes as $n \rightarrow \infty$. Furthermore, if $\dot{R} < \frac{\log e}{N_0}$, then the probability of erroneously decoding the message also vanishes for this code, which follows from the proof of Theorem 3. This proves Part 1) of Theorem 9.

2) *Proof of Part 2)*: Fano's inequality yields that $H(\hat{W}_i | W_i) \leq 1 + P_{e,i} \log M_n$. Since $H(W_i) = H_2(\alpha_n) + \alpha_n \log M_n$, we have

$$H_2(\alpha_n) + \alpha_n \log M_n \leq 1 + P_{e,i} \log M_n + I(W_i; \hat{W}_i)$$

for $i = 1, \dots, \ell_n$. Averaging over all i 's then gives

$$\begin{aligned} H_2(\alpha_n) + \alpha_n \log M_n &\leq 1 + \frac{1}{\ell_n} \sum_{i=1}^{\ell_n} P_{e,i} \log M_n + \frac{1}{\ell_n} I(\mathbf{W}; \hat{\mathbf{W}}) \\ &\leq 1 + P_{e,A}^{(n)} \log M_n + \frac{1}{\ell_n} I(\mathbf{W}; \mathbf{Y}) \\ &\leq 1 + P_{e,A}^{(n)} \log M_n + \frac{n}{2\ell_n} \log \left(1 + \frac{2k_n E_n}{nN_0} \right). \end{aligned} \quad (84)$$

Here, the first inequality follows because the messages $W_i, i = 1, \dots, \ell_n$ are independent and because conditioning reduces entropy, the second inequality follows from the definition of $P_{e,A}^{(n)}$ and the data processing inequality, and the third inequality follows from (58).

Dividing both sides of (84) by E_n , and rearranging terms, yields the following upper-bound on the rate per unit-energy \dot{R}^A :

$$\dot{R}^A \leq \frac{1 - H_2(\alpha_n)}{E_n} + \frac{n}{2\ell_n E_n} \log \left(1 + \frac{2k_n E_n}{nN_0} \right) \frac{1}{\alpha_n - P_{e,A}^{(n)}}. \quad (85)$$

As noted before, $P_{e,A}^{(n)} \rightarrow 0$ only if $E_n \rightarrow \infty$. It follows that $\frac{1 - H_2(\alpha_n)}{E_n}$ vanishes as $n \rightarrow \infty$. Furthermore, together with the assumptions $\ell_n = \Omega(n)$ and $\liminf_{n \rightarrow \infty} \alpha_n > 0$, $E_n \rightarrow \infty$ implies that $k_n E_n/n = \alpha_n \ell_n E_n/n$ tends to infinity as $n \rightarrow \infty$. This in turn implies that

$$\frac{n}{2\ell_n E_n} \log \left(1 + \frac{2k_n E_n}{nN_0} \right) = \frac{n\alpha_n}{2k_n E_n} \log \left(1 + \frac{2k_n E_n}{nN_0} \right)$$

vanishes as $n \rightarrow \infty$. It thus follows from (85) that \dot{R}^A vanishes as $n \rightarrow \infty$, thereby proving Part 2) of Theorem 9.

V. COMPARISON WITH THE POLYANSKIY SETTING OF MANY-ACCESS CHANNELS

In this paper, we follow the setting of the MnAC introduced by Chen *et al.* [1]. That is, we assume that each user has a different codebook and require the probability of error to vanish as $n \rightarrow \infty$. By Lemma 4, the latter requirement can only be satisfied if $E_n \rightarrow \infty$ as $n \rightarrow \infty$, which for a fixed rate per unit-energy implies that $M_n \rightarrow \infty$. In other words, the payload of each user tends to infinity as $n \rightarrow \infty$.

In an attempt to introduce a notion of a random-access code that is appealing to the different communities interested in the multiple-access problem, Polyanskiy [4] proposed a different setting, where

- 1) all encoders use the same codebook;
- 2) the decoding is up to permutations of messages;
- 3) the probability of error is not required to vanish as $n \rightarrow \infty$.

He further introduced the per-user probability of error

$$\frac{1}{k_n} \sum_{i=1}^{k_n} \Pr(\{\hat{W}_i \neq W_i\} \cup \{W_j = W_i \text{ for some } j \neq i\}). \quad (86)$$

As argued in [4], the probability that two messages are equal is typically small, in which case the event $\{W_j = W_i \text{ for some } j \neq i\}$ can be ignored and (86) is essentially equivalent to the APE defined in (7).

The setting where all encoders use the same codebook and decoding is up to permutations of messages is sometimes also referred to as *unsourced multiple-access*. Unsourced multiple-access has two benefits: it may be more practical in scenarios with a large number of users, and many popular schemes, such as slotted ALOHA and coded slotted ALOHA, become achievability bounds and can be compared against each other and against information-theoretic benchmarks. By not requiring the probability of error to vanish as $n \rightarrow \infty$, it is not necessary to let M_n tend to infinity with the blocklength. So, in the above setting, the payload can be of fixed size, which may be appealing from a practical perspective.

In [4], Polyanskiy presented a random-coding achievability bound and used it as a benchmark for the performance of practical schemes, including coded slotted ALOHA, treating interference as noise, and time-division multiple-access. He further studied the minimum energy-per-bit that can be achieved by an (n, M_n, E_n, ϵ) code for APE when each user has a different codebook, the payload M_n and the probability of error ϵ are fixed, and the number of users grows linearly with the blocklength, i.e., $k_n = \mu n$ for some $0 < \mu \ll 1$. The bounds obtained in [4] and in the follow-up work [13] suggest that, whenever μ is below some critical value, the minimum energy-per-bit is independent of μ . In other words, there exists a critical density of users below which interference-free communication is feasible. This is consistent with the conclusions we drew from Theorems 1 and 7 for JPE, and from Theorems 3 and 9 for APE. However, these theorems also demonstrate that there is an important difference: According to Theorems 1 and 3, a linear growth of the number of users in n implies that the capacity per unit-energy \dot{C} is zero, irrespective of the value of μ , and irrespective of whether JPE or APE is considered. Since rate per unit-energy is the reciprocal of energy-per-bit, this implies that the minimum energy-per-bit is infinite. In contrast, the bounds presented in [4] and [13] show that the minimum energy-per-bit for a fixed probability of error ϵ is finite or, equivalently, that the ϵ -capacity per unit-energy \dot{C}_ϵ is strictly positive. Thus, the capacity per unit-energy is strictly smaller than the ϵ -capacity per unit-energy. In other words, for APE, the strong converse does not hold.

In order to explore this point further, we discuss in the rest of this section how the largest achievable rate per unit-energy changes if we allow for a non-vanishing error probability. For the sake of simplicity, we shall assume throughout the section that users are active with probability one, i.e., $\alpha_n = 1$.

We first argue that, when the number of users is bounded in n , then a simple orthogonal-access scheme achieves an ϵ -capacity per unit-energy that can even be larger than the single-user capacity per unit-energy $\frac{\log e}{N_0}$, irrespective of whether JPE or APE is assumed. We shall do so by means of the following example.

Example 1: Consider a k -user Gaussian MAC with normalized noise variance $N_0/2 = 1$ and where the number of users is independent of n . Suppose that each user has two messages to transmit using energy $E_n = 1$. Consider an orthogonal-access scheme where each user gets one channel use and remains silent in the remaining channel uses. In this channel use, the user transmits either $+1$ or -1 to convey its message. Since the access scheme is orthogonal, the receiver can perform independent decoding for each user, which yields $\Pr(\hat{W}_i \neq W_i) = Q(1)$. Consequently, we can achieve the rate per unit-energy $\frac{\log M_n}{E_n} = 1$ at APE $P_{e,A}^{(n)} = Q(1)$ and at JPE $P_e^{(n)} = 1 - (1 - Q(1))^k$. Since $\frac{\log e}{N_0} = \frac{\log e}{2} \approx 0.7213$, we conclude that, if $\epsilon \geq Q(1)$ (for APE) or $\epsilon \geq 1 - (1 - Q(1))^k$ (for JPE), then the ϵ -capacity per unit-energy exceeds the single-user capacity per unit-energy.

Remark 4: A crucial ingredient in the above scheme is that the energy E_n is bounded in n . Indeed, it follows from [20, Th. 3] that, if $E_n \rightarrow \infty$ as $n \rightarrow \infty$, as required, e.g., in [14, Def. 2] (See Remark 1), then the ϵ -capacity per unit-energy of the Gaussian single-user channel is equal to $\frac{\log e}{N_0}$, irrespective of $0 < \epsilon < 1$. For the Gaussian MnAC, the genie argument provided at the beginning of the proof of Theorem 3 then demonstrates that the maximum rate per unit-energy that is ϵ -achievable with $E_n \rightarrow \infty$ cannot exceed $\frac{\log e}{N_0}$.

In the following two subsections, we discuss the ϵ -capacity per unit-energy when the number of users k_n tends to infinity as n tends to infinity. Specifically, in Subsection V-A we demonstrate that, irrespective of the order of growth of k_n , the ϵ -capacity per unit-energy for JPE is the same as \dot{C} , i.e., the strong converse holds in this case. In Subsection V-B, we consider the case where $k_n = \mu n$ and show by means of a simple example that, for some fixed payload M_n and sufficiently small μ , the ϵ -capacity per unit-energy for APE is indeed independent of μ , as suggested by the bounds in [4] and [13].

A. Non-Vanishing JPE

The following theorem characterizes the behavior of the ϵ -capacity per unit-energy for JPE and an unbounded number of users.

Theorem 13: The ϵ -capacity per unit-energy \dot{C}_ϵ of the non-random MnAC with JPE has the following behavior:

- 1) If $k_n = \omega(1)$ and $k_n = o(n/\log n)$, then $\dot{C}_\epsilon = \frac{\log e}{N_0}$ for every $0 < \epsilon < 1$.
- 2) If $k_n = \omega(n/\log n)$, then $\dot{C}_\epsilon = 0$ for every $0 < \epsilon < 1$.

Proof: We first prove Part 1). It follows from (184) in the proof of Lemma 12 that, for $M_n \geq 2$ and $k_n \geq 5$,

$$P_e^{(n)} \geq 1 - \frac{256E_n/N_0 + \log 2}{\log k_n}. \quad (87)$$

This implies that $P_e^{(n)}$ tends to one unless $E_n = \Omega(\log k_n)$. Since, by the theorem's assumption, we have $k_n = \omega(1)$, it follows that $E_n \rightarrow \infty$ is necessary to achieve a JPE strictly smaller than one. As argued in Remark 4 (see also Remark 1), if $E_n \rightarrow \infty$ as $n \rightarrow \infty$, then the ϵ -capacity per unit-energy of the Gaussian MnAC cannot exceed the single-user capacity per unit-energy $\frac{\log e}{N_0}$. Furthermore, by Theorem 3, if $k_n = o(n/\log n)$, then any rate per unit-energy satisfying $\dot{R} < \frac{\log e}{N_0}$ is achievable, hence it is also ϵ -achievable. We thus conclude that, if $k_n = \omega(1)$ and $k_n = o(n/\log n)$, then $\dot{C}_\epsilon = \frac{\log e}{N_0}$ for every $0 < \epsilon < 1$.

To prove Part 2), we use the upper bound (13), namely

$$\dot{R} \leq \frac{\frac{1}{k_n E_n} + \frac{n}{2k_n E_n} \log(1 + \frac{2k_n E_n}{nN_0})}{1 - P_e^{(n)}}. \quad (88)$$

By (87), $P_e^{(n)}$ tends to one unless $E_n = \Omega(\log k_n)$. For $k_n = \omega(n/\log n)$, this implies that $k_n E_n/n \rightarrow \infty$ as $n \rightarrow \infty$, so the RHS of (88) vanishes as n tends to infinity. We thus conclude that, if $k_n = \omega(n/\log n)$, then $\dot{C}_\epsilon = 0$ for every $0 < \epsilon < 1$. ■

Theorems 1 and 13 demonstrate that $\dot{C}_\epsilon = \dot{C}$ for every $0 < \epsilon < 1$, provided that the number of users is unbounded in n . Consequently, the strong converse holds for JPE. As argued in the proof of Theorem 13, this result hinges on the fact that the probability of error can be strictly smaller than one only if the energy tends to infinity as $n \rightarrow \infty$. As explained in Remarks 1 and 4, in this case the capacity per unit-energy cannot exceed $\frac{\log e}{N_0}$. As we shall see in the next subsection, an APE strictly smaller than one can also be achieved at a positive rate per unit-energy if the energy is bounded in n . This allows for a positive ϵ -capacity per unit-energy for APE when k_n grows linearly in n .

B. Non-Vanishing APE

In this subsection, we focus on the case where $k_n = \mu n$ and show that, when the payload of each user is 1 bit and $\mu \leq 1$, the ϵ -capacity per unit-energy for APE is indeed independent of μ . This supports the conjecture in [13] that there exists a critical density of users below which interference-free communication is feasible.

Let $\mathcal{E}^*(M, \mu, \epsilon)$ denote the minimum energy-per-bit required to send M messages at an APE not exceeding ϵ when the number of users is given by $k_n = \mu n$. While it is difficult to obtain the exact closed form expression of $\mathcal{E}^*(M, \mu, \epsilon)$ for general M, μ and ϵ , upper and lower bounds on $\mathcal{E}^*(M, \mu, \epsilon)$ were derived in [4], [13]. Furthermore, as we shall argue next, if the payload of each user is 1 bit and $\mu \leq 1$, then $\mathcal{E}^*(M, \mu, \epsilon)$ can be evaluated in closed form.

For simplicity, assume that $N_0/2 = 1$. Then,

$$\mathcal{E}^*(2, \mu, \epsilon) = (\max\{0, Q^{-1}(\epsilon)\})^2, \quad 0 < \mu \leq 1 \quad (89)$$

where Q^{-1} denotes the inverse of the Q -function. Indeed, that $\mathcal{E}^*(2, \mu, \epsilon) \geq (\max\{0, Q^{-1}(\epsilon)\})^2$ follows from (30). Furthermore, if $\mu \leq 1$, then we can assign each user one channel use. Following the orthogonal-access scheme presented in Example 1, but where each user transmits either $+\sqrt{E}$ or $-\sqrt{E}$ (instead of $+1$ or -1) with energy $E = (\max\{0, Q^{-1}(\epsilon)\})^2$, we can achieve $P_{e,A}^{(n)} \leq \epsilon$. Thus, with energy (89) we can send 2 messages at an APE not exceeding ϵ .

Observe that the RHS of (89) does not depend on μ and agrees with the minimum energy-per-bit required to send one bit over the Gaussian single-user channel with error probability ϵ . Thus, when $\mu \leq 1$, we can send one bit free of interference. Further observe that (89) is finite for every positive ϵ . Consequently, the ϵ -capacity per unit-energy, which is given by the reciprocal of (89), is strictly positive. This is in contrast to the capacity per unit-energy which, by Part 2) of Theorem 3, is zero. Thus, the strong converse does not hold for APE when the number of users grows linearly in n .

As mentioned in the previous subsection, to achieve a positive rate per unit-energy, it is crucial that the energy E_n and payload $\log M_n$ are bounded in n . Indeed, for $k_n = \mu n$, the RHS of (33) vanishes as E_n tends to infinity, in which case no positive rate per unit-energy is ϵ -achievable. Moreover, for $k_n = \mu n$ and a bounded E_n , (32) implies that the payload $\log M_n$ is bounded, too. We conclude that the arguably most common assumptions in the literature on MnACs—linear growth of the number of users, a non-vanishing APE, and a fixed payload—are the only set of assumptions under which a positive rate per unit-energy is achievable, unless we consider sublinear growths of k_n .

