

Minimum Energy per Bit of Unsourced Multiple Access with Location-Based Codebook Partitioning

Deekshith Pathayappilly Krishnan*, Kaan Okumus*, Khac-Hoang Ngo†, and Giuseppe Durisi*

*Department of Electrical Engineering, Chalmers University of Technology, 41296 Gothenburg, Sweden

†Department of Electrical Engineering, Linköping University, 58183 Linköping, Sweden

Email: {deepat, okumus}@chalmers.se, khac-hoang.ngo@liu.se, durisi@chalmers.se

Abstract—We derive finite-blocklength bounds on the minimum achievable energy per bit over a Gaussian unsourced multiple access (UMA) channel in the presence of heterogeneous path-loss conditions. We consider a setting in which the path loss is known to the users, which enables the use of location-based codebook partitioning [Çakmak et al., 2025]. Through numerical simulations and a large-system analysis based on the replica method, we quantify the performance gain of this strategy relative to the conventional UMA approach in which all users employ a common codebook.

I. INTRODUCTION

Massive machine-type communication (mMTC) is a rapidly growing use-case in wireless networks due to the fast expansion of Internet of Things (IoT) systems. mMTC is characterized by sporadic, uplink-centered transmissions of short packets from a high density of devices often operating under stringent energy-efficiency requirements [1]. As first formalized in [2], the mMTC problem has unique features, which makes it different from the traditional multiple access channel (MAC). One key difference is that, to capture the massiveness of the user population, it is fundamental to assume that it is impossible for the system to assign to each user a different codebook. The resulting scenario, in which all users are equipped with the same codebook, is commonly referred to in the literature as unsourced multiple-access (UMA).

Finite-blocklength bounds on the minimum energy per bit for the Gaussian UMA scenario were first obtained in [2], under the assumption that all users are received at the same power. These bounds have been recently improved and generalized to different scenarios, including the case in which the number of active users is random and unknown to the receiver [3] and the case in which transmission occurs over a quasi-static multiple-input multiple-output (MIMO) fading channel [4]. See [5] for a recent review of the area. Furthermore, coding schemes approaching these bounds have been designed. A particularly promising approach [6]–[9] leverages the similarity of UMA decoding and sparse signal recovery and relies on approximate message passing (AMP) for message recovery. This strategy, however, incurs a challenge when applied to realistic channel models in which signals from different users are received at different average-power levels because of path-loss effects. Indeed, since in UMA it is, in general, not possible to establish any association between the position of a user (and, hence, its path loss) and the codeword the user will transmit, one is forced

to use at the AMP denoiser a *diffuse* prior, which involves an averaging over all possible user positions.

This problem has been recently sidestepped in [10] via the insightful observation that, in most cellular wireless networks, an estimate of the path loss between users and base-stations can be obtained at the users via the downlink control information transmitted by the cellular base stations. This information can be used in a UMA system as follows: in the system-design phase, one quantizes the possible path loss values using a pre-determined number Q of levels; then, one partitions the codebook in Q subcodebooks. In the operational phase, each user estimates its path loss, quantizes it, and uses the corresponding subcodebook to transmit its message. This strategy, referred in [10] as *location-based codebook partitioning*, allows one to establish a link between transmitted codewords and path loss, and results in a much more concentrated prior for the AMP denoiser. As shown in [10] both theoretically and experimentally, this yields better AMP decoder performance.

Contributions: The purpose of this paper is to assess the effectiveness of location-based codebook partitioning via finite-blocklength information-theoretic bounds similar to the ones developed in [2]. For simplicity, we restrict our attention to a toy-model version of the scenario considered in [10]. Specifically, we assume that the channel between each user and a single-antenna receiver is modeled as a nonfading Gaussian channel, with (deterministic) path loss that can take only two different values, which we denote by g_1 and g_2 , respectively.