VI. CONCLUSIONS

In this work, we analyzed scaling laws of a Gaussian random MnAC where the total number of users as well as the average number of active users may grow with the blocklength. In particular, we characterized the behavior of the capacity per unit-energy as a function of the order of growth of the number of users for two notions of probability of error: the classical JPE and the APE proposed by Polyanskiy in [4]. For both cases, we demonstrated that there is a sharp transition between orders of growth where all users can achieve the single-user capacity per unit-energy and orders of growth where no positive rate per unit-energy is feasible. When all users are active with probability one, we showed that the transition threshold separating the two regimes is at the order of growth $n/\log n$ for JPE, and at the order of growth n for APE. While the qualitative behavior of the capacity per unit-energy remains the same in both cases, there are some interesting differences between JPE and APE in some other aspects. For example, we showed that an orthogonal-access scheme together with orthogonal codebooks is optimal for APE, but it is suboptimal for JPE. Furthermore, when the number of users is unbounded in n , the strong converse holds for JPE, but it does not hold for APE. For MnACs where the number of users grows linearly in n and APE—the most common assumptions in the literature—our results imply that a positive rate per unit-energy is infeasible if we require the APE to vanish asymptotically. In contrast, due to the absence of a

strong converse, a positive ϵ -rate per unit-energy is feasible. To this end, however, it is necessary that the energy E_n and the payload $\log M_n$ are bounded in n .

For the case of random user activity and JPE, we characterized the behavior of the capacity per unit-energy in terms of the total number of users ℓ_n and the average number of active users k_n . We showed that, if $k_n \log \ell_n$ is sublinear in n , then all users can achieve the single-user capacity per unit-energy, and if $k_n \log \ell_n$ is superlinear in n , then the capacity per unit-energy is zero. *Inter alia*, this result recovers our characterization of the non-random-access case ($\alpha_n = 1$), since $k_n \log k_n = \Theta(n)$ is equivalent to $k_n = \Theta(n/\log n)$. Our result further implies that the orders of growth of ℓ_n for which interference-free communication is feasible are in general larger than $n/\log n$, and the orders of growth of k_n for which interference-free communication is feasible may be smaller than $n/\log n$. This suggests that treating a random MnAC with total number of users ℓ_n and average number of users k_n as a non-random MnAC with k_n users may be overly-optimistic.

We finally showed that, for JPE, orthogonal-access schemes achieve the single-user capacity per unit-energy when the order of growth of ℓ_n is strictly below $n/\log n$, and they cannot achieve a positive rate per unit-energy when the order of growth of ℓ_n is strictly above $n/\log n$, irrespective of the behavior of k_n . Intuitively, by using an orthogonal-access scheme, we treat the random MnAC as if it were non-random. Consequently, orthogonal-access schemes are optimal when all users are active with probability one. However, for general α_n , non-orthogonal-access schemes may be necessary to achieve the capacity per unit-energy.

APPENDIX I PROOF OF LEMMA 4

The probability of error of the Gaussian MnAC cannot be smaller than that of the Gaussian point-to-point channel. Indeed, suppose a genie informs the receiver about all transmitted codewords except that of user i . Then the receiver can subtract the known codewords from the received vector, resulting in a point-to-point Gaussian channel. Since access to additional information does not increase the probability of error, the claim follows.

We next note that, for a Gaussian point-to-point channel, any (n, M_n, E_n, ϵ) -code satisfies [20, Th. 2]

$$\frac{1}{M_n} \geq Q \left(\sqrt{\frac{2E_n}{N_0}} + Q^{-1}(1 - \epsilon) \right). \quad (90)$$

Solving (90) for ϵ yields

$$\epsilon \geq 1 - Q \left(Q^{-1} \left(\frac{1}{M_n} \right) - \sqrt{\frac{2E_n}{N_0}} \right).$$

It follows that the probability of error tends to zero as $n \rightarrow \infty$ only if $Q^{-1}(1/M_n) - \sqrt{\frac{2E_n}{N_0}} \rightarrow -\infty$. Since $Q^{-1}(1/M_n) \geq 0$ for $M_n \geq 2$, this in turn is only the case if $E_n \rightarrow \infty$. This proves Lemma 4.

APPENDIX II PROOF OF LEMMA 6

The upper bounds on the probability of error presented in (22) and (23) are proved in Appendix II-A. The lower bounds are proved in Appendix II-B.

A. Upper bounds

An upper bound on the probability of error for M orthogonal codewords of maximum energy E can be found in [16, Sec. 2.5]:

$$\begin{aligned} P_{e,1} &\leq (M-1)^\rho \exp \left[-\frac{E}{N_0} \left(\frac{\rho}{\rho+1} \right) \right] \\ &\leq \exp \left[-\frac{E}{N_0} \left(\frac{\rho}{\rho+1} \right) + \rho \ln M \right]. \end{aligned} \quad (91)$$

for $0 \leq \rho \leq 1$. For the rate per unit-energy $\dot{R} = \frac{\log M}{E}$, it follows from (91) that

$$P_{e,1} \leq \exp[-EE_0(\rho, \dot{R})], \quad \text{for } 0 \leq \rho \leq 1 \quad (92)$$

where

$$E_0(\rho, \dot{R}) \triangleq \left(\frac{1}{N_0} \frac{\rho}{\rho+1} - \frac{\rho \dot{R}}{\log e} \right). \quad (93)$$

When $0 < \dot{R} \leq \frac{1}{4} \frac{\log e}{N_0}$, the maximum of $E_0(\rho, \dot{R})$ over all $0 \leq \rho \leq 1$ is achieved for $\rho = 1$. When $\frac{1}{4} \frac{\log e}{N_0} \leq \dot{R} \leq \frac{\log e}{N_0}$, the maximum of $E_0(\rho, \dot{R})$ is achieved for $\rho = \sqrt{\frac{\log e}{N_0} \frac{1}{\dot{R}}} - 1 \in [0, 1]$. So we have

$$\max_{0 \leq \rho \leq 1} E_0(\rho, \dot{R}) = \begin{cases} \frac{1}{2N_0} - \frac{\dot{R}}{\log e}, & 0 < \dot{R} \leq \frac{1}{4} \frac{\log e}{N_0} \\ \left(\sqrt{\frac{1}{N_0}} - \sqrt{\frac{\dot{R}}{\log e}} \right)^2, & \frac{1}{4} \frac{\log e}{N_0} \leq \dot{R} \leq \frac{\log e}{N_0}. \end{cases} \quad (94)$$

Since $E = \frac{\log M}{\dot{R}}$, we obtain from (92) and (94) that

$$P_{e,1} \leq e^{-\frac{\ln M}{\dot{R}} \left(\frac{\log e}{2N_0} - \dot{R} \right)}, \quad \text{if } 0 < \dot{R} \leq \frac{1}{4} \frac{\log e}{N_0}$$

and

$$P_{e,1} \leq e^{-\frac{\ln M}{\dot{R}} \left(\sqrt{\frac{\log e}{N_0}} - \sqrt{\dot{R}} \right)^2}, \quad \text{if } \frac{1}{4} \frac{\log e}{N_0} \leq \dot{R} \leq \frac{\log e}{N_0}.$$

This proves the upper bounds on the probability of error in (22) and (23).

B. Lower bounds

To prove the lower bounds on the probability of error presented in (22) and (23), we first argue that, for an orthogonal codebook, the optimal probability of error is achieved by codewords of equal energy. Then, for any given \dot{R} and an orthogonal codebook where all codewords have equal energy, we derive the lower bound in (23), which is optimal at high rates. We further obtain an improved lower bound on the probability of error for low rates. Finally, the lower bound in (22) follows by showing that a combination of the two lower bounds yields a lower bound, too.

1) *Equal-energy codewords are optimal*: We shall argue that, for an orthogonal code with energy upper-bounded by E_n , there is no loss in optimality in assuming that all codewords have energy E_n . To this end, we first note that, without loss of generality, we can restrict ourselves to codewords of the form

$$\mathbf{x}_m = (0, \dots, \sqrt{E_{\mathbf{x}_m}}, \dots, 0), \quad m = 1, \dots, M \quad (95)$$

where $E_{\mathbf{x}_m} \leq E_n$ denotes the energy of codeword \mathbf{x}_m . Indeed, any orthogonal codebook can be multiplied by an orthogonal matrix to obtain this form. Since the additive Gaussian noise \mathbf{Z} is zero mean and has a diagonal covariance matrix, this does not change the probability of error.

To argue that equal-energy codewords are optimal, let us consider a code \mathcal{C} for which some codewords have energy strictly less than E_n . From \mathcal{C} , we can construct a new code \mathcal{C}' by multiplying each codeword \mathbf{x}_m by $\sqrt{E_n/E_{\mathbf{x}_m}}$. Clearly, each codeword in \mathcal{C}' has energy E_n . Let \mathbf{Y} and \mathbf{Y}' denote the channel outputs when we transmit codewords from \mathcal{C} and \mathcal{C}' , respectively, and let $P_e(\mathcal{C})$ and $P_e(\mathcal{C}')$ denote the corresponding probabilities of error. By multiplying each dimension of the channel output \mathbf{Y}' by $\sqrt{E_{\mathbf{x}_m}/E_n}$ and adding Gaussian noise of zero mean and variance $E_n/E_{\mathbf{x}_m}$, we can construct a new channel output $\tilde{\mathbf{Y}}$ that has the same distribution as \mathbf{Y} . Consequently, \mathcal{C}' can achieve the same probability of error as \mathcal{C} by applying the decoding rule of \mathcal{C} to $\tilde{\mathbf{Y}}$. It follows that $P_e(\mathcal{C}') \leq P_e(\mathcal{C})$. We conclude that, in order to find lower bounds on the probability of error, it suffices to consider codes whose codewords all have energy E_n .

2) *High-rate lower bound*: We next derive lower bound (23), which applies to high rates per unit-energy. To obtain this bound, we follow the analysis given in [15] (see also [16, Sec. 3.6.1]). To this end, we shall first derive a lower bound on the maximum probability of error

$$P_{e_{\max}} \triangleq \max_m P_{e_m}$$

where P_{e_m} denotes the probability of error in decoding message m . In a second step, we derive from this bound a lower bound on the average probability of error $P_{e,1}$ by means of expurgation. For $P_{e_{\max}}$, it was shown that at least one of the following two inequalities is always satisfied [16, Sec. 3.6.1]:

$$1/M \geq \frac{1}{4} e^{\mu(s) - s\mu'(s) - s\sqrt{2\mu''(s)}} \quad (96)$$

$$P_{e_{\max}} \geq \frac{1}{4} e^{\mu(s) + (1-s)\mu'(s) - (1-s)\sqrt{2\mu''(s)}} \quad (97)$$

for all $0 \leq s \leq 1$, where

$$\mu(s) = -\frac{E}{N_0} s(1-s), \quad (98)$$

$$\mu'(s) = -\frac{E}{N_0} (1-2s), \quad (99)$$

$$\mu''(s) = \frac{2E}{N_0}. \quad (100)$$

By substituting these values in (96), we obtain

$$\ln M \leq \frac{E}{N_0} \left[s^2 + \frac{2s}{\sqrt{E/N_0}} + \frac{\ln 4}{E/N_0} \right].$$

Using that $0 \leq s \leq 1$ and that $E = \frac{\log M}{\dot{R}}$, this yields

$$\dot{R} \leq \frac{\log e}{N_0} \left[s^2 + \frac{2}{\sqrt{E/N_0}} + \frac{\ln 4}{E/N_0} \right]. \quad (101)$$

Similarly, substituting (98)-(100) in (97) yields

$$\begin{aligned} P_{e_{\max}} &\geq e^{-\frac{E}{N_0}(1-s)^2 - 2(1-s)\sqrt{\frac{E}{N_0}} - \ln 4} \\ &\geq e^{-\frac{E}{N_0} \left((1-s)^2 + \frac{2}{\sqrt{E/N_0}} + \frac{\ln 4}{E/N_0} \right)}. \end{aligned} \quad (102)$$

For a given E , let δ_E be defined as

$$\delta_E \triangleq 2 \left(\frac{2}{\sqrt{E/N_0}} + \frac{\ln 4}{E/N_0} \right)$$

and let

$$s_E \triangleq \sqrt{\dot{R} \frac{N_0}{\log e} - \delta_E}.$$

For $s = s_E$, the bound (101), and hence also (96), is violated, which implies that (102) must be satisfied for $s = s_E$. By substituting $s = s_E$ in (102), we obtain

$$P_{e_{\max}} \geq e^{-E \left(\left(\sqrt{\frac{1}{N_0}} - \sqrt{\frac{\dot{R}}{\log e} - \frac{\delta_E}{N_0}} \right)^2 + \frac{\delta_E}{2N_0} \right)}. \quad (103)$$

We next use (103) and expurgation to derive a lower bound on $P_{e,1}$. Indeed, we divide the codebook \mathcal{C} with M messages and average probability of error $P_e(\mathcal{C})$ into two codebooks \mathcal{C}_1 and \mathcal{C}_2 of $M/2$ messages each, such that \mathcal{C}_1 contains the codewords with the smallest probabilities of error and \mathcal{C}_2 contains the codewords with the largest probabilities of error. It then holds that each codeword in \mathcal{C}_1 has a probability of error satisfying $P_{e_m} \leq 2P_e(\mathcal{C})$. Consequently, the largest error probability of code \mathcal{C}_1 , denoted as $P_{e_{\max}}(\mathcal{C}_1)$, and the average error probability of code \mathcal{C} satisfy

$$P_e(\mathcal{C}) \geq \frac{1}{2} P_{e_{\max}}(\mathcal{C}_1). \quad (104)$$

Applying (103) for \mathcal{C}_1 , and using that the rate per unit-energy of \mathcal{C}_1 satisfies $\dot{R}' = \frac{\log(M/2)}{E} = \dot{R} - \frac{1}{E}$, we obtain

$$P_{e_{\max}}(\mathcal{C}_1) \geq e^{-E \left(\left(\sqrt{\frac{1}{N_0}} - \sqrt{\frac{\dot{R}}{\log e} - \frac{1}{E} - \frac{\delta_E}{N_0}} \right)^2 + \frac{\delta_E}{2N_0} \right)}.$$

Together with (104), this yields

$$P_{e,1} \geq e^{-E \left(\left(\sqrt{\frac{1}{N_0}} - \sqrt{\frac{\dot{R}}{\log e} - \frac{1}{E} - \frac{\delta_E}{N_0}} \right)^2 + \frac{\delta_E}{2N_0} - \frac{\ln 2}{E} \right)}. \quad (105)$$

Let $\delta'_E \triangleq \frac{1}{E} + \frac{\delta_E}{N_0}$. Then

$$\begin{aligned} \sqrt{\frac{\dot{R}}{\log e} - \frac{1}{E} - \frac{\delta_E}{N_0}} &= \sqrt{\frac{\dot{R}}{\log e} - \delta'_E} \\ &= \sqrt{\frac{\dot{R}}{\log e}} + O(\delta'_E) \\ &= \sqrt{\frac{\dot{R}}{\log e}} + O\left(\frac{1}{\sqrt{E}}\right) \end{aligned}$$

where the last step follows by noting that δ'_E and δ_E are both of order $O(1/\sqrt{E})$. Further defining $\delta''_E \triangleq \frac{\delta_E}{2N_0} - \frac{\ln 2}{E}$, we may write (105) as

$$\begin{aligned} P_{e,1} &\geq e^{-E \left(\left(\sqrt{\frac{1}{N_0}} - \sqrt{\frac{\dot{R}}{\log e}} + O\left(\frac{1}{\sqrt{E}}\right) \right)^2 + \delta''_E \right)} \\ &= e^{-E \left(\left(\sqrt{\frac{1}{N_0}} - \sqrt{\frac{\dot{R}}{\log e}} \right)^2 + O\left(\frac{1}{\sqrt{E}}\right) \right)} \end{aligned} \quad (106)$$

since $O(\delta''_E) = O(\delta_E) = O(1/\sqrt{E})$. By substituting $E = \frac{\log M}{\dot{R}}$, (106) yields

$$P_{e,1} \geq e^{-\frac{\ln M}{\dot{R}} \left(\left(\sqrt{\frac{\log e}{N_0}} - \sqrt{\dot{R}} \right)^2 + O\left(\frac{1}{\sqrt{E}}\right) \right)}. \quad (107)$$

We can thus find a function $E \mapsto \beta'_E$ of order $O(1/\sqrt{E})$ for which the lower bound in (23) holds.

3) *Low-rate lower bound:* We next derive a lower bound on the probability of error that, for low rates per unit-energy, is tighter than (107). This bound will then be used later to derive the lower bound (22). The bound is based on the fact that, for M codewords of energy E , the minimum Euclidean distance d_{\min} between codewords is upper-bounded by $\sqrt{2EM}/(M-1)$ [16, Sec. 3.7.1]. Since, for the Gaussian channel, the maximum error probability is lower-bounded by the largest pairwise error probability, it follows that

$$\begin{aligned} P_{e,\max} &\geq Q\left(\frac{d_{\min}}{\sqrt{2N_0}}\right) \\ &\geq Q\left(\sqrt{\frac{EM}{N_0(M-1)}}\right) \\ &\geq \left(1 - \frac{1}{EM/(N_0(M-1))}\right) \frac{e^{-\frac{EM}{2N_0(M-1)}}}{\sqrt{2\pi\sqrt{EM}/(N_0(M-1))}} \end{aligned} \quad (108)$$

where the last inequality follows because [22, Prop. 19.4.2]

$$Q(\beta) \geq \left(1 - \frac{1}{\beta^2}\right) \frac{e^{-\beta^2/2}}{\sqrt{2\pi}\beta}, \quad \beta > 0.$$

Let $\beta_E \triangleq \sqrt{EM/N_0(M-1)}$. It follows that

$$\sqrt{E/N_0} \leq \beta_E \leq \sqrt{2E/N_0}, \quad M \geq 2. \quad (109)$$

Applying (109) to (108) yields

$$\begin{aligned} P_{e,\max} &\geq \frac{1}{\sqrt{2\pi}} e^{-E\left(\frac{1}{2N_0}\left(1+\frac{1}{M-1}\right)\right)} e^{\ln\left(\frac{1}{\beta_E} - \frac{1}{\beta'_E}\right)} \\ &\geq \frac{1}{\sqrt{2\pi}} e^{-E\left(\frac{1}{2N_0}\left(1+\frac{1}{M-1}\right)\right)} e^{-E\frac{\frac{3}{2}\ln(2E/N_0) - \ln(E/N_0 - 1)}{E}} \\ &= e^{-E\left(\frac{1}{2N_0}\left(1+\frac{1}{M-1}\right) + O\left(\frac{\ln E}{E}\right)\right)}. \end{aligned} \quad (110)$$

Following similar steps of expurgation as before, we obtain from (110) the lower bound

$$P_{e,1} \geq \exp\left[-E\left(\frac{1}{2N_0}\left(1 + \frac{1}{\frac{M}{2} - 1}\right) + O\left(\frac{\ln E}{E}\right)\right)\right].$$

By using that $M = 2^{\dot{R}E}$, it follows that

$$P_{e,1} \geq \exp\left[-E\left(\frac{1}{2N_0}\left(1 + \frac{1}{\frac{2^{\dot{R}E}}{2} - 1}\right) + O\left(\frac{\ln E}{E}\right)\right)\right] \quad (111)$$

from which we obtain that, for any rate per unit-energy $\dot{R} > 0$,

$$P_{e,1} \geq \exp\left[-E\left(\frac{1}{2N_0} + O\left(\frac{\ln E}{E}\right)\right)\right]. \quad (112)$$

4) *Combining the high-rate and low-rate bounds:* We finally show that a combination of the lower bounds (106) and (111) yields the lower bound in (22).

Let $P_e^\perp(E, M)$ denote the smallest probability of error that can be achieved by an orthogonal codebook with M codewords of energy E . We first note that $P_e^\perp(E, M)$ is monotonically increasing in M . Indeed, without loss of optimality, we can restrict ourselves to codewords of the form (95), all having energy E . In this case, the probability of correctly decoding message m is given by [18, Sec. 8.2]

$$\begin{aligned} P_{c,m}^\perp &= \Pr\left(\bigcap_{i \neq m} \{Y_m > Y_i\} \mid \mathbf{X} = \mathbf{x}_m\right) \\ &= \int_{-\infty}^{\infty} \frac{e^{-\frac{(y_m - \sqrt{E})^2}{N_0}}}{\sqrt{\pi N_0}} \Pr\left(\bigcap_{i \neq m} \{Y_i < y_m\} \mid \mathbf{X} = \mathbf{x}_m\right) dy_m \\ &= \int_{-\infty}^{\infty} \frac{e^{-\frac{(y_m - \sqrt{E})^2}{N_0}}}{\sqrt{\pi N_0}} (1 - Q(y_m))^{M-1} dy_m \end{aligned} \quad (113)$$

where Y_i denotes the i -th component of the received vector \mathbf{Y} . In the last step of (113), we have used that, conditioned on $\mathbf{X} = \mathbf{x}_m$, the events $\{Y_i < y_m\}$, $i \neq m$ are independent and $\Pr(Y_i < y_m | \mathbf{X} = \mathbf{x}_m)$ can be computed as $1 - Q(y_m)$. Since $P_{c,m}^\perp$ is the same for all m , we have $P_e^\perp(E, M) = 1 - P_{c,m}^\perp$. The claim then follows by observing that (113) is monotonically decreasing in M .

Let \tilde{M} be the largest power of 2 less than or equal to M . It follows by the monotonicity of $P_e^\perp(E, M)$ in M that

$$P_e^\perp(E, M) \geq P_e^\perp(E, \tilde{M}). \quad (114)$$

We next show that, for every E_1 and E_2 satisfying $E = E_1 + E_2$, we have

$$P_e^\perp(E, \tilde{M}) \geq P_e(E_1, \tilde{M}, L) P_e(E_2, L + 1) \quad (115)$$

where $P_e(E_1, \tilde{M}, L)$ denotes the smallest probability of error that can be achieved by a codebook with \tilde{M} codewords of energy E_1 and a list decoder of list size L , and $P_e(E_2, L + 1)$ denotes the smallest probability of error that can be achieved by a codebook with $L + 1$ codewords of energy E_2 .

To prove (115), we follow along the lines of [15], which showed the corresponding result for codebooks of a given blocklength rather than a given energy. Specifically, it was shown in [15, Th. 1] that, for every codebook \mathcal{C} with M codewords of blocklength n , and for any n_1 and n_2 satisfying $n = n_1 + n_2$, we can lower-bound the probability of error by

$$P_e(\mathcal{C}) \geq P_e(n_1, M, L) P_e(n_2, L + 1) \quad (116)$$

where $P_e(n_1, M, L)$ denotes the smallest probability of error that can be achieved by a codebook with M codewords of blocklength n_1 and a list decoder of list size L , and $P_e(n_2, L + 1)$ denotes the smallest probability of error that can be achieved by a codebook with $L + 1$ codewords of blocklength n_2 . This result follows by writing the codewords \mathbf{x}_m of blocklength n as concatenations of the vectors

$$\mathbf{x}'_m = (x_{m,1}, x_{m,2}, \dots, x_{m,n_1})$$

and

$$\mathbf{x}''_m = (x_{m,n_1+1}, x_{m,n_1+2}, \dots, x_{m,n_1+n_2})$$

and, likewise, by writing the received vector \mathbf{y} as the concatenation of the vectors \mathbf{y}' and \mathbf{y}'' of length n_1 and n_2 , respectively. Defining Δ_m as the decoding region for message m and $\Delta''_m(\mathbf{y}')$ as the decoding region for message m when \mathbf{y}' was received, we can then write $P_e(\mathcal{C})$ as

$$P_e(\mathcal{C}) = \frac{1}{M} \sum_{m=1}^M \sum_{\mathbf{y}'} p(\mathbf{y}' | \mathbf{x}'_m) \sum_{\mathbf{y}'' \in \bar{\Delta}''_m} p(\mathbf{y}'' | \mathbf{x}''_m) \quad (117)$$

where $\bar{\Delta}''_m$ denotes the complement of Δ''_m . Lower-bounding first the inner-most sum in (117) and then the remaining terms, one can prove (116).

A codebook with \tilde{M} codewords of the form (95) can be transmitted in \tilde{M} time instants, since in the remaining time instants all codewords are zero. We can thus assume without loss of optimality that the codebook's blocklength is \tilde{M} . Unfortunately, for such codewords, the above approach yields (115) only in the trivial cases where either $E_1 = 0$ or $E_2 = 0$. Indeed, E_1 and E_2 correspond to the energies of the vectors \mathbf{x}'_m and \mathbf{x}''_m , respectively, and for (95) we have $\mathbf{x}'_m = \mathbf{0}$ if $m > n_1$ and $\mathbf{x}''_m = \mathbf{0}$ if $m \leq n_1$, where $\mathbf{0}$ denotes the all-zero vector. We sidestep this problem by multiplying the codewords by a normalized Hadamard matrix. The Hadamard matrix, denoted by H_j , is a square matrix of size $j \times j$ with entries ± 1 and has the property that all rows are orthogonal. Sylvester's construction shows that there exists a Hadamard matrix of order j if j is a power of 2. Recalling that \tilde{M} is a power of 2, we can thus find a normalized Hadamard matrix

$$\tilde{H} \triangleq \frac{1}{\sqrt{\tilde{M}}} H_{\tilde{M}}.$$

Since the rows of \tilde{H} are orthonormal, it follows that the matrix \tilde{H} is orthogonal. Further noting that the additive Gaussian noise \mathbf{Z} is zero mean and has a diagonal covariance matrix, we conclude that the set of codewords $\{\tilde{H}\mathbf{x}_m, m = 1, \dots, \tilde{M}\}$ achieve the same probability of error as the set of codewords $\{\mathbf{x}_m, m = 1, \dots, \tilde{M}\}$. Thus, without loss of generality, we can restrict ourselves to codewords of the form $\tilde{\mathbf{x}}_m = \tilde{H}\mathbf{x}_m$, where \mathbf{x}_m is as in (95). Such codewords have constant modulus, i.e., $|\tilde{x}_{m,k}| = \sqrt{\frac{E}{\tilde{M}}}, k = 1, \dots, \tilde{M}$. This has the advantage that the energies of the vectors

$$\tilde{\mathbf{x}}'_m = (\tilde{x}_{m,1}, \tilde{x}_{m,2}, \dots, \tilde{x}_{m,n_1})$$

and

$$\tilde{\mathbf{x}}''_m = (\tilde{x}_{m,n_1+1}, \tilde{x}_{m,n_1+2}, \dots, \tilde{x}_{m,n_1+n_2})$$

are proportional to n_1 and n_2 , respectively. Thus, by emulating the proof of (116), we can show that, for every n_1 and n_2 satisfying $\tilde{M} = n_1 + n_2$ and $E_i = En_i/\tilde{M}, i = 1, 2$, we have

$$P_e^\perp(E, \tilde{M}) \geq P_e(E_1, n_1, \tilde{M}, L) P_e(E_2, n_2, L + 1) \quad (118)$$

where $P_e(E_1, n_1, \tilde{M}, L)$ denotes the smallest probability of error that can be achieved by a codebook with \tilde{M} codewords of energy E_1 and blocklength n_1 and a list decoder of list size L , and $P_e(E_2, n_2, L + 1)$ denotes the smallest probability of error that can be achieved by a codebook with $L + 1$ codewords of energy E_2 and blocklength n_2 . We then obtain (115) from (118) because

$$P_e(E_1, n_1, \tilde{M}, L) \geq P_e(E_1, \tilde{M}, L)$$

and

$$P_e(E_2, n_2, L + 1) \geq P_e(E_2, L + 1).$$

We next give a lower bound on $P_e(E_1, \tilde{M}, L)$. Indeed, for list decoding of list size L , the inequalities (96) and (97) can be replaced by [16, Lemma 3.8.1]

$$L/M \geq \frac{1}{4} e^{\mu(s) - s\mu'(s) - s\sqrt{2\mu''(s)}} \quad (119)$$

$$P_{e_{\max}} \geq \frac{1}{4} e^{\mu(s) + (1-s)\mu'(s) - (1-s)\sqrt{2\mu''(s)}}. \quad (120)$$

Let $\dot{R}_1 \triangleq \frac{\log(M/L)}{E_1}$ and $\tilde{R}_1 \triangleq \frac{\log(\tilde{M}/L)}{E_1}$. From the definition of \tilde{M} , we have $\tilde{M} \leq M \leq 2\tilde{M}$. Consequently,

$$\dot{R}_1 - \frac{1}{E_1} \leq \tilde{R}_1 \leq \dot{R}_1. \quad (121)$$

By following the steps that led to (106), we thus obtain

$$\begin{aligned} & P_e(E_1, \tilde{M}, L) \\ & \geq \exp \left[-E_1 \left(\left(\sqrt{\frac{1}{N_0}} - \sqrt{\frac{\tilde{R}_1}{\log e}} \right)^2 + O\left(\frac{1}{\sqrt{E_1}}\right) \right) \right] \\ & = \exp \left[-E_1 \left(\left(\sqrt{\frac{1}{N_0}} - \sqrt{\frac{\dot{R}_1}{\log e}} \right)^2 + O\left(\frac{1}{\sqrt{E_1}}\right) \right) \right]. \end{aligned} \quad (122)$$

To lower-bound $P_e(E_2, L + 1)$, we use the monotonicity of $P_e(E_2, L + 1)$ in L and then apply (111) with $\dot{R}_2 \triangleq \frac{\log L}{E_2}$. This yields

$$\begin{aligned} & P_e(E_2, L + 1) \\ & \geq P_e(E_2, L) \\ & \geq \exp \left[-E_2 \left(\frac{1}{2N_0} \left(1 + \frac{1}{\frac{2\dot{R}_2 E_2}{2} - 1} \right) + O\left(\frac{\ln E_2}{E_2}\right) \right) \right]. \end{aligned} \quad (123)$$

Let

$$\Xi_1(\dot{R}_1) \triangleq \left(\sqrt{\frac{1}{N_0}} - \sqrt{\frac{\dot{R}_1}{\log e}} \right)^2$$

and

$$\Xi_2(\dot{R}_2) \triangleq \frac{1}{2N_0} \left(1 + \frac{1}{\frac{2\dot{R}_2 E_2}{2} - 1} \right).$$

Then, by substituting (122) and (123) in (115), and by using (114), we obtain

$$P_e^\perp(E, M) \geq e^{-E_1 \left(\Xi_1(\dot{R}_1) + O\left(\frac{1}{\sqrt{E_1}}\right) \right)} e^{-E_2 \left(\Xi_2(\dot{R}_2) + O\left(\frac{\ln E_2}{E_2}\right) \right)}. \quad (124)$$

This implies that the error exponent of $P_e^\perp(E, M)$ is upper-bounded by a convex combination of $\Xi_1(\dot{R}_1)$ and $\Xi_2(\dot{R}_2)$. Indeed, let $\lambda \triangleq \frac{E_1}{E}$. Then, (124) can be written as

$$P_e^\perp(E, M) \geq e^{-E \left(\lambda \Xi_1(\dot{R}_1) + (1-\lambda) \Xi_2(\dot{R}_2) + O\left(\frac{1}{\sqrt{E}}\right) \right)} \quad (125)$$

and

$$\begin{aligned} \frac{\log M}{E} &= \frac{\log(M/L) + \log L}{E} \\ &= \lambda \frac{\log(M/L)}{E_1} + (1-\lambda) \frac{\log L}{E_2} \\ &= \lambda \dot{R}_1 + (1-\lambda) \dot{R}_2. \end{aligned}$$

Let $\dot{R} \triangleq \frac{\log M}{E} \leq \frac{\log e}{4N_0}$ and $\gamma_E \triangleq \min\left\{\frac{1}{\sqrt{E}}, \frac{\dot{R}}{2}\right\}$. We conclude the proof of the lower bound in (22) by choosing in (125)

$$\lambda = \lambda_E \triangleq \frac{\dot{R} - \gamma_E}{\frac{\log e}{4N_0} - \gamma_E}$$

and the rates per unit-energy $\dot{R}_1 = \frac{1}{4} \frac{\log e}{N_0}$ and $\dot{R}_2 = \gamma_E$. It follows that

$$\begin{aligned} P_e^\perp(E, M) &\geq e^{-E \left(\frac{\lambda_E}{4N_0} + \frac{1-\lambda_E}{2N_0} + \frac{1-\lambda_E}{N_0 2^{\gamma_E(1-\lambda_E)E} E^{-2N_0}} + O\left(\frac{1}{\sqrt{E}}\right) \right)} \\ &= e^{-E \left(\frac{1}{2N_0} - \frac{\lambda_E}{4N_0} + \frac{1-\lambda_E}{N_0 2^{\gamma_E(1-\lambda_E)E} E^{-2N_0}} + O\left(\frac{1}{\sqrt{E}}\right) \right)}. \quad (126) \end{aligned}$$

Noting that $\lambda_E = \frac{\dot{R}}{(\log e)/4N_0} + O\left(\frac{1}{\sqrt{E}}\right)$ and that $\frac{1}{2^{\gamma_E(1-\lambda_E)E} E^{-2N_0}}$ is of order $O(1/\sqrt{E})$, (126) can be written as

$$P_e^\perp(E, M) \geq e^{-E \left(\frac{1}{2N_0} - \frac{\dot{R}}{\log e} + O\left(\frac{1}{\sqrt{E}}\right) \right)}, \quad 0 < \dot{R} \leq \frac{1}{4} \frac{\log e}{N_0}. \quad (127)$$

We can thus find a function $E \mapsto \beta_E$ of order $O(1/\sqrt{E})$ for which the lower bound in (22) holds.