For this setup, we derive finite-blocklength bounds on the minimum energy per bit achievable when the codebook is partitioned into two subcodebooks and each user selects the subcodebook corresponding to its path loss. Furthermore, we compare this achievability bound with those obtained when all users select codewords from the same codebook, and when the decoder employs successive interference cancellation. Through numerical results, we show that the bound on the minimum energy per bit achieved via location-based codebook partitioning lies below the two alternative bounds. We also present simulation results obtained by combining the coded compressive sensing (CCS) coding scheme proposed in [8] with the multisource-AMP decoder introduced in [10]. These results exhibit a similar performance ordering.

To provide insights into the benefits of location-based codebook partitioning, we finally present a large-system characterization of the per-user probability of error (PUPE) via

replica analysis [11], in the regime where both the number of users and the blocklength grow to infinity with a fixed ratio. This (non-rigorous) large-system analysis reveals that, with location-based codebook partitioning, the UMA large-system performance can be characterized by analyzing two equivalent scalar Gaussian channels with SNR proportional to g_1^2 and g_2^2 , respectively. On the contrary, when a single codebook is used, the relevant scalar channel is a fading channel, with instantaneous fading value (not known to the receiver), taking value in $\{g_1, g_2\}$ with probability depending on the asymptotic fraction of users experiencing path loss g_1 and g_2 , respectively.

Notation: We denote system parameters by uppercase non-italic letters, e.g., K . Uppercase italic letters, e.g., X , denote scalar random variables and their realizations are in lowercase, e.g., x . We also use Greek letters to denote random variables when appropriate; such choices are stated explicitly. Vectors are denoted likewise in boldface, e.g., a random vector \mathbf{X} and its realization \mathbf{x} . We denote their i th entries as $[X]_i$ and $[x]_i$. We use a script font for random matrices, e.g., \mathcal{C} , and a sans-serif font for deterministic matrices, e.g., \mathbf{C} . We denote the $n \times n$ identity matrix by \mathbf{I}_n , and the all-zero vector by $\mathbf{0}$. The superscript T stands for transposition. We denote sets with calligraphic letters, e.g., \mathcal{S} , the set of integers $\{m, \dots, n\}$, $m \leq n$, as $[m : n]$, the set $[1 : n]$ as $[n]$, and the set of all size- k subsets of \mathcal{A} by $\binom{\mathcal{A}}{k}$. We denote the set of natural numbers by \mathbb{N} and the set of reals by \mathbb{R} . We denote the real-valued Gaussian vector distribution with mean μ and covariance matrix \mathbf{A} by $\mathcal{N}(\mu, \mathbf{A})$, and the Bernoulli distribution with parameter p by $\text{Ber}(p)$. We denote convergence in distribution by \xrightarrow{D} . Finally, $x^+ = \max\{0, x\}$; \otimes denotes the Kronecker product; $\mathbb{1}\{\cdot\}$ is the indicator function; $\text{diag}(x_1, \dots, x_n)$ denotes the diagonal matrix with (x_1, \dots, x_n) as the diagonal.

II. SYSTEM MODEL

We consider a stationary memoryless Gaussian UMA scenario, in which K_a users transmit their messages to a receiver over N channel uses. The users are assumed to be clustered according to their path loss. Specifically, users within the same cluster ℓ experience the same path loss g_ℓ . For simplicity, we consider the case of 2 clusters. Our results can however be readily generalized to an arbitrary finite number of clusters. We focus on the impact of heterogeneous path loss, and do not model small-scale fading. Let $\mathbf{X}_{\ell,k} \in \mathbb{R}^N$ be the signal transmitted by the k th user in cluster ℓ . The received signal is

$$\mathbf{Y} = g_1 \sum_{k=1}^{K_{a1}} \mathbf{X}_{1,k} + g_2 \sum_{k=1}^{K_{a2}} \mathbf{X}_{2,k} + \mathbf{Z} \quad (1)$$

where K_{a1} and K_{a2} , with $K_{a1} + K_{a2} = K_a$, are the number of active users that belong to clusters 1 and 2, respectively, and $\mathbf{Z} \sim \mathcal{N}(\mathbf{0}, \mathbf{I}_N)$ is the Gaussian noise, which is independent of the transmitted signals. We consider the power constraint $\|\mathbf{X}_{\ell,k}\|^2 \leq NP$ for all ℓ and k . We also assume that K_a, K_{a1} , and K_{a2} are fixed and known to the receiver. Finally, we assume that each user has perfect knowledge of its path loss. As already pointed out, this information can be obtained in practical

systems via the downlink control information transmitted by cellular base stations.