APPENDIX III PROOF OF LEMMA 10

To prove Lemma 10, we treat the cases where $\ell_n = O(1)$ and where $\ell_n = \omega(1)$ separately. In the former case, each user is assigned an exclusive channel use to convey whether it is active or not. The probability of a detection error $P(\mathcal{D})$ can then be analyzed by similar steps as in the proof of Theorem 8. In the latter case, we proceed similarly as in the proof of [1, Th. 2]. That is, we draw signatures i.i.d. at random according to a zero-mean Gaussian distribution, followed by a truncation step to ensure that the energy of each signature is upper-bounded by E_n'' . The decoder then produces a vector of length ℓ_n with zeros and ones, where a one in the i -th position indicates that user i is active. To this end, it chooses the vector that, among all zero-one vectors with not more than a predefined

number of ones, approximates the received symbols best in terms of Euclidean distance. The probability of a detection error probability $P(\mathcal{D})$ can then be analyzed by following similar steps as in the proof of [1, Th. 2].

A. Bounded ℓ_n

When ℓ_n is bounded in n , one can employ a scheme where each user gets an exclusive channel use to convey whether it is active or not. For such a scheme, it is easy to show that (see the proof of Theorem 8) the probability of a detection error $P(\mathcal{D})$ is upper-bounded by

$$P(\mathcal{D}) \leq \ell_n e^{-E_n'' t}$$

for some $t > 0$. Clearly, when ℓ_n is bounded, we have $k_n \log \ell_n = o(n)$. Thus, the energy E_n'' used for detection is given by $bc_n \ln \ell_n$ and tends to infinity since $c_n \rightarrow \infty$ as $n \rightarrow \infty$. It follows that $P(\mathcal{D})$ tends to zero as $n \rightarrow \infty$.

B. Unbounded ℓ_n

Next we prove Lemma 10 for the case where $\ell_n \rightarrow \infty$ as $n \rightarrow \infty$. To this end, we closely follow the proof of [1, Th. 2], but with the power constraint replaced by an energy constraint. Specifically, we analyze $P(\mathcal{D})$ for the user-detection scheme given in [1], where signatures are drawn i.i.d. according to a zero-mean Gaussian distribution. Note that the proof in [1] assumes that

$$\lim_{n \rightarrow \infty} \ell_n e^{-\delta k_n} = 0 \quad (128)$$

for all $\delta > 0$. However, in our case this assumption is not necessary.

To show that all signatures satisfy the energy constraint, we follow the technique used in the proof of Lemma 11. Similar to Lemma 11, we denote by $\tilde{q}(\cdot)$ the probability density function of a zero-mean Gaussian random variable with variance $E_n''/(2n'')$. We further let

$$\tilde{\mathbf{q}}(\mathbf{u}) = \prod_{i=1}^{n''} \tilde{q}(u_i), \quad \mathbf{u} = (u_1, \dots, u_{n''})$$

and

$$\mathbf{q}(\mathbf{u}) = \frac{1}{\mu} \mathbf{1}(\|\mathbf{u}\|^2 \leq E_n'') \tilde{\mathbf{q}}(\mathbf{u})$$

where

$$\mu = \int \mathbf{1}(\|\mathbf{u}\|^2 \leq E_n'') \tilde{\mathbf{q}}(\mathbf{u}) d\mathbf{u}$$

is a normalizing constant. Clearly, any vector \mathbf{S}_i distributed according to $\mathbf{q}(\cdot)$ satisfies the energy constraint E_n'' with probability one. For any index set $\mathcal{I} \subseteq \{1, \dots, \ell_n\}$, let the matrices $\underline{\mathbf{S}}_{\mathcal{I}}$ and $\tilde{\underline{\mathbf{S}}}_{\mathcal{I}}$ denote the set of signatures for the users in \mathcal{I} that are distributed as

$$\underline{\mathbf{S}}_{\mathcal{I}} \sim \prod_{i \in \mathcal{I}} \mathbf{q}(\mathbf{S}_i)$$

and

$$\tilde{\underline{\mathbf{S}}}_{\mathcal{I}} \sim \prod_{i \in \mathcal{I}} \tilde{\mathbf{q}}(\mathbf{S}_i)$$

respectively. As noted in the proof of Lemma 11, we have

$$\mathbf{q}(\mathbf{s}_i) \leq \frac{1}{\mu} \tilde{\mathbf{q}}(\mathbf{s}_i). \quad (129)$$

To analyze the detection error probability, we first define the ℓ_n -length vector \mathbf{D}^a as

$$\mathbf{D}^a \triangleq (\mathbf{1}(W_1 \neq 0), \dots, \mathbf{1}(W_{\ell_n} \neq 0)).$$

For some $c'' > 0$, let

$$v_n \triangleq k_n(1 + c'').$$

Further let

$$\mathcal{B}^n(v_n) \triangleq \{\mathbf{d} \in \{0, 1\}^{\ell_n} : 1 \leq |\mathbf{d}| \leq v_n\}$$

where $|\mathbf{d}|$ denotes the number of 1's in \mathbf{d} . We denote by \mathbf{S}^a the matrix of signatures of all users, which are generated independently according to $\mathbf{q}(\cdot)$, and we denote by \mathbf{Y}^a the first n'' received symbols, based on which the receiver performs user detection. The receiver outputs the length- ℓ_n vector

$$\hat{\mathbf{d}} = \arg \min_{\mathbf{d} \in \mathcal{B}^n(v_n)} \|\mathbf{Y}^a - \mathbf{S}^a \mathbf{d}\| \quad (130)$$

indicating the set of active users. By the union bound, the probability of a detection error $P(\mathcal{D})$ is upper-bounded by

$$\begin{aligned} P(\mathcal{D}) &\leq \Pr(|\mathbf{D}^a| > v_n) \\ &\quad + \sum_{\mathbf{d} \in \mathcal{B}^n(v_n)} \Pr(\mathcal{E}_d | \mathbf{D}^a = \mathbf{d}) \Pr(\mathbf{D}^a = \mathbf{d}) \\ &\quad + \Pr(\mathcal{E}_d | |\mathbf{D}^a| = 0) \Pr(|\mathbf{D}^a| = 0) \end{aligned} \quad (131)$$

where $|\mathbf{D}^a|$ denotes the number of 1's in \mathbf{D}^a and \mathcal{E}_d denotes the event that there is a detection error. Next, we show that each term on the RHS of (131) vanishes as $n \rightarrow \infty$.

Using the Chernoff bound for the binomial distribution, we have

$$\Pr(|\mathbf{D}^a| > v_n) \leq \exp(-k_n c''/3). \quad (132)$$

For unbounded k_n , this probability of error vanishes as $n \rightarrow \infty$. For bounded k_n , it vanishes by first letting $n \rightarrow \infty$ and then letting $c'' \rightarrow \infty$.

We continue with the term $\Pr(\mathcal{E}_d | \mathbf{D}^a = \mathbf{d})$. For a given $\mathbf{D}^a = \mathbf{d}$, let κ_1 and κ_2 denote the number of miss detections and false alarms, respectively, i.e.,

$$\begin{aligned} \kappa_1 &= |\{j : d_j \neq 0, \hat{d}_j = 0\}| \\ \kappa_2 &= |\{j : d_j = 0, \hat{d}_j \neq 0\}| \end{aligned}$$

where d_j and \hat{d}_j denote the j -th components of the vectors \mathbf{d} and $\hat{\mathbf{d}}$, respectively. An error happens only if either κ_1 , or κ_2 , or both are strictly positive. The number of users that are either active or are declared as active by the receiver satisfies $|\mathbf{d}| + \kappa_2 = |\hat{\mathbf{d}}| + \kappa_1$, so

$$|\mathbf{d}| + \kappa_2 \leq v_n + \kappa_1$$

since $|\hat{\mathbf{d}}|$ is upper-bounded by v_n by the decoding rule (130). So, the pair (κ_1, κ_2) belongs to the following set:

$$\begin{aligned} \mathcal{W}_{\mathbf{d}}^{\ell_n} &= \left\{ (\kappa_1, \kappa_2) : \kappa_1 \in \{0, 1, \dots, |\mathbf{d}|\}, \kappa_2 \in \{0, 1, \dots, v_n\}, \right. \\ &\quad \left. \kappa_1 + \kappa_2 \geq 1, |\mathbf{d}| + \kappa_2 \leq v_n + \kappa_1 \right\}. \end{aligned} \quad (133)$$

Let $\Pr(\mathcal{E}_{\kappa_1, \kappa_2} | \mathbf{D}^a = \mathbf{d})$ be the probability of having exactly κ_1 miss detections and κ_2 false alarms given that $\mathbf{D}^a = \mathbf{d}$. For given \mathbf{d} and $\hat{\mathbf{d}}$, let $\mathcal{A}^* \triangleq \{j : d_j \neq 0\}$ and $\mathcal{A} \triangleq \{j : \hat{d}_j \neq 0\}$. We further define $\mathcal{A}_1 \triangleq \mathcal{A}^* \setminus \mathcal{A}$, $\mathcal{A}_2 \triangleq \mathcal{A} \setminus \mathcal{A}^*$, and

$$T_{\mathcal{A}} \triangleq \|\mathbf{Y}^a - \sum_{j \in \mathcal{A}} \mathbf{S}_j\|^2 - \|\mathbf{Y}^a - \sum_{j \in \mathcal{A}^*} \mathbf{S}_j\|^2.$$

Using the analysis that led to [1, Eq. (67)], we obtain

$$\begin{aligned} &\Pr(\mathcal{E}_{\kappa_1, \kappa_2} | \mathbf{D}^a = \mathbf{d}) \\ &\leq \binom{|\mathcal{A}^*|}{\kappa_1} \binom{\ell_n}{\kappa_2} \mathbb{E}_{\underline{\mathbf{S}}_{\mathcal{A}^*}, \mathbf{Y}} \left[(\mathbb{E}_{\underline{\mathbf{S}}_{\mathcal{A}_2}} [\mathbf{1}(T_{\mathcal{A}} \leq 0) | \underline{\mathbf{S}}_{\mathcal{A}^*}, \mathbf{Y}])^\rho \right] \\ &\leq \binom{|\mathcal{A}^*|}{\kappa_1} \binom{\ell_n}{\kappa_2} \left(\frac{1}{\mu} \right)^{|\mathcal{A}^*|} \left(\frac{1}{\mu} \right)^{\rho \kappa_2} \\ &\quad \times \mathbb{E}_{\underline{\mathbf{S}}_{\mathcal{A}^*}, \mathbf{Y}} \left[(\mathbb{E}_{\underline{\mathbf{S}}_{\mathcal{A}_2}} [\mathbf{1}(T_{\mathcal{A}} \leq 0) | \tilde{\underline{\mathbf{S}}}_{\mathcal{A}^*}, \mathbf{Y}])^\rho \right] \end{aligned} \quad (134)$$

where we used that

$$\mathbf{q}(\underline{\mathbf{S}}_{\mathcal{A}_2}) \leq \left(\frac{1}{\mu} \right)^{\kappa_2} \prod_{i \in \mathcal{A}_2} \tilde{\mathbf{q}}(\mathbf{s}_i) \quad (135)$$

and

$$\mathbf{q}(\underline{\mathbf{S}}_{\mathcal{A}^*}) \leq \left(\frac{1}{\mu} \right)^{|\mathcal{A}^*|} \prod_{i \in \mathcal{A}^*} \tilde{\mathbf{q}}(\mathbf{s}_i) \quad (136)$$

which follow from (129).

For every $\rho \in [0, 1]$ and $\lambda \geq 0$, we obtain from [1, Eq. (78)] that

$$\begin{aligned} &\binom{|\mathcal{A}^*|}{\kappa_1} \binom{\ell_n}{\kappa_2} \mathbb{E}_{\underline{\mathbf{S}}_{\mathcal{A}^*}, \mathbf{Y}} \left[(\mathbb{E}_{\underline{\mathbf{S}}_{\mathcal{A}_2}} [\mathbf{1}(T_{\mathcal{A}} \leq 0) | \tilde{\underline{\mathbf{S}}}_{\mathcal{A}^*}, \mathbf{Y}])^\rho \right] \\ &\leq \exp[-\tilde{E}_n g_{\lambda, \rho}^n(\kappa_1, \kappa_2, \mathbf{d})] \end{aligned} \quad (137)$$

where

$$\tilde{E}_n \triangleq E_n''/2$$

and

$$\begin{aligned} &g_{\lambda, \rho}^n(\kappa_1, \kappa_2, \mathbf{d}) \\ &\triangleq -\frac{(1-\rho)n''}{2\tilde{E}_n} \log \left(1 + \lambda \kappa_2 \frac{\tilde{E}_n}{n''} \right) \\ &\quad + \frac{n''}{2\tilde{E}_n} \log \left(1 + \lambda(1-\lambda\rho)\kappa_2 \frac{\tilde{E}_n}{n''} + \lambda\rho(1-\lambda\rho)\kappa_1 \frac{\tilde{E}_n}{n''} \right) \\ &\quad - \frac{|\mathbf{d}|}{\tilde{E}_n} H_2 \left(\frac{\kappa_1}{|\mathbf{d}|} \right) - \frac{\rho \ell_n}{\tilde{E}_n} H_2 \left(\frac{\kappa_2}{\ell_n} \right). \end{aligned} \quad (138)$$

It thus follows from (134) and (137) that

$$\begin{aligned} &\Pr(\mathcal{E}_{\kappa_1, \kappa_2} | \mathbf{D}^a = \mathbf{d}) \\ &\leq \left(\frac{1}{\mu} \right)^{|\mathcal{A}^*| + \rho \kappa_2} \exp[-\tilde{E}_n g_{\lambda, \rho}^n(\kappa_1, \kappa_2, \mathbf{d})]. \end{aligned} \quad (139)$$

We next show that the RHS of (139) vanishes as $n \rightarrow \infty$. To this end, we first show that $(1/\mu)^{|\mathcal{A}^*| + \rho \kappa_2} \rightarrow 1$ as $n \rightarrow \infty$ uniformly in $(\kappa_1, \kappa_2) \in \mathcal{W}_{\mathbf{d}}^{\ell_n}$ and $\mathbf{d} \in \mathcal{B}^n(v_n)$. From the definition of μ , we have

$$\mu = 1 - \Pr \left(\|\tilde{\mathbf{S}}_1\|_2^2 > E_n'' \right).$$

Furthermore, by defining $\tilde{\mathbf{S}}_0 \triangleq \frac{2n''}{\tilde{E}_n} \|\tilde{\mathbf{S}}_1\|_2^2$ and following the steps that led to (42), we obtain that, for $(\kappa_1, \kappa_2) \in \mathcal{W}_{\mathbf{d}}^{\ell_n}$ and $\mathbf{d} \in \mathcal{B}^n(v_n)$,

$$\begin{aligned} 1 &\leq \left(\frac{1}{\mu}\right)^{|\mathcal{A}^*| + \rho\kappa_2} \\ &\leq \left(\frac{1}{\mu}\right)^{2v_n} \\ &\leq \left(1 - \exp\left[-\frac{n''}{2}\tau\right]\right)^{-2v_n} \end{aligned} \quad (140)$$

where $\tau = (1 - \ln 2)$. Here, in the second inequality we used that $|\mathcal{A}^*| = |\mathbf{d}| \leq v_n$ and $\rho\kappa_2 \leq v_n$. Since $k_n \log \ell_n = O(n)$, we have $k_n = o(n)$. This implies that, for every fixed $c'' > 0$, we have $v_n = o(n)$ because in this case $v_n = \Theta(k_n)$. Furthermore, $n'' = \Theta(n)$. As noted before, for any two non-negative sequences $\{a_n\}$ and $\{b_n\}$ satisfying $a_n \rightarrow 0$ and $a_n b_n \rightarrow 0$ as $n \rightarrow \infty$, it holds that $(1 - a_n)^{-b_n} \rightarrow 1$ as $n \rightarrow \infty$. It follows that the RHS of (140) tends to one as $n \rightarrow \infty$ uniformly in $(\kappa_1, \kappa_2) \in \mathcal{W}_{\mathbf{d}}^{\ell_n}$ and $\mathbf{d} \in \mathcal{B}^n(v_n)$. Consequently, there exists a positive constant n_0 that is independent of κ_1, κ_2 , and \mathbf{d} and satisfies

$$\left(\frac{1}{\mu}\right)^{|\mathcal{A}^*| + \rho\kappa_2} \leq 2, \quad (\kappa_1, \kappa_2) \in \mathcal{W}_{\mathbf{d}}^{\ell_n}, \mathbf{d} \in \mathcal{B}^n(v_n), n \geq n_0. \quad (141)$$

To bound the exponential term on the RHS of (139), we need the following lemma.