For this channel, an (M, N, P, ϵ) UMA code with codebook size M and codeword length N consists of

- two encoding functions $f_\ell : [M] \rightarrow \mathbb{R}^N$, $\ell \in \{1, 2\}$, that produce the transmitted codeword $\mathbf{X}_{\ell,k} = f_\ell(W_k)$, satisfying the power constraint, of user k in cluster ℓ , for a user message W_k uniformly distributed over $[M]$;
- a decoding function $g : \mathbb{R}^N \rightarrow \binom{[M]}{K_a}$ that provides an estimate $\widehat{\mathcal{W}} = \{\widehat{W}_1, \dots, \widehat{W}_{|\widehat{\mathcal{W}}|}\} = g(\mathbf{Y})$ of the list of transmitted messages.

The decoding function satisfies the following constraint on the PUPE:

$$P_e = \frac{1}{|\widehat{\mathcal{W}}|} \sum_{i=1}^{|\widehat{\mathcal{W}}|} \mathbb{P}[\widehat{W}_i \notin \widehat{\mathcal{W}}] \leq \epsilon, \quad (2)$$

where $\widehat{\mathcal{W}} = \{\widehat{W}_1, \dots, \widehat{W}_{|\widehat{\mathcal{W}}|}\}$ denotes the set of distinct elements of $\mathcal{W} = \{W_1, \dots, W_{K_a}\}$. In (2), we use the convention $0/0 = 0$ to circumvent the case $|\widehat{\mathcal{W}}| = 0$.

The main difference between the definition of UMA coding scheme just provided and the one originally provided in [2] is that we allow the encoder to depend on the cluster. This allows us to model location-based codebook partitioning.

III. RANDOM CODING BOUND

In this section, we first derive a random-coding achievability bound on the PUPE achievable over the channel (1) that exploits location-based codebook partitioning. Then, we provide in Section III-B two bounds for the case in which $f_1 = f_2$, which we refer to as common codebook case. The first bound relies on joint decoding, whereas the second bound relies on interference cancellation.

A. Location-Based Codebook Partitioning

We assume that the codewords of each of the two codebooks $\mathcal{C}_\ell = \{\mathbf{C}_{\ell,m}\}_{m=1}^M$, $\ell \in \{1, 2\}$ are drawn independently (across both ℓ and m) from a $\mathcal{N}(\mathbf{0}, P' \mathbf{I}_N)$ distribution, for a fixed $P' < P$. To convey message W_k , an active user k in cluster ℓ transmits \mathbf{C}_{ℓ,W_k} , provided that $\|\mathbf{C}_{\ell,W_k}\|^2 \leq NP$. Otherwise, the user transmits the all-zero codeword. That is,

$$f_\ell(W_k) = \mathbf{C}_{\ell,W_k} \mathbb{1}\{\|\mathbf{C}_{\ell,W_k}\|^2 \leq NP\}. \quad (3)$$

We consider a joint decoder, whose output is the set of estimated messages $\widehat{\mathcal{W}} = \widehat{\mathcal{W}}_1 \cup \widehat{\mathcal{W}}_2$, where

$$(\widehat{\mathcal{W}}_1, \widehat{\mathcal{W}}_2) = \arg \min_{\substack{\mathcal{W}'_1, \mathcal{W}'_2 \subset [M]: \\ |\mathcal{W}'_1| = K_{a1}, |\mathcal{W}'_2| = K_{a2}}} \|\mathbf{Y} - g_1 c_1(\mathcal{W}'_1) - g_2 c_2(\mathcal{W}'_2)\| \quad (4)$$

with $c_\ell(\mathcal{W}') = \sum_{w \in \mathcal{W}'} \mathbf{C}_{\ell,w}$, $\ell \in \{1, 2\}$.

An error analysis of this random-coding scheme yields the following achievability bound.

Theorem 1 (Random-coding bound, location-based codebook partitioning, joint decoding). *Fix $P' < P$. For the Gaussian*

UMA channel (1) there exists an (M, N, P, ϵ) random-access code for which

$$\epsilon \leq \sum_{t=0}^{K_a} \frac{t}{K_a} p_t + p_0 \quad (5)$$

where

$$p_0 = 1 - \frac{M!}{M^{K_a} (M - K_a)!} + K_a \frac{\Gamma(\frac{N}{2}, \frac{NP}{2P'})}{\Gamma(N/2)}, \quad (6)$$

$$p_t = \sum_{t_{MD1} \in \mathcal{T}_t} \sum_{t_{FP1} \in \mathcal{T}_t} \sum_{t_{AC1} \in \mathcal{T}'_{t, t_{MD1}, t_{FP1}}} \exp(-NE(t, t_{MD1}, t_{FP1}, t_{AC1})), \quad (7)$$

$$\begin{aligned} E(t, t_{MD1}, t_{FP1}, t_{AC1}) &= \max_{\rho_1, \rho_2, \rho_3 \in [0, 1]} -\rho_1 \rho_2 \rho_3 (R_1 + R_2) \\ &\quad - \rho_2 \rho_3 (R_3 + R_4) - \rho_3 (R_5 + R_6) \\ &\quad + E_0(\rho_1, \rho_2, \rho_3), \end{aligned}$$

$$R_1 = \frac{1}{N} \ln \left(\frac{K_{a1} - t_{MD1}}{t_{AC1}} \right),$$

$$R_2 = \frac{1}{N} \ln \left(\frac{K_{a2} - t + t_{MD1}}{t_{AC1} + t_{MD1} - t_{FP1}} \right),$$

$$R_3 = \frac{1}{N} \ln \left(\frac{M - K_a}{t_{FP1}} \right),$$

$$R_4 = \frac{1}{N} \ln \left(\frac{M - K_a - t_{FP1}}{t - t_{FP1}} \right),$$

$$R_5 = \frac{1}{N} \ln \left(\frac{K_{a1}}{t_{MD1}} \right),$$

$$R_6 = \frac{1}{N} \ln \left(\frac{K_{a2}}{t - t_{MD1}} \right),$$

$$E_0(\rho_1, \rho_2, \rho_3) = \max_{\lambda} \rho_3 \rho_2 a_1 + \rho_3 a_2 + \frac{1}{2} \ln(1 - 2\rho_3 b), \quad (15)$$

$$a_1 = \frac{\rho_1}{2} \ln(1 + 2\lambda \kappa_{AC} P') + \frac{1}{2} \ln(1 + 2\mu_1 \kappa_{FP} P'), \quad (16)$$

$$a_2 = \frac{1}{2} \ln(1 + 2\mu_2 \kappa_{MD} P'), \quad (17)$$

$$b = \lambda \rho_1 \rho_2 - \frac{\mu_2}{1 + 2\mu_2 \kappa_{MD} P'}, \quad (18)$$

$$\mu_1 = \frac{\lambda \rho_1}{1 + 2\lambda \kappa_{AC} P'}, \quad (19)$$

$$\mu_2 = \frac{\mu_1 \rho_2}{1 + 2\mu_1 \kappa_{FP} P'}, \quad (20)$$

$$\kappa_{AC} = (g_1^2 + g_2^2)(2t_{AC1} + t_{MD1} - t_{FP1}), \quad (21)$$

$$\kappa_{MD} = g_1^2 t_{MD1} + g_2^2 (t - t_{MD1}), \quad (22)$$

$$\kappa_{FP} = g_1^2 t_{FP1} + g_2^2 (t - t_{FP1}), \quad (23)$$

$$\mathcal{T}_t = [(t - K_{a2})^+ : \min\{t, K_{a1}\}], \quad (24)$$

$$\mathcal{T}'_{t, t_{MD1}, t_{FP1}} = [\max\{0, t_{FP1} - t_{MD1}\} : \min\{K_{a1} - t_{MD1}, K_{a2} - t + t_{FP1}\}]. \quad (25)$$