Lemma 14: Assume that $k_n = \Omega(1)$ and $k_n \log \ell_n = O(n)$. If c' and c'' are sufficiently large, then there exist two positive constants γ and n'_0 such that $g_{\frac{2}{3}, \frac{3}{4}}^n(\kappa_1, \kappa_2, \mathbf{d})$, i.e., (138) evaluated at $\lambda = 2/3$ and $\rho = 3/4$, satisfies

$$\min_{\mathbf{d} \in \mathcal{B}^n(v_n)} \min_{(\kappa_1, \kappa_2) \in \mathcal{W}_{\mathbf{d}}^{\ell_n}} g_{\frac{2}{3}, \frac{3}{4}}^n(\kappa_1, \kappa_2, \mathbf{d}) \geq \gamma, \quad n \geq n'_0. \quad (142)$$

Proof: See Appendix III-C. ■

Lemma 14 implies that $\Pr(\mathcal{E}_{\mathbf{d}} | \mathbf{D}^a = \mathbf{d})$ vanishes as $n \rightarrow \infty$ uniformly in $\mathbf{d} \in \mathcal{B}^n(v_n)$. Indeed, if $\mathbf{d} \in \mathcal{B}^n(v_n)$, then $|\mathbf{d}| \leq v_n$, which implies that $\kappa_1 \leq v_n$. Furthermore, since the decoder outputs a vector in $\mathcal{B}^n(v_n)$, we also have $\kappa_2 \leq v_n$. It thus follows from (139), (141), and (142) that

$$\begin{aligned} \Pr(\mathcal{E}_{\mathbf{d}} | \mathbf{D}^a = \mathbf{d}) &= \sum_{(\kappa_1, \kappa_2) \in \mathcal{W}_{\mathbf{d}}^{\ell_n}} \Pr(\mathcal{E}_{\kappa_1, \kappa_2} | \mathbf{D}^a = \mathbf{d}) \\ &\leq 2v_n^2 \exp[-\tilde{E}_n \gamma] \\ &= 2 \exp\left[-\tilde{E}_n \left(\gamma - \frac{2 \ln v_n}{\tilde{E}_n}\right)\right] \end{aligned} \quad (143)$$

for $\mathbf{d} \in \mathcal{B}^n(v_n)$ and $n \geq \max(n_0, n'_0)$. By the definition of v_n and \tilde{E}_n ,

$$\frac{2 \ln v_n}{\tilde{E}_n} = \frac{4 \ln(1 + c'')}{bc_n \ln \ell_n} + \frac{4 \ln k_n}{bc_n \ln \ell_n}. \quad (144)$$

The first term on the RHS of (144) vanishes as $n \rightarrow \infty$ since ℓ_n is unbounded. The second term on the RHS of (144) is upper-bounded by $4/(bc_n)$ since $\ln k_n \leq \ln \ell_n$. This vanishes as $c_n \rightarrow \infty$ (which is the case when $k_n \log \ell_n = o(n)$), or it can be made arbitrarily small by choosing $c_n = c'$ sufficiently

large (when $k_n \log \ell_n = \Theta(n)$). Consequently, we obtain that $\frac{2 \ln v_n}{\tilde{E}_n} < \gamma$ for sufficiently large n and c_n , which implies that the RHS of (143) tends to zero as $n \rightarrow \infty$. This, in turn, demonstrates that the second term on the RHS of (131) vanishes as $n \rightarrow \infty$ upon averaging over $\mathbf{d} \in \mathcal{B}^n(v_n)$.

We finish the proof of Lemma 10 by analyzing the third term on the RHS of (131). Since $\Pr(|\mathbf{D}^a| = 0) = ((1 - \alpha_n)^{\frac{1}{\alpha_n}})^{k_n}$, this term is given by

$$\begin{aligned} &\Pr(\mathcal{E}_{\mathbf{d}} | |\mathbf{D}^a| = 0) \Pr(|\mathbf{D}^a| = 0) \\ &= \Pr(\mathcal{E}_{\mathbf{d}} | |\mathbf{D}^a| = 0) \left((1 - \alpha_n)^{\frac{1}{\alpha_n}} \right)^{k_n} \end{aligned}$$

and vanishes if k_n is unbounded. Next, we show that this term also vanishes when k_n is bounded. When $|\mathbf{D}^a| = 0$, an error occurs only if there are false alarms. For κ_2 false alarms, let $\tilde{\mathbf{S}} \triangleq \sum_{j=1}^{\kappa_2} \mathbf{S}_j$, and let S'_i denote the i -th component of $\tilde{\mathbf{S}}$. From [1, Eq. (303)], we obtain the following upper bound on the probability that there are κ_2 false alarms when $|\mathbf{D}^a| = 0$:

$$\begin{aligned} &\Pr(\mathcal{E}_{\kappa_2} | |\mathbf{d}| = 0) \\ &\leq \binom{\ell_n}{\kappa_2} \mathbb{E}_{\tilde{\mathbf{S}}_{\mathcal{A}_2}} \left[\Pr\left\{ \sum_{i=1}^{n''} Z_i S'_i \geq \frac{1}{2} \|\tilde{\mathbf{S}}\|^2 \mid \tilde{\mathbf{S}} \right\} \right] \\ &\leq \left(\frac{1}{\mu}\right)^{\kappa_2} \binom{\ell_n}{\kappa_2} \mathbb{E}_{\tilde{\mathbf{S}}_{\mathcal{A}_2}} \left[\Pr\left\{ \sum_{i=1}^{n''} Z_i \tilde{S}'_i \geq \frac{1}{2} \|\tilde{\mathbf{S}}\|^2 \mid \tilde{\mathbf{S}} \right\} \right] \end{aligned}$$

where in the last inequality we used (129). Here, $\tilde{\mathbf{S}} \triangleq \sum_{j=1}^{\kappa_2} \tilde{\mathbf{S}}_j$ and \tilde{S}'_i denotes the i -th component of $\tilde{\mathbf{S}}$. By following the analysis that led to [1, Eq. (309)], we obtain

$$\Pr(\mathcal{E}_{\kappa_2} | |\mathbf{d}| = 0) \leq \left(\frac{1}{\mu}\right)^{\kappa_2} \exp\left[-\tilde{E}_n (q'_n(\kappa_2) - u'_n(\kappa_2))\right]$$

where

$$q'_n(\kappa_2) \triangleq \frac{n''}{2\tilde{E}_n} \log \left(1 + \frac{\kappa_2 \tilde{E}_n}{4n''} \right)$$

and

$$u'_n(\kappa_2) \triangleq \frac{\ell_n}{\tilde{E}_n} H_2 \left(\frac{\kappa_2}{\ell_n} \right).$$

As in (141), we upper-bound $(1/\mu)^{\kappa_2} \leq 2$ uniformly in κ_2 for $n \geq n_0$. Furthermore, we observe that the behaviors of $q'_n(\kappa_2)$ and $u'_n(\kappa_2)$ are similar to $q_n(\kappa_2)$ and $v_n(\kappa_2)$ given later in (167) and in (169), respectively. So by following the steps in Appendix III-C2, we can thus show that

$$\liminf_{n \rightarrow \infty} \min_{1 \leq \kappa_2 \leq v_n} q'_n(\kappa_2) > 0$$

and

$$\limsup_{n \rightarrow \infty} \min_{1 \leq \kappa_2 \leq v_n} \frac{u'_n(\kappa_2)}{q'_n(\kappa_2)} < 1.$$

It follows that there exist positive constants τ' and \tilde{n}_0 such that

$$\begin{aligned} \Pr(\mathcal{E}_{\mathbf{d}} | |\mathbf{d}| = 0) &= \sum_{\kappa_2=1}^{v_n} \Pr(\mathcal{E}_{\kappa_2} | |\mathbf{d}| = 0) \\ &\leq 2v_n \exp\left[-\tilde{E}_n \tau'\right] \end{aligned} \quad (145)$$

for $n \geq \max(n_0, \tilde{n}_0)$. We have already shown that $v_n^2 \exp[-\tilde{E}_n \tau']$ vanishes as $n \rightarrow \infty$ (cf. (143)–(144)), which implies that the same is true for $2v_n \exp[-\tilde{E}_n \tau']$. It thus follows that $P(\mathcal{E}_d | |\mathbf{d}| = 0)$ tends to zero as $n \rightarrow \infty$. This was the last step required to prove Lemma 10.

C. Proof of Lemma 14

We first note that

$$\begin{aligned} & \min_{\mathbf{d} \in \mathcal{B}^n(v_n)} \min_{(\kappa_1, \kappa_2) \in \mathcal{W}_d^{\ell_n}} g_{\lambda, \rho}^n(\kappa_1, \kappa_2, \mathbf{d}) \\ &= \min \left\{ \begin{aligned} & \min_{\mathbf{d} \in \mathcal{B}^n(v_n)} \min_{1 \leq \kappa_1 \leq v_n} g_{\lambda, \rho}^n(\kappa_1, 0, \mathbf{d}), \\ & \min_{\mathbf{d} \in \mathcal{B}^n(v_n)} \min_{1 \leq \kappa_2 \leq v_n} g_{\lambda, \rho}^n(0, \kappa_2, \mathbf{d}), \\ & \min_{\mathbf{d} \in \mathcal{B}^n(v_n)} \min_{\substack{1 \leq \kappa_1 \leq v_n \\ 1 \leq \kappa_2 \leq v_n}} g_{\lambda, \rho}^n(\kappa_1, \kappa_2, \mathbf{d}) \end{aligned} \right\}. \end{aligned}$$

Then, we show that, for $\lambda = 2/3$ and $\rho = 3/4$,

$$\liminf_{n \rightarrow \infty} \min_{\mathbf{d} \in \mathcal{B}^n(v_n)} \min_{1 \leq \kappa_1 \leq v_n} g_{\lambda, \rho}^n(\kappa_1, 0, \mathbf{d}) > 0 \quad (146)$$

$$\liminf_{n \rightarrow \infty} \min_{\mathbf{d} \in \mathcal{B}^n(v_n)} \min_{1 \leq \kappa_2 \leq v_n} g_{\lambda, \rho}^n(0, \kappa_2, \mathbf{d}) > 0 \quad (147)$$

$$\liminf_{n \rightarrow \infty} \min_{\mathbf{d} \in \mathcal{B}^n(v_n)} \min_{\substack{1 \leq \kappa_1 \leq v_n \\ 1 \leq \kappa_2 \leq v_n}} g_{\lambda, \rho}^n(\kappa_1, \kappa_2, \mathbf{d}) > 0 \quad (148)$$

from which Lemma 14 follows.

In order to prove (146)–(148), we first lower-bound $g_{\lambda, \rho}^n(\kappa_1, \kappa_2, \mathbf{d})$ by using that, for $0 \leq \lambda \rho \leq 1$, we have

$$\begin{aligned} & 2 \log \left(1 + \lambda(1 - \lambda \rho) \kappa_2 \tilde{E}_n / n'' + \lambda \rho(1 - \lambda \rho) \kappa_1 \tilde{E}_n / n'' \right) \\ & \geq \log \left(1 + \lambda(1 - \lambda \rho) \kappa_2 \tilde{E}_n / n'' \right) \\ & \quad + \log \left(1 + \lambda \rho(1 - \lambda \rho) \kappa_1 \tilde{E}_n / n'' \right). \end{aligned} \quad (149)$$

Applying (149) in the second term on the RHS of (138), we obtain that

$$g_{\lambda, \rho}^n(\kappa_1, \kappa_2, \mathbf{d}) \geq a_{\lambda, \rho}^n(\kappa_1, \mathbf{d}) + b_{\lambda, \rho}^n(\kappa_2) \quad (150)$$

where

$$\begin{aligned} a_{\lambda, \rho}^n(\kappa_1, \mathbf{d}) & \triangleq \frac{n''}{4\tilde{E}_n} \log \left(1 + \lambda \rho(1 - \lambda \rho) \kappa_1 \tilde{E}_n / n'' \right) \\ & \quad - \frac{|\mathbf{d}|}{\tilde{E}_n} H_2 \left(\frac{\kappa_1}{|\mathbf{d}|} \right) \end{aligned}$$

and

$$\begin{aligned} b_{\lambda, \rho}^n(\kappa_2) & \triangleq \frac{n''}{4\tilde{E}_n} \log \left(1 + \lambda(1 - \lambda \rho) \kappa_2 \tilde{E}_n / n'' \right) \\ & \quad - \frac{(1 - \rho)}{2\tilde{E}_n} \log(1 + \lambda \kappa_2 \tilde{E}_n / n'') - \frac{\rho \ell_n}{\tilde{E}_n} H_2 \left(\frac{\kappa_2}{\ell_n} \right). \end{aligned}$$

1) *Proof of (146):* We have

$$\begin{aligned} g_{\lambda, \rho}^n(\kappa_1, 0, \mathbf{d}) & \geq a_{\lambda, \rho}^n(\kappa_1, \mathbf{d}) + b_{\lambda, \rho}^n(0) \\ & \geq a_{\lambda, \rho}^n(\kappa_1, \mathbf{d}) \end{aligned} \quad (151)$$

by (150) and because $b_{\lambda, \rho}^n(0) = 0$. Consequently,

$$\begin{aligned} & \min_{\mathbf{d} \in \mathcal{B}^n(v_n)} \min_{1 \leq \kappa_1 \leq v_n} g_{\lambda, \rho}^n(\kappa_1, 0, \mathbf{d}) \\ & \geq \min_{\mathbf{d} \in \mathcal{B}^n(v_n)} \min_{1 \leq \kappa_1 \leq v_n} a_{\lambda, \rho}^n(\kappa_1, \mathbf{d}) \end{aligned}$$

and (146) follows by showing that

$$\liminf_{n \rightarrow \infty} \min_{\mathbf{d} \in \mathcal{B}^n(v_n)} \min_{1 \leq \kappa_1 \leq v_n} a_{\lambda, \rho}^n(\kappa_1, \mathbf{d}) > 0. \quad (152)$$