Proof. The proof follows similar steps as the proof of [2, Th. 1], namely, a change of measure and a Gallager-type

error exponent analysis that makes use of Chernoff bound, Gallager's ρ -trick, and Gaussian statistics. One fundamental difference compared to [2] is that the decoder, when analyzing codewords received at power Pg_2^2 , may put out a set of messages, which we denote by \mathcal{W}_{AC1} , that are false positives from the perspective of cluster 2, but happen to coincide with the messages from cluster 1, and vice versa. We refer to these messages as "accidentally correct" (AC) messages. Compared to [2], this results in an additional union bound over $t_{AC1} = |\mathcal{W}_{AC1}|$ (see (7)). See Appendix B for details. \square

B. Common Codebook

We now consider the common codebook case $\mathcal{C}_1 = \mathcal{C}_2 = \{C_1, \dots, C_M\}$.

1) *Joint Decoding:* We first obtain a bound for the case of joint decoding.

Corollary 1 (Random-coding bound, common codebook, joint decoding). *Fix $P' < P$. For the Gaussian UMA channel (1), there exists an (M, N, P, ϵ) random-access code for which ϵ is bounded as in (5) with (21) replaced by*

$$\kappa_{AC} = (g_1 - g_2)^2 (2t_{AC1} + t_{MD1} - t_{FP1}). \quad (26)$$

Proof. The proof follows along the same lines as the proof of Theorem 1, with the fundamental difference that the assumption of common codebook causes an increase in κ_{AC} , which represents the variance of a term related to the accidentally corrected messages. See Appendix C. \square

2) *Interference-Cancellation Decoding:* Assume without loss of generality that $g_1 \geq g_2$. We now consider an interference-cancellation decoder that operates by first decoding messages from cluster 1 as

$$\widehat{\mathcal{W}}_1 = \arg \min_{\mathcal{W}'_1 \subset [M] : |\mathcal{W}'_1| = K_{a1}} \|\mathbf{Y} - g_1 c(\mathcal{W}'_1)\| \quad (27)$$

with $c(\mathcal{W}) = \sum_{w \in \mathcal{W}} \mathbf{C}_w$, and then canceling the interference from cluster 1 to decode messages coming from cluster 2 as

$$\widehat{\mathcal{W}}_2 = \arg \min_{\mathcal{W}'_2 \subset [M] \setminus \widehat{\mathcal{W}}_1 : |\mathcal{W}'_2| = K_{a2}} \|\mathbf{Y} - g_1 c(\widehat{\mathcal{W}}_1) - g_2 c(\mathcal{W}'_2)\|. \quad (28)$$

We state a random-coding bound for this strategy in the following theorem.

Theorem 2 (Random-coding bound, common codebooks, interference-cancellation decoding). *Fix $P' < P$. For the Gaussian UMA channel (1), there exists an (M, N, P, ϵ) random-access code for which ϵ is bounded as in (5) with $E_0(\rho_1, \rho_2, \rho_3)$ replaced by*

$$\begin{aligned} E_0(\rho_1, \rho_2, \rho_3) &= \max_{\lambda_1, \lambda_2} \left(\frac{1}{2} \rho_1 \rho_2 \rho_3 \ln \det(\mathbf{I}_2 - 2\boldsymbol{\Sigma}_{AC} \mathbf{U}_{AC}) \right. \\ &\quad + \frac{1}{2} \rho_2 \rho_3 \ln \det(\mathbf{I}_2 - 2\boldsymbol{\Sigma}_{FP} \mathbf{U}_{FP}) \\ &\quad + \frac{1}{2} \rho_3 \ln \det(\mathbf{I}_2 - 2\boldsymbol{\Sigma}_{MD} \mathbf{U}_{MD}) \\ &\quad \left. + \frac{1}{2} \ln \det(\mathbf{I}_2 - 2\boldsymbol{\Sigma}_{ZC} \mathbf{U}_{ZC}) \right), \end{aligned} \quad (29)$$

$$\boldsymbol{\Sigma}_{AC} = \text{diag}(t_{AC1} P', (t_{AC1} + t_{MD1} - t_{FP1}) P'), \quad (30)$$