To this end, let

$$\begin{aligned} i_n(\kappa_1) & \triangleq \frac{n''}{4\tilde{E}_n} \log \left(1 + \lambda \rho(1 - \lambda \rho) \kappa_1 \tilde{E}_n / n'' \right) \\ j_n(\kappa_1, \mathbf{d}) & \triangleq \frac{|\mathbf{d}|}{\tilde{E}_n} H_2 \left(\frac{\kappa_1}{|\mathbf{d}|} \right) \end{aligned}$$

so that

$$a_{\lambda, \rho}^n(\kappa_1, \mathbf{d}) = i_n(\kappa_1) \left(1 - \frac{j_n(\kappa_1, \mathbf{d})}{i_n(\kappa_1)} \right). \quad (153)$$

Note that

$$i_n(\kappa_1) \geq \frac{n''}{4\tilde{E}_n} \log \left(1 + \lambda \rho(1 - \lambda \rho) \frac{\tilde{E}_n}{n''} \right), \quad 1 \leq \kappa_1 \leq v_n \quad (154)$$

and

$$\begin{aligned} & \frac{j_n(\kappa_1, \mathbf{d})}{i_n(\kappa_1)} \\ &= \frac{4|\mathbf{d}| H_2 \left(\frac{\kappa_1}{|\mathbf{d}|} \right)}{n'' \log \left(1 + \lambda \rho(1 - \lambda \rho) \kappa_1 \frac{\tilde{E}_n}{n''} \right)} \\ &= \frac{4\kappa_1 \log \left(\frac{|\mathbf{d}|}{\kappa_1} \right) + 4|\mathbf{d}| \left(\frac{\kappa_1}{|\mathbf{d}|} - 1 \right) \log \left(1 - \frac{\kappa_1}{|\mathbf{d}|} \right)}{n'' \log \left(1 + \lambda \rho(1 - \lambda \rho) \kappa_1 \frac{\tilde{E}_n}{n''} \right)}. \end{aligned} \quad (155)$$

Next, we upper-bound $(\kappa_1/|\mathbf{d}| - 1) \log(1 - \kappa_1/|\mathbf{d}|)$. To this end, we note that the function $f(p) = p - (p - 1) \ln(1 - p)$, $0 \leq p \leq 1$ satisfies $f(0) = 0$ and is monotonically increasing in p . It follows that $(p - 1) \ln(1 - p) \leq p$, $0 \leq p \leq 1$, which for $p = \kappa_1/|\mathbf{d}|$ gives

$$\left(\frac{\kappa_1}{|\mathbf{d}|} - 1 \right) \log \left(1 - \frac{\kappa_1}{|\mathbf{d}|} \right) \leq \log e \frac{\kappa_1}{|\mathbf{d}|}. \quad (156)$$

Using (156) in (155), we obtain that

$$\begin{aligned} \frac{j_n(\kappa_1, \mathbf{d})}{i_n(\kappa_1)} & \leq \frac{4 \log(|\mathbf{d}|/\kappa_1) + 4 \log e}{n'' \log \left(1 + \lambda \rho(1 - \lambda \rho) \kappa_1 \tilde{E}_n / n'' \right) / \kappa_1} \\ & \leq \frac{4 \log(|\mathbf{d}|/\kappa_1) + 4 \log e}{n'' \log \left(1 + \lambda \rho(1 - \lambda \rho) v_n \tilde{E}_n / n'' \right) / v_n} \\ & \leq \frac{v_n (4 \log(v_n) + 4 \log e)}{n'' \log \left(1 + \lambda \rho(1 - \lambda \rho) v_n \tilde{E}_n / n'' \right)} \end{aligned} \quad (157)$$

$$= \frac{4 \log v_n + 4 \log e}{\tilde{E}_n \frac{\log(1 + \lambda \rho(1 - \lambda \rho) v_n \tilde{E}_n / n'')}{v_n \tilde{E}_n / n''}} \quad (158)$$

where we have used that $\frac{\log(1+x)}{x}$ is monotonically decreasing in $x > 0$ and that $|\mathbf{d}| \leq v_n$ and $1 \leq \kappa_1 \leq v_n$. Combining (153), (154), and (158), $a_{\lambda,\rho}^n(\kappa_1, \mathbf{d})$ can thus be lower-bounded by

$$a_{\lambda,\rho}^n(\kappa_1, \mathbf{d}) \geq \frac{n''}{4\tilde{E}_n} \log \left(1 + \lambda\rho(1 - \lambda\rho)\tilde{E}_n/n'' \right) \times \left(1 - \frac{4 \log v_n + 4 \log e}{\tilde{E}_n \frac{\log(1+\lambda\rho(1-\lambda\rho)v_n\tilde{E}_n/n'')}{v_n\tilde{E}_n/n''}} \right). \quad (159)$$

Note that the RHS of (159) is independent of κ_1 and \mathbf{d} . To show (152), we consider the following two cases:

Case 1— $k_n \log \ell_n = o(n)$: Recall that if $k_n \log \ell_n = o(n)$, then $\tilde{E}_n = bc_n \ln \ell_n/2$. It follows that the term

$$\frac{v_n \tilde{E}_n}{n''} = \frac{(1 + c'')}{2} c_n \frac{k_n \ln \ell_n}{n} \quad (160)$$

tends to zero as $n \rightarrow \infty$ since $c_n = \ln\left(\frac{n}{k_n \ln \ell_n}\right)$ and $\frac{k_n \ln \ell_n}{n}$ is of order $o(1)$ by assumption. Using that $v_n = \Theta(k_n) = \Omega(1)$, we further have that, for this choice of \tilde{E}_n , $\tilde{E}_n/n'' \rightarrow 0$, $\tilde{E}_n \rightarrow \infty$, and $\frac{\log v_n}{\tilde{E}_n} \rightarrow 0$ as $n \rightarrow \infty$. It follows that

$$\begin{aligned} & \liminf_{n \rightarrow \infty} \min_{\mathbf{d} \in \mathcal{B}^n(v_n)} \min_{1 \leq \kappa_1 \leq v_n} a_{\lambda,\rho}^n(\kappa_1, \mathbf{d}) \\ & \geq \lim_{n \rightarrow \infty} \frac{n''}{4\tilde{E}_n} \log \left(1 + \lambda\rho(1 - \lambda\rho)\tilde{E}_n/n'' \right) \\ & \quad \times \lim_{n \rightarrow \infty} \left(1 - \frac{4 \log v_n + 4 \log e}{\tilde{E}_n \frac{\log(1+\lambda\rho(1-\lambda\rho)v_n\tilde{E}_n/n'')}{v_n\tilde{E}_n/n''}} \right) \\ & = \frac{(\log e) \lambda\rho(1 - \lambda\rho)}{4} \end{aligned} \quad (161)$$

which for $\lambda = 2/3$ and $\rho = 3/4$ is equal to $(\log e)/16$.

Case 2— $k_n \log \ell_n = \Theta(n)$: To analyze this case, we first note that, by the definition of v_n , and because $\log k_n \leq \log \ell_n$, the numerator in (157) satisfies $v_n(4 \log(v_n) + 4 \log e) = O(k_n \log \ell_n)$. Since $k_n \log \ell_n = \Theta(n)$ and $n'' = \Theta(n)$, this further implies that there exist $a_2 > 0$ and $\tilde{n}'_0 > 0$ such that

$$\frac{v_n(4 \log(v_n) + 4 \log e)}{n''} \leq a_2, \quad n \geq \tilde{n}'_0. \quad (162)$$

We next note that (159) can be written as

$$a_{\lambda,\rho}^n(\kappa_1, \mathbf{d}) \geq \frac{n''}{4\tilde{E}_n} \log \left(1 + \lambda\rho(1 - \lambda\rho)\tilde{E}_n/n'' \right) \times \left(1 - \frac{v_n(4 \log(v_n) + 4 \log e)}{n'' \log \left(1 + \lambda\rho(1 - \lambda\rho)v_n\tilde{E}_n/n'' \right)} \right). \quad (163)$$

The RHS of (163) is independent of κ_1 and \mathbf{d} . We next show that it is bounded away from zero.

Recall that, if $k_n \log \ell_n = \Theta(n)$, then $\tilde{E}_n = bc' \ln \ell_n/2$. We then choose c' sufficiently large such that, for some $\tilde{n}''_0 \geq \tilde{n}'_0$,

$$\log \left(1 + \lambda\rho(1 - \lambda\rho)v_n\tilde{E}_n/n'' \right) > a_2, \quad n \geq \tilde{n}''_0. \quad (164)$$

Such a choice is possible since we have

$$\frac{v_n \tilde{E}_n}{n''} = \frac{1 + c''}{2} c' \frac{k_n \ln \ell_n}{n}$$

and, by assumption, $\frac{k_n \ln \ell_n}{n} = \Theta(1)$. Consequently, for sufficiently large n , $v_n \tilde{E}_n/n''$ is monotonically increasing in c' and ranges from zero to infinity. Combining (164) with (162) implies that the expression inside the large parentheses on the RHS of (163) is bounded away from zero for $n \geq \tilde{n}''_0$.

We next consider the remaining term on the RHS of (163). To this end, we note that, if k_n is unbounded, then the assumption $k_n \log \ell_n = \Theta(n)$ implies that $\ln \ell_n = o(n)$. It follows that $\tilde{E}_n/n'' = c' \frac{\ln \ell_n}{2n} \rightarrow 0$ as $n \rightarrow \infty$. If k_n is bounded, then $\ln \ell_n = \Theta(n)$, so \tilde{E}_n/n'' is bounded. In both cases, $\frac{n''}{4\tilde{E}_n} \log(1 + \lambda\rho(1 - \lambda\rho)\tilde{E}_n/n'')$ is bounded away from zero for sufficiently large n .

Applying the above lines of argument to (163), we obtain that

$$\liminf_{n \rightarrow \infty} \min_{\mathbf{d} \in \mathcal{B}^n(v_n)} \min_{1 \leq \kappa_1 \leq v_n} a_{\lambda,\rho}^n(\kappa_1, \mathbf{d}) > 0 \quad (165)$$

which concludes the analysis of the second case.

The claim (146) follows now by combining the above two cases, i.e., (161) and (165).

2) *Proof of (147):* Since $a_{\lambda,\rho}^n(0, \mathbf{d}) = 0$, we have that

$$\min_{\mathbf{d} \in \mathcal{B}^n(v_n)} \min_{1 \leq \kappa_2 \leq v_n} g_{\lambda,\rho}^n(0, \kappa_2, \mathbf{d}) \geq \min_{1 \leq \kappa_2 \leq v_n} b_{\lambda,\rho}^n(\kappa_2).$$

Thus, (147) follows by showing that

$$\liminf_{n \rightarrow \infty} \min_{1 \leq \kappa_2 \leq v_n} b_{\lambda,\rho}^n(\kappa_2) > 0. \quad (166)$$

To prove (166), we define

$$q_n(\kappa_2) \triangleq \frac{n''}{4\tilde{E}_n} \log \left(1 + \lambda(1 - \lambda\rho)\kappa_2\tilde{E}_n/n'' \right) \quad (167)$$

$$r_n(\kappa_2) \triangleq \frac{(1 - \rho)}{2\tilde{E}_n} \log(1 + \lambda\kappa_2\tilde{E}_n/n'') \quad (168)$$

$$u_n(\kappa_2) \triangleq \frac{\rho \ell_n}{\tilde{E}_n} H_2 \left(\frac{\kappa_2}{\ell_n} \right) \quad (169)$$

so that

$$b_{\lambda,\rho}^n(\kappa_1) = q_n(\kappa_2) \left(1 - \frac{r_n(\kappa_2)}{q_n(\kappa_2)} - \frac{u_n(\kappa_2)}{q_n(\kappa_2)} \right). \quad (170)$$

Note that

$$q_n(\kappa_2) \geq \frac{n''}{4\tilde{E}_n} \log \left(1 + \lambda(1 - \lambda\rho)\frac{\tilde{E}_n}{n''} \right), \quad 1 \leq \kappa_2 \leq v_n. \quad (171)$$

Furthermore,

$$\begin{aligned} \frac{r_n(\kappa_2)}{q_n(\kappa_2)} &= \frac{\frac{(1-\rho)}{2\tilde{E}_n} \log(1 + \lambda\kappa_2\tilde{E}_n/n'')}{\frac{n''}{4\tilde{E}_n} \log \left(1 + \lambda(1 - \lambda\rho)\kappa_2\tilde{E}_n/n'' \right)} \\ &\leq \frac{\frac{(1-\rho)}{2\tilde{E}_n} \log(1 + \lambda v_n \tilde{E}_n/n'')}{\frac{n''}{4\tilde{E}_n} \log \left(1 + \lambda(1 - \lambda\rho)\tilde{E}_n/n'' \right)} \\ &= \frac{\frac{(1-\rho)v_n \log(1 + \lambda v_n \tilde{E}_n/n'')}{2n''}}{\frac{\tilde{E}_n v_n/n''}{\log(1 + \lambda(1 - \lambda\rho)\tilde{E}_n/n'')}}}, \quad 1 \leq \kappa_2 \leq v_n. \end{aligned} \quad (172)$$

Finally,

$$\begin{aligned} & \frac{u_n(\kappa_2)}{q_n(\kappa_2)} \\ &= \frac{4\rho\ell_n H_2(\kappa_2/\ell_n)}{n'' \log\left(1 + \lambda(1 - \lambda\rho)\kappa_2 \tilde{E}_n/n''\right)} \\ &= \frac{4\rho[\kappa_2 \log(\ell_n/\kappa_2) + \ell_n(\kappa_2/\ell_n - 1) \log(1 - \kappa_2/\ell_n)]}{n'' \log\left(1 + \lambda(1 - \lambda\rho)\kappa_2 \tilde{E}_n/n''\right)} \\ &\leq \frac{4\rho[\kappa_2 \log(\ell_n/\kappa_2) + \kappa_2 \log e]}{n'' \log\left(1 + \lambda(1 - \lambda\rho)\kappa_2 \tilde{E}_n/n''\right)} \\ &\leq \frac{4\rho v_n [\log \ell_n + \log e]}{n'' \log\left(1 + \lambda(1 - \lambda\rho)v_n \tilde{E}_n/n''\right)} \quad (173) \end{aligned}$$

$$= \frac{4\rho [\log \ell_n + \log e]}{\tilde{E}_n \frac{\log(1 + \lambda(1 - \lambda\rho)v_n \tilde{E}_n/n'')}{v_n \tilde{E}_n/n''}}, \quad 1 \leq \kappa_2 \leq v_n \quad (174)$$

where the first inequality follows from (156). Combining (171)–(174) with (170) yields the lower bound

$$\begin{aligned} b_{\lambda,\rho}^n(\kappa_2) &\geq \frac{n''}{4\tilde{E}_n} \log\left(1 + \lambda(1 - \lambda\rho)\tilde{E}_n/n''\right) \\ &\times \left(1 - \frac{\frac{(1-\rho)v_n}{2n''} \frac{\log\left(1 + \lambda \frac{v_n \tilde{E}_n}{n''}\right)}{\frac{v_n \tilde{E}_n}{n''}}}{\frac{\log\left(1 + \lambda(1 - \lambda\rho)\tilde{E}_n/n''\right)}{4\frac{\tilde{E}_n}{n''}}} - \frac{4\rho [\log \ell_n + \log e]}{\tilde{E}_n \frac{\log\left(1 + \lambda(1 - \lambda\rho)\frac{v_n \tilde{E}_n}{n''}\right)}{\frac{v_n \tilde{E}_n}{n''}}}\right) \quad (175) \end{aligned}$$

which is independent of κ_2 and \mathbf{d} .

To prove (166), we first note that, since $k_n = \Omega(1)$, we have $v_n \geq 1 - \lambda\rho$ for c'' sufficiently large. Thus, by the monotonicity of $x \mapsto \frac{\log(1+x)}{x}$,

$$\frac{\frac{\log(1 + \lambda v_n \tilde{E}_n/n'')}{\tilde{E}_n v_n/n''}}{\frac{\log(1 + \lambda(1 - \lambda\rho)\tilde{E}_n/n'')}{\tilde{E}_n/n''}} \leq \frac{1}{1 - \lambda\rho}, \quad v_n \geq 1 - \lambda\rho. \quad (176)$$

Furthermore, the term

$$\frac{2(1 - \rho)v_n}{n''} = \frac{2(1 - \rho)k_n(1 + c'')}{bn} \quad (177)$$

vanishes as $n \rightarrow \infty$ since $k_n = o(n)$ by the lemma's assumption that $k_n \log \ell_n = O(n)$. Consequently, the RHS of (172) tends to zero as $n \rightarrow \infty$, hence

$$\begin{aligned} & \liminf_{n \rightarrow \infty} \min_{1 \leq \kappa_2 \leq v_n} b_{\lambda,\rho}^n(\kappa_2) \\ &\geq \lim_{n \rightarrow \infty} \frac{n''}{4\tilde{E}_n} \log\left(1 + \lambda(1 - \lambda\rho)\tilde{E}_n/n''\right) \\ &\times \left(1 - \limsup_{n \rightarrow \infty} \frac{4\rho [\log \ell_n + \log e]}{\tilde{E}_n \frac{\log(1 + \lambda(1 - \lambda\rho)v_n \tilde{E}_n/n'')}{v_n \tilde{E}_n/n''}}\right). \quad (178) \end{aligned}$$

To show that the RHS of (178) is positive, we consider the following two cases:

Case 1— $k_n \log \ell_n = o(n)$: Recall that, in this case, $\tilde{E}_n = bc_n \ln \ell_n/2$ and $c_n \rightarrow \infty$ as $n \rightarrow \infty$. This implies that $\tilde{E}_n \rightarrow \infty$, $\frac{\log \ell_n}{\tilde{E}_n} \rightarrow 0$, and $v_n \tilde{E}_n/n'' \rightarrow 0$ as $n \rightarrow \infty$. It follows that the RHS of (174) vanishes as $n \rightarrow \infty$, so (178) becomes

$$\begin{aligned} & \liminf_{n \rightarrow \infty} \min_{1 \leq \kappa_2 \leq v_n} b_{\lambda,\rho}^n(\kappa_2) \\ &\geq \lim_{n \rightarrow \infty} \frac{n''}{4\tilde{E}_n} \log\left(1 + \lambda(1 - \lambda\rho)\tilde{E}_n/n''\right) \\ &= \frac{(\log e) \lambda(1 - \lambda\rho)}{4} \quad (179) \end{aligned}$$

which for $\lambda = 2/3$ and $\rho = 3/4$ is equal to $(\log e)/12$. Here, the last step follows by noting that $v_n \tilde{E}_n/n'' \rightarrow 0$ implies that $\tilde{E}_n/n'' \rightarrow 0$ since $v_n = \Omega(1)$.

Case 2— $k_n \log \ell_n = \Theta(n)$: We first note that, in this case, $4\rho v_n [\log \ell_n + \log e] = \Theta(n)$. Thus, there exist two positive constants a_3 and \tilde{n}_0''' such that

$$\frac{4\rho v_n [\log \ell_n + \log e]}{n''} \leq a_3, \quad n \geq \tilde{n}_0'''. \quad (180)$$

By the same arguments that yield (164), we can show that c' can be chosen sufficiently large so that, for some $\bar{n}_0 \geq \tilde{n}_0'''$,

$$\log\left(1 + \lambda\rho(1 - \lambda\rho)v_n \tilde{E}_n/n''\right) > a_3, \quad n \geq \bar{n}_0.$$

For such a c' , the RHS of (173) is strictly less than one. Consequently, the expression inside the large parentheses on the RHS of (178) is bounded away from zero for $n \geq \bar{n}_0$. Furthermore, as noted in the proof of (146), when $k_n \log \ell_n = \Theta(n)$, the expression $\frac{n''}{4\tilde{E}_n} \log(1 + \lambda\rho(1 - \lambda\rho)\tilde{E}_n/n'')$ is bounded away from zero for sufficiently large n . It follows that

$$\liminf_{n \rightarrow \infty} \min_{1 \leq \kappa_2 \leq v_n} b_{\lambda,\rho}^n(\kappa_2) > 0 \quad (180)$$

which concludes the analysis of the second case.

The claim (147) follows now by combining the above two cases, i.e., (179) and (180).

3) *Proof of (148):* We use (150), (159), and (175) to lower-bound

$$\begin{aligned} & g_{\lambda,\rho}^n(\kappa_1, \kappa_2, \mathbf{d}) \\ &\geq \frac{n''}{4\tilde{E}_n} \log\left(1 + \lambda\rho(1 - \lambda\rho)\tilde{E}_n/n''\right) \\ &\times \left(1 - \frac{4 \log v_n + 4 \log e}{\tilde{E}_n \frac{\log(1 + \lambda\rho(1 - \lambda\rho)v_n \tilde{E}_n/n'')}{v_n \tilde{E}_n/n''}}\right) \\ &+ \frac{n''}{4\tilde{E}_n} \log\left(1 + \lambda(1 - \lambda\rho)\tilde{E}_n/n''\right) \\ &\times \left(1 - \frac{\frac{(1-\rho)v_n}{2n''} \frac{\log(1 + \lambda v_n \tilde{E}_n/n'')}{\tilde{E}_n v_n/n''}}{\frac{\log(1 + \lambda(1 - \lambda\rho)\tilde{E}_n/n'')}{4\tilde{E}_n/n''}} - \frac{4\rho [\log \ell_n + \log e]}{\tilde{E}_n \frac{\log(1 + \lambda(1 - \lambda\rho)v_n \tilde{E}_n/n'')}{v_n \tilde{E}_n/n''}}\right) \end{aligned}$$

which is independent of κ_1, κ_2 , and \mathbf{d} . Consequently,

$$\liminf_{n \rightarrow \infty} \min_{\mathbf{d} \in \mathcal{B}^n(v_n)} \min_{\substack{1 \leq \kappa_1 \leq v_n \\ 1 \leq \kappa_2 \leq v_n}} g_{\lambda, \rho}^n(\kappa_1, \kappa_2, \mathbf{d}) \geq \underline{a} + \underline{b}$$

where

$$\underline{a} \triangleq \liminf_{n \rightarrow \infty} \left\{ \frac{n''}{4\tilde{E}_n} \log \left(1 + \lambda \rho (1 - \lambda \rho) \tilde{E}_n / n'' \right) \times \left(1 - \frac{4 \log v_n + 4 \log e}{\tilde{E}_n \frac{\log(1 + \lambda \rho (1 - \lambda \rho) v_n \tilde{E}_n / n'')}{v_n \tilde{E}_n / n''}} \right) \right\}$$

and

$$\underline{b} \triangleq \liminf_{n \rightarrow \infty} \left\{ \frac{n''}{4\tilde{E}_n} \log \left(1 + \lambda (1 - \lambda \rho) \tilde{E}_n / n'' \right) \times \left(1 - \frac{\frac{(1-\rho)v_n \log(1 + \lambda v_n \tilde{E}_n / n'')}{2n''} \frac{\tilde{E}_n v_n / n''}{\log(1 + \lambda (1 - \lambda \rho) \tilde{E}_n / n'')}}{4\tilde{E}_n / n''} - \frac{4\rho [\log \ell_n + \log e]}{\tilde{E}_n \frac{\log(1 + \lambda (1 - \lambda \rho) v_n \tilde{E}_n / n'')}{v_n \tilde{E}_n / n''}} \right) \right\}.$$

It was shown in the proof of (146) that $\underline{a} > 0$, and in the proof of (147) that $\underline{b} > 0$. The claim (148) thus follows.

Since (146)–(148) prove Lemma 14, this concludes the proof.

APPENDIX IV PROOF OF LEMMA 12

Let \mathcal{W} denote the set of the $(M_n + 1)^{\ell_n}$ messages of all users. To prove Lemma 12, we represent each $\mathbf{w} \in \mathcal{W}$ using a length- ℓ_n vector such that the i -th position of the vector is set to j if user i has message j . The Hamming distance d_H between two messages $\mathbf{w} = (w_1, \dots, w_{\ell_n})$ and $\mathbf{w}' = (w'_1, \dots, w'_{\ell_n})$ is defined as the number of positions at which \mathbf{w} differs from \mathbf{w}' , i.e., $d_H(\mathbf{w}, \mathbf{w}') \triangleq |\{i : w_i \neq w'_i\}|$.

We first group the set \mathcal{W} into $\ell_n + 1$ subgroups. Two messages $\mathbf{w}, \mathbf{w}' \in \mathcal{W}$ belong to the same subgroup if they have the same number of zeros. Note that all the messages in a subgroup have the same probability, since the probability of a message \mathbf{w} is determined by the number of zeros in it.

Let \mathcal{T}_t denote the set of messages $\mathbf{w} \in \mathcal{W}$ with t non-zero entries, where $t = 0, \dots, \ell_n$. Further let

$$\Pr(\mathcal{T}_t) \triangleq \Pr(\mathbf{W} \in \mathcal{T}_t)$$

which can be evaluated as

$$\Pr(\mathcal{T}_t) = (1 - \alpha_n)^{\ell_n - t} \left(\frac{\alpha_n}{M_n} \right)^t |\mathcal{T}_t|. \quad (181)$$

We define

$$P_e(\mathcal{T}_t) \triangleq \frac{1}{|\mathcal{T}_t|} \sum_{\mathbf{w} \in \mathcal{T}_t} P_e(\mathbf{w}) \quad (182)$$

where $P_e(\mathbf{w})$ denotes the probability of error in decoding the set of messages $\mathbf{w} = (w_1, \dots, w_{\ell_n})$. It follows that

$$\begin{aligned} P_e^{(n)} &= \sum_{\mathbf{w} \in \mathcal{W}} \Pr(\mathbf{W} = \mathbf{w}) P_e(\mathbf{w}) \\ &= \sum_{t=0}^{\ell_n} \sum_{\mathbf{w} \in \mathcal{T}_t} (1 - \alpha_n)^{\ell_n - t} \left(\frac{\alpha_n}{M_n} \right)^t |\mathcal{T}_t| \frac{1}{|\mathcal{T}_t|} P_e(\mathbf{w}) \\ &= \sum_{t=0}^{\ell_n} \Pr(\mathcal{T}_t) \frac{1}{|\mathcal{T}_t|} \sum_{\mathbf{w} \in \mathcal{T}_t} P_e(\mathbf{w}) \\ &= \sum_{t=0}^{\ell_n} \Pr(\mathcal{T}_t) P_e(\mathcal{T}_t) \\ &\geq \sum_{t=1}^{\ell_n} \Pr(\mathcal{T}_t) P_e(\mathcal{T}_t) \end{aligned} \quad (183)$$

where we have used the definitions of $\Pr(\mathcal{T}_t)$ and $P_e(\mathcal{T}_t)$ in (181) and (182), respectively. To prove Lemma 12, we next show that

$$P_e(\mathcal{T}_t) \geq 1 - \frac{256E_n/N_0 + \log 2}{\log \ell_n}, \quad t = 1, \dots, \ell_n. \quad (184)$$

To this end, we partition each $\mathcal{T}_t, t = 1, \dots, \ell_n$ into D_t sets \mathcal{S}_d^t . For every $t = 1, \dots, \ell_n$, we then show that this partition satisfies

$$\frac{1}{|\mathcal{S}_d^t|} \sum_{\mathbf{w} \in \mathcal{S}_d^t} P_e(\mathbf{w}) \geq 1 - \frac{256E_n/N_0 + \log 2}{\log \ell_n}. \quad (185)$$

This yields (184) since

$$P_e(\mathcal{T}_t) = \sum_{d=1}^{D_t} \frac{|\mathcal{S}_d^t|}{|\mathcal{T}_t|} \frac{1}{|\mathcal{S}_d^t|} \sum_{\mathbf{w} \in \mathcal{S}_d^t} P_e(\mathbf{w}). \quad (186)$$

Before we continue by defining the sets \mathcal{S}_d^t , we note that

$$M_n \geq 2 \quad (187)$$

since $M_n = 1$ would contradict the lemma's first assumption that $\dot{R} > 0$. We further have that

$$\ell_n \geq 5 \quad (188)$$

by the lemma's second assumption.

We next define a partition of $\mathcal{T}_t, t = 1, \dots, \ell_n$ that satisfies the following:

$$|\mathcal{S}_d^t| \geq \ell_n + 1, \quad d = 1, \dots, D_t \quad (189)$$

and

$$d_H(\mathbf{w}, \mathbf{w}') \leq 8, \quad \mathbf{w}, \mathbf{w}' \in \mathcal{S}_d^t. \quad (190)$$

To this end, we consider the following four cases:

Case 1— $t = 1$: For $t = 1$, we do not partition the set, i.e., $\mathcal{S}_1^1 = \mathcal{T}_1$. Thus, we have $|\mathcal{S}_1^1| = \ell_n M_n$. From (187) and (188), it follows that $|\mathcal{S}_1^1| \geq \ell_n + 1$. Since any two messages $\mathbf{w}, \mathbf{w}' \in \mathcal{T}_1$ have only one non-zero entry, we further have that $d_H(\mathbf{w}, \mathbf{w}') \leq 2$. Consequently, (189) and (190) are satisfied.

Case 2— $t = 2, \dots, \ell_n - 2$: In this case, we obtain a partition by finding a code \mathcal{C}_t in \mathcal{T}_t that has minimum Hamming distance 5, and for every $\mathbf{w} \in \mathcal{T}_t$, there exists at least one codeword in \mathcal{C}_t which is at most at Hamming distance 4 from it. Such a code exists because, if for some $\mathbf{w} \in \mathcal{T}_t$ all codewords were at Hamming distance 5 or more, then we could add \mathbf{w} to \mathcal{C}_t without affecting its minimum distance. Thus, for all $\mathbf{w} \notin \mathcal{C}_t$, there exists at least one index j such that $d_H(\mathbf{w}, \mathbf{c}_t(j)) \leq 4$, where $\mathbf{c}_t(1), \dots, \mathbf{c}_t(|\mathcal{C}_t|)$ denote the codewords of \mathcal{C}_t . With this code \mathcal{C}_t , we partition \mathcal{T}_t into the sets \mathcal{S}_d^t , $d = 1, \dots, D_t$ with $D_t = |\mathcal{C}_t|$ using the following procedure:

- 1) For a given $d = 1, \dots, D_t$, we assign $\mathbf{c}_t(d)$ to \mathcal{S}_d^t as well as all $\mathbf{w} \in \mathcal{T}_t$ that satisfy $d_H(\mathbf{w}, \mathbf{c}_t(d)) \leq 2$. These assignments are unique since the code \mathcal{C}_t has minimum Hamming distance 5.
- 2) We then consider all $\mathbf{w} \in \mathcal{T}_t$ for which there is no codeword $\mathbf{c}_t(1), \dots, \mathbf{c}_t(|\mathcal{C}_t|)$ satisfying $d_H(\mathbf{w}, \mathbf{c}_t(d)) \leq 2$ and assign them to the set \mathcal{S}_d^t with index

$$d = \min\{j = 1, \dots, D_t : d_H(\mathbf{w}, \mathbf{c}_t(j)) \leq 4\}.$$

Like this, we obtain a partition of \mathcal{T}_t . Since any two $\mathbf{w}, \mathbf{w}' \in \mathcal{S}_d^t$ are at most at a Hamming distance 4 from the codeword $\mathbf{c}_t(d)$, we have that $d_H(\mathbf{w}, \mathbf{w}') \leq 8$. Consequently, (190) is satisfied.

To show that (189) is satisfied, too, we use the following fact:

For two natural numbers a and b ,
if $a \geq 4$ and $2 \leq b \leq a - 2$, then $b(a - b) \geq a$. (191)

This fact follows since $b(a - b)$ is increasing in b from $b = 2$ to $b = \lfloor a/2 \rfloor$ and is decreasing in b from $b = \lfloor a/2 \rfloor$ to $b = a - 2$. So $b(a - b)$ is minimized at $b = 2$ and $b = a - 2$, where it has the value $2a - 4$. For $a \geq 4$, this value is greater than or equal to a , hence the claim follows.