$$\begin{aligned}
\Sigma_{\text{FP}} &= \text{diag}(t_{\text{FP}1}\mathbf{P}', (t - t_{\text{FP}1})\mathbf{P}'), \\
\Sigma_{\text{MD}} &= \text{diag}(t_{\text{MD}1}\mathbf{P}', (t - t_{\text{MD}1})\mathbf{P}'), \\
\Sigma_{\text{ZC}} &= \text{diag}(1, (\mathbf{K}_{\text{a}2} - t + t_{\text{FP}1} - t_{\text{AC}1})\mathbf{P}'), \\
\mathbf{U}_{\text{AC}} &= \begin{bmatrix} u_{\text{AC}}^{(1)} & u_{\text{AC}}^{(2)} \\ u_{\text{AC}}^{(2)} & u_{\text{AC}}^{(3)} \end{bmatrix}, \\
u_{\text{AC}}^{(1)} &= -\lambda_1 g_1^2 - \lambda_2 g_2(g_2 - 2g_1), \\
u_{\text{AC}}^{(2)} &= \lambda_1 g_1(g_1 - g_2) + \lambda_2 g_2(g_2 - 2g_1), \\
u_{\text{AC}}^{(3)} &= -\lambda_1 g_1(g_1 - 2g_2) - \lambda_2 g_2(g_2 - 2g_1), \\
\mathbf{U}_{\text{FP}} &= 2\rho_1 \Lambda_{\text{FP}} \mathbf{Q}_{\text{FP}} - \rho_1 \begin{bmatrix} \lambda_1 g_1^2 & \lambda_2 g_1 g_2 \\ \lambda_2 g_1 g_2 & \lambda_2 g_2^2 \end{bmatrix}, \\
\mathbf{Q}_{\text{FP}} &= \begin{bmatrix} \lambda_1 g_1^2 - \lambda_2 g_1 g_2 & \lambda_2 g_2(g_1 - g_2) \\ -\lambda_1 g_1(g_1 - g_2) + \lambda_2 g_1 g_2 & -\lambda_2 g_2(g_1 - g_2) \end{bmatrix}, \\
\Lambda_{\text{FP}} &= \mathbf{Q}_{\text{FP}}^T (\Sigma_{\text{AC}}^{-1} - 2\mathbf{U}_{\text{AC}})^{-1}, \\
\mathbf{U}_{\text{MD}} &= 2\rho_2 \Lambda_{\text{MD}} \mathbf{Q}_{\text{MD}} + 2\rho_2 \rho_1 \Lambda_{\mathbf{M}} \mathbf{M} \\
&\quad - \rho_2 \rho_1 \begin{bmatrix} \lambda_1 g_1^2 & (\lambda_1 + \lambda_2) g_1 g_2 \\ (\lambda_1 + \lambda_2) g_1 g_2 & \lambda_2 g_2^2 \end{bmatrix}, \\
\mathbf{M} &= \lambda_1 g_1 g_2 \begin{bmatrix} 0 & -1 \\ 0 & 1 \end{bmatrix} - \mathbf{Q}_{\text{FP}}, \\
\mathbf{Q}_{\text{MD}} &= 2\rho_1 \Lambda_{\text{FP}} \mathbf{M} + \rho_1 \begin{bmatrix} \lambda_1 g_1^2 & (\lambda_1 + \lambda_2) g_1 g_2 \\ \lambda_2 g_1 g_2 & \lambda_2 g_2^2 \end{bmatrix}, \\
\Lambda_{\text{MD}} &= \mathbf{Q}_{\text{MD}}^T (\Sigma_{\text{FP}}^{-1} - 2\mathbf{U}_{\text{FP}})^{-1}, \\
\Lambda_{\mathbf{M}} &= \mathbf{M}^T (\Sigma_{\text{AC}}^{-1} - 2\mathbf{U}_{\text{AC}})^{-1}, \\
\mathbf{U}_{\text{ZC}} &= 2\rho_3 \mathbf{Q}_{\text{ZC}}^T (\Sigma_{\text{MD}}^{-1} - 2\mathbf{U}_{\text{MD}})^{-1} \mathbf{Q}_{\text{ZC}} \\
&\quad + 2\rho_3 \rho_2 \Lambda_{\text{ZCa}}^T (\Sigma_{\text{FP}}^{-1} - 2\mathbf{U}_{\text{FP}})^{-1} \Lambda_{\text{ZCa}} \\
&\quad + 4\rho_3 \rho_2 \rho_1 \Lambda_{\text{ZCb}}^T (\Sigma_{\text{AC}}^{-1} - 2\mathbf{U}_{\text{AC}})^{-1} \Lambda_{\text{ZCb}}, \\
\mathbf{Q}_{\text{ZC}} &= \rho_2 \rho_1 \left(-\mathbf{I}_2 + (4\Lambda_{\text{MD}} \Lambda_{\text{FP}} + 2\Lambda_{\mathbf{M}}) \begin{bmatrix} -1 & 1 \\ 1 & -1 \end{bmatrix} + 2\Lambda_{\text{MD}} \right) \\
&\quad \cdot \begin{bmatrix} \lambda_1 g_1 & \lambda_1 g_1 g_2 \\ \lambda_2 g_2 & 0 \end{bmatrix}, \\
\Lambda_{\text{ZCa}} &= \rho_1 \left(\mathbf{I}_2 + 2\Lambda_{\text{FP}} \begin{bmatrix} -1 & 1 \\ 1 & -1 \end{bmatrix} \right) \begin{bmatrix} \lambda_1 g_1 & \lambda_1 g_1 g_2 \\ \lambda_2 g_2 & 0 \end{bmatrix}, \\
\Lambda_{\text{ZCb}} &= \begin{bmatrix} -1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} \lambda_1 g_1 & \lambda_1 g_1 g_2 \\ \lambda_2 g_2 & 0 \end{bmatrix}.
\end{aligned}$$