Applying (191) with $a = \ell_n$ and $b = t$, we obtain that, if $|\mathcal{S}_d^t| \geq 1 + t(\ell_n - t)$, then $|\mathcal{S}_d^t| \geq 1 + \ell_n$. It thus remains to show that $|\mathcal{S}_d^t| \geq 1 + t(\ell_n - t)$. To this end, for every codeword $\mathbf{c}_t(d)$, consider all sequences in \mathcal{T}_t that differ exactly in one non-zero position and in one zero position from $\mathbf{c}_t(d)$. There are $t(\ell_n - t)M_n$ such sequences in \mathcal{T}_t which, by (187), can be lower-bounded as

$$t(\ell_n - t)M_n \geq t(\ell_n - t). \quad (192)$$

Since the codeword $\mathbf{c}_t(d)$ also belongs to \mathcal{S}_d^t , it follows that

$$|\mathcal{S}_d^t| \geq \ell_n + 1.$$

Consequently, (189) is satisfied.

Case 3— $t = \ell_n - 1$: We obtain a partition by defining a code \mathcal{C}_t in $\mathcal{T}_{\ell_n - 1}$ that has the same properties as the code used for Case 2. We then use the same procedure as in Case 2 to assign messages in $\mathbf{w} \in \mathcal{T}_{\ell_n - 1}$ to the sets \mathcal{S}_d^t , $d = 1, \dots, D_t$. This gives a partition of $\mathcal{T}_{\ell_n - 1}$ where any two $\mathbf{w}, \mathbf{w}' \in \mathcal{S}_d^t$ satisfy $d_H(\mathbf{w}, \mathbf{w}') \leq 8$. Consequently, this partition satisfies (190).

We next show that this partition also satisfies (189). To this end, for every codeword $\mathbf{c}_t(d)$, consider all the sequences that differ exactly in two non-zero positions from $\mathbf{c}_t(d)$. There are

$\binom{\ell_n - 1}{2}(M_n - 1)^2$ such sequences in $\mathcal{T}_{\ell_n - 1}$. Since \mathcal{S}_d^t also contains the codeword $\mathbf{c}_t(d)$, we obtain that

$$\begin{aligned} |\mathcal{S}_d^t| &\geq 1 + \binom{\ell_n - 1}{2}(M_n - 1)^2 \\ &\geq 1 + \binom{\ell_n - 1}{2} \\ &\geq 1 + \ell_n \end{aligned}$$

by (187) and (188).

Case 4— $t = \ell_n$: We obtain a partition by defining a code \mathcal{C}_t in \mathcal{T}_{ℓ_n} that has the same properties as the code used in Case 2. We then use the same procedure as in Case 2 to assign messages in $\mathbf{w} \in \mathcal{T}_t$ to the sets \mathcal{S}_d^t , $d = 1, \dots, D_t$. This gives a partition of \mathcal{T}_t where any two $\mathbf{w}, \mathbf{w}' \in \mathcal{S}_d^t$ satisfy $d_H(\mathbf{w}, \mathbf{w}') \leq 8$. Consequently, this partition satisfies (190).

We next show that this partition also satisfies (189). To this end, for every codeword $\mathbf{c}_t(d)$, consider all sequences that are at Hamming distance 1 from $\mathbf{c}_t(d)$. There are $\ell_n(M_n - 1)$ such sequences. Since \mathcal{S}_d^t also contains $\mathbf{c}_t(d)$, we have

$$\begin{aligned} |\mathcal{S}_d^t| &\geq 1 + \ell_n(M_n - 1) \\ &\geq 1 + \ell_n \end{aligned}$$

by (187).

Having obtained a partition of \mathcal{T}_t that satisfies (189) and (190), we next derive the lower bound (185). To this end, we use a stronger form of Fano's inequality sometimes known as Birgé's inequality.

Lemma 15 (Birgé's inequality [23]): Let $(\mathcal{Y}, \mathcal{B})$ be a measurable space with a σ -field, and let P_1, \dots, P_N be probability measures on \mathcal{B} , where $N \geq 2$. Consider an estimator δ of the measures defined on \mathcal{Y} , and denote by \mathcal{A}_i the event that the estimator's guess $\delta(Y)$ is P_i . Then

$$\frac{1}{N} \sum_{i=1}^N P_i(\mathcal{A}_i) \leq \frac{\frac{1}{N^2} \sum_{i,j} D(P_i \| P_j) + \log 2}{\log(N - 1)}.$$

Proof: See [24] and references therein. ■

To apply Lemma 15 to the problem at hand, we set $N = |\mathcal{S}_d^t|$ and $P_j = P_{\mathbf{Y}|\mathbf{X}}(\cdot|\mathbf{x}(j))$, where $\mathbf{x}(j)$ denotes the set of codewords transmitted to convey the set of messages $j \in \mathcal{S}_d^t$. We further define \mathcal{A}_j as the subset of \mathcal{Y}^n for which the decoder declares the set of messages $j \in \mathcal{S}_d^t$. Then, the probability of error in decoding messages $j \in \mathcal{S}_d^t$ is given by $P_e(j) = 1 - P_j(\mathcal{A}_j)$, and $\frac{1}{|\mathcal{S}_d^t|} \sum_{j \in \mathcal{S}_d^t} P_j(\mathcal{A}_j)$ denotes the average probability of correctly decoding a set of messages in \mathcal{S}_d^t .

For two multivariate Gaussian distributions $\mathbf{Z}_1 \sim \mathcal{N}(\boldsymbol{\mu}_1, \frac{N_0}{2} I)$ and $\mathbf{Z}_2 \sim \mathcal{N}(\boldsymbol{\mu}_2, \frac{N_0}{2} I)$ (where I denotes the identity matrix), the relative entropy $D(\mathbf{Z}_1 \| \mathbf{Z}_2)$ is given by $\frac{\|\boldsymbol{\mu}_1 - \boldsymbol{\mu}_2\|^2}{N_0}$. We next note that $P_{\mathbf{w}} = \mathcal{N}(\bar{\mathbf{x}}(\mathbf{w}), \frac{N_0}{2} I)$ and $P_{\mathbf{w}'} = \mathcal{N}(\bar{\mathbf{x}}(\mathbf{w}'), \frac{N_0}{2} I)$, where $\bar{\mathbf{x}}(j)$ denotes the sum of codewords contained in $\mathbf{x}(j)$. By construction, any two messages $\mathbf{w}, \mathbf{w}' \in \mathcal{S}_d^t$ are at a Hamming distance of at most

8. Without loss of generality, let us assume that $w_j = w'_j$ for $j = 9, \dots, \ell_n$. Then

$$\begin{aligned} \left\| \sum_{j=1}^{\ell_n} \mathbf{x}_j(w_j) - \sum_{i=1}^{\ell_n} \mathbf{x}_j(w'_i) \right\|^2 &= \left\| \sum_{i=1}^8 \mathbf{x}_j(w_j) - \mathbf{x}_j(w'_i) \right\|^2 \\ &\leq \left\| \sum_{j=1}^8 |\mathbf{x}_j(w_j) - \mathbf{x}_j(w'_j)| \right\|^2 \\ &\leq (8 \times 2\sqrt{E_n})^2 \\ &= 256E_n \end{aligned}$$

where we have used the triangle inequality and that the energy of a codeword for any user is upper-bounded by E_n . Thus, $D(P_{\mathbf{w}} \| P_{\mathbf{w}'}) \leq 256E_n/N_0$.

It follows from Lemma 15 that

$$\begin{aligned} \frac{1}{|\mathcal{S}_d^t|} \sum_{\mathbf{w} \in \mathcal{S}_d^t} P_e(\mathbf{w}) &\geq 1 - \frac{256E_n/N_0 + \log 2}{\log(|\mathcal{S}_d^t| - 1)} \\ &\geq 1 - \frac{256E_n/N_0 + \log 2}{\log \ell_n} \end{aligned} \quad (193)$$

where the last step holds because $|\mathcal{S}_d^t| - 1 \geq \ell_n$. This proves (185) and hence also (184).

Combining (184) and (183), we obtain

$$\begin{aligned} P_e^{(n)} &\geq \left(1 - \frac{256E_n/N_0 + \log 2}{\log \ell_n}\right) \sum_{i=1}^{\ell_n} \Pr(\mathcal{T}_i) \\ &= \left(1 - \frac{256E_n/N_0 + \log 2}{\log \ell_n}\right) (1 - \Pr(\mathcal{T}_0)). \end{aligned}$$

The probability $\Pr(\mathcal{T}_0) = \left((1 - \alpha_n)^{\frac{1}{\alpha_n}}\right)^{k_n}$ is upper-bounded by e^{-k_n} so, by the lemma's assumption $k_n = \Omega(1)$,

$$\limsup_{n \rightarrow \infty} \Pr(\mathcal{T}_0) < 1.$$

Consequently, $P_e^{(n)}$ may tend to zero as $n \rightarrow \infty$ only if

$$E_n = \Omega(\log \ell_n).$$

This proves Lemma 12.

ACKNOWLEDGMENT

The authors wish to thank the Associate Editor A. Anastopoulos and the anonymous referees for their valuable comments.

REFERENCES

- [1] X. Chen, T. Y. Chen, and D. Guo, "Capacity of Gaussian many-access channels," *IEEE Transactions on Information Theory*, vol. 63, no. 6, pp. 3516–3539, June 2017.
- [2] L. Liu, E. G. Larsson, W. Yu, P. Popovski, C. Stefanovic, and E. de Carvalho, "Sparse signal processing for grant-free massive connectivity: A future paradigm for random access protocols in the internet of things," *IEEE Signal Processing Magazine*, vol. 35, no. 5, pp. 88–99, September 2018.
- [3] S. Shahi, D. Tuninetti, and N. Devroye, "The strongly asynchronous massive access channel," *arXiv: 1807.09934 [cs.IT]*, July 2018.
- [4] Y. Polyanskiy, "A perspective on massive random-access," in *IEEE International Symposium on Information Theory (ISIT)*, Aachen, Germany, June 2017, pp. 2523–2527.

- [5] O. Ordentlich and Y. Polyanskiy, "Low complexity schemes for the random access gaussian channel," in *2017 IEEE International Symposium on Information Theory (ISIT)*, Aachen, Germany, June 2017, pp. 2528–2532.
- [6] A. Vem, K. R. Narayanan, J. Chamberland, and J. Cheng, "A user-independent successive interference cancellation based coding scheme for the unsourced random access Gaussian channel," *IEEE Transactions on Communications*, vol. 67, no. 12, pp. 8258–8272, December 2019.
- [7] V. K. Amalladinne, J. F. Chamberland, and K. R. Narayanan, "A coded compressed sensing scheme for unsourced multiple access," *IEEE Transactions on Information Theory*, vol. 66, no. 10, pp. 6509–6533, October 2020.
- [8] A. Fengler, P. Jung, and G. Caire, "SPARCs for unsourced random access," *IEEE Transactions on Information Theory*, vol. 67, no. 10, pp. 6894–6915, October 2021.
- [9] A. Fengler, P. Jung, and G. Caire, "Unsourced multiuser sparse regression codes achieve the symmetric MAC capacity," in *2020 IEEE International Symposium on Information Theory (ISIT)*, Los Angeles, USA, June 2020, pp. 3001–3006.
- [10] S. S. Kowshik and Y. Polyanskiy, "Quasi-static fading MAC with many users and finite payload," in *IEEE International Symposium on Information Theory (ISIT)*, Paris, France, July 2019, pp. 440–444.
- [11] —, "Fundamental limits of many-user MAC with finite payloads and fading," *IEEE Transactions on Information Theory*, vol. 67, no. 9, pp. 5853–5884, September 2021.
- [12] S. S. Kowshik, K. Andreev, A. Frolov, and Y. Polyanskiy, "Energy efficient coded random access for the wireless uplink," *IEEE Transactions on Communications*, vol. 68, no. 8, pp. 4694–4708, August 2020.
- [13] I. Zadik, Y. Polyanskiy, and C. Thrampoulidis, "Improved bounds on Gaussian MAC and sparse regression via Gaussian inequalities," in *IEEE International Symposium on Information Theory (ISIT)*, Paris, France, July 2019, pp. 430–434.
- [14] S. Verdú, "On channel capacity per unit cost," *IEEE Transactions on Information Theory*, vol. 36, no. 5, pp. 1019–1030, September 1990.
- [15] C. E. Shannon, R. G. Gallager, and E. R. Berlekamp, "Lower bounds to error probability for coding on discrete memoryless channels I," *Information and Control*, vol. 10, pp. 65–103, January 1967.
- [16] A. J. Viterbi and J. K. Omura, *Principles of Digital Communication and Coding*, 1st ed. New York, NY, USA: McGraw-Hill Book Company, 1979.
- [17] Y. Polyanskiy, "Information theoretic perspective on massive multiple-access," <http://people.lids.mit.edu/yp/homepage/data/NASIT18-MAC-tutorial.pdf>, June 2018.
- [18] R. G. Gallager, *Information Theory and Reliable Communication*, 1st ed. New York, NY, USA: John Wiley & Sons, 1968.
- [19] T. Cover and J. Thomas, *Elements of Information Theory*, 2nd ed. New York, NY, USA: Wiley-Interscience, 2006.
- [20] Y. Polyanskiy, H. V. Poor, and S. Verdú, "Minimum energy to send k bits through the Gaussian channel with and without feedback," *IEEE Transactions on Information Theory*, vol. 57, no. 8, pp. 4880–4902, August 2011.
- [21] R. Gallager, "A perspective on multiaccess channels," *IEEE Transactions on Information Theory*, vol. 31, no. 2, pp. 124–142, March 1985.
- [22] A. Lapidoth, *A Foundation in Digital Communication*, 2nd ed. Cambridge, UK: Cambridge University Press, 2017.
- [23] L. Birgé, "Approximation dans les espaces métriques et théorie de l'estimation," *Zeitschrift für Wahrscheinlichkeitstheorie und Verwandte Gebiete*, vol. 65, pp. 181–237, December 1983.
- [24] Y. G. Yatrocos, "A lower bound on the error in nonparametric regression type problems," *The Annals of Statistics*, vol. 16, no. 3, pp. 1180–1187, September 1988.

Jithin Ravi (Member, IEEE) received the B.Tech. degree in electronics and communication from the University of Kerala, Thiruvananthapuram, India, in 2006, and the M.Tech+Ph.D. dual degree in Electrical Engineering from the Indian Institute of Technology Bombay, Mumbai, India in 2017. From 2006 to 2008, he worked as a software engineer for Infosys Technologies Limited. He was a Postdoctoral Researcher at Tata Institute of Fundamental Research, Mumbai, India, in 2017. He is currently a Postdoctoral Researcher at the Signal Theory and Communications Department, Universidad Carlos III de Madrid, Leganés, Spain. His research interests include information theory, wireless communications, information-theoretic security and network coding.

Tobias Koch (Senior Member, IEEE) is an Associate Professor with the Signal Theory and Communications Department of Universidad Carlos III de Madrid (UC3M). He received the M.Sc. degree in electrical engineering (with distinction) in 2004 and the Ph.D. degree in electrical engineering in 2009, both from ETH Zurich, Switzerland. From June 2010 until May 2012 he was a Marie Curie Intra-European Research Fellow with the University of Cambridge, UK. He was also a research intern at Bell Labs, Murray Hill, NJ, USA, in 2004, and the Universitat Pompeu Fabra (UPF), Barcelona, Spain, in 2007. He joined the Signal Processing Group of UC3M in June 2012.

Dr. Koch received a Starting Grant from the European Research Council (ERC), a Ramón y Cajal Research Fellowship, a Marie Curie Intra-European Fellowship, a Marie Curie Career Integration Grant, and a Fellowship for Prospective Researchers from the Swiss National Science Foundation. He further received a medal of the 2018 Young Researchers Award "Agustín de Betancourt y Molina" by the Real Academia de Ingeniería. He served as Vice Chair of the Spain Chapter of the IEEE Information Theory Society from 2013–2016, and he is serving as the chapter's Chair in 2020–2023. Since 2020, he is also serving as Associate Editor for Communications for the IEEE TRANSACTIONS ON INFORMATION THEORY. His research interests are in digital communication theory and information theory.