Proof. The proof follows similar steps as the proof of Theorem 1, with some extensions to capture the sequential nature of the decoding operations (27) and (28). See Appendix D. \square

IV. REPLICA METHOD PREDICTION

To obtain insights on system performance, we provide next a large-system limit characterization of the PUPE achievable over the channel (1). To derive the result, we rely on the replica method, in line with its application to multiuser detection systems [12]–[14], and the original UMA problem [15].

To state the main results of this section, we first introduce the following definition of multiuser spectral efficiency.

Definition 1. Let

$$B = \sqrt{a}A + N, \quad (50)$$

with $a > 0$, $A \sim \text{Ber}(p)$, $p \in (0, 1)$, and $N \sim \mathcal{N}(0, 1)$. Let $I(a)$ denote the mutual information $I(A; B)$ and let G be a binary random variable taking values in $\{g_1, g_2\}$ with probability $\mathbb{P}[G = g_\ell] = \gamma_\ell$. Then, for every $\beta > 0$, the multiuser efficiency η is defined as

$$\eta = \arg \min_x (\beta \mathbb{E}_G[I(xPG^2)] + \frac{1}{2}(x - 1 - \ln x)). \quad (51)$$

A. Location-Based Codebook Partitioning

We describe the random codebook corresponding to cluster ℓ as a matrix \mathcal{C}_ℓ with M columns drawn independently from a $\mathcal{N}(\mathbf{0}, \mathbf{I}_N/N)$ distribution. For a fixed $\mu \in (0, 1)$, we consider the regime in which the total number of active users satisfies $K_a = \mu N$. In contrast to Section III, where each user independently selects a message uniformly at random yielding a message selection probability $1 - (1 - 1/M)^{K_a} \approx K_a/M$, we consider a setting in which, within each cluster ℓ with $K_{a\ell}$ active users, each message is selected independently according to a $\text{Ber}(K_{a\ell}/M)$ distribution. Let $\alpha_\ell = K_{a\ell}/K_a$ and $\beta = 2M/N$. Furthermore, let \mathbf{U}'_ℓ denote an $M \times 1$ vector with entries drawn independently from a $\text{Ber}(\alpha_\ell \mu / \beta)$ distribution, representing message selection in cluster ℓ . Let finally $\mathbf{Z}' \sim \mathcal{N}(\mathbf{0}, \mathbf{I}_N)$. We analyze the large-system performance of location-based codebook partitioning achievable over the channel

$$\mathbf{Y}' = \sqrt{P}g_1 \mathcal{C}_1 \mathbf{U}'_1 + \sqrt{P}g_2 \mathcal{C}_2 \mathbf{U}'_2 + \mathbf{Z}'. \quad (52)$$

We have the following result.

Claim 1 (Replica decoupling, location-based codebook partitioning). *Let $\ell \in \{1, 2\}$. Fix $p_\ell = \alpha_\ell \mu / \beta$, and $\gamma_\ell = 1/2$. Denote by*

$$V'_{\ell, N} = \mathbb{P}[[\mathbf{U}'_\ell]_1 = 1 \mid \mathbf{Y}', \mathcal{C}_1, \mathcal{C}_2] \quad (53)$$

the marginal posterior probability associated with (52). Consider also the following scalar channels for $\ell \in \{1, 2\}$:

$$B_\ell = \sqrt{P} \eta g_\ell A_\ell + N_\ell. \quad (54)$$

Here, $A_\ell \sim \text{Ber}(p_\ell \gamma_\ell)$, and $N_\ell \sim \mathcal{N}(0, 1)$, independent of A_ℓ . Let $M, N, K_a \rightarrow \infty$ with β, μ , and α_ℓ held constant. Then,

$$V'_{\ell, N} \xrightarrow{D} \mathbb{P}[A_\ell = 1 \mid B_\ell]. \quad (55)$$

Proof. The proof follows from [14, Prop. 1]. See for details. \square

Remark 1. *Claim 1 implies that, in the large-system limit, the channel (52) decouples into the two scalar channels in (54). Note in particular that the two scalar channels have deterministic path losses known to the receiver. Following an approach similar to the one detailed in [15], we can use these two scalar channels to obtain a large-system characterization of the PUPE. Specifically, let ϵ_ℓ be the solution of*

$$\sqrt{P} \eta g_\ell = Q^{-1}(\epsilon_\ell) + Q^{-1}(p_\ell \gamma_\ell \epsilon_\ell / (1 - p_\ell \gamma_\ell)). \quad (56)$$

In the large-system limit, the PUPE is given by $(\epsilon_1 + \epsilon_2)/2$.

B. Common Codebook

We denote the common codebook as a matrix \mathcal{C} with M columns drawn independently from a $\mathcal{N}(\mathbf{0}, \mathbf{I}_N/N)$ distribution. We let μ and α_ℓ to be defined as before, but set now $\beta = M/N$, and use a $\text{Ber}(K_a/M)$ distribution for message selection. Note that $K_a/M = \mu/\beta$. Let \mathbf{U}'' be the binary vector describing the message selection. Let also G be a random variable taking values in $\{g_1, g_2\}$ with $\mathbb{P}[G = g_\ell] = \alpha_\ell$. Finally, let $\mathbf{Z}'' \sim \mathcal{N}(\mathbf{0}, \mathbf{I}_N)$. We analyze the large-system performance achievable over the channel

$$\mathbf{Y}'' = \sqrt{P}G\mathcal{C}\mathbf{U}'' + \mathbf{Z}''. \quad (57)$$

We have the following result.

Claim 2 (Replica decoupling, common codebook). *Let $\ell \in \{1, 2\}$. Fix $p = \mu/\beta$, and $\gamma_\ell = \alpha_\ell$. Denote by*

$$V_N'' = \mathbb{P}[[\mathbf{U}'']_1 = 1 \mid \mathbf{Y}'', \mathcal{C}''], \quad (58)$$

the marginal posterior probability associated with (57). Consider the scalar channel

$$B'' = \sqrt{P\eta}GA'' + N''. \quad (59)$$

Here, $A'' \sim \text{Ber}(p)$, G takes values in $\{g_1, g_2\}$ with $\mathbb{P}[G = g_\ell] = \alpha_\ell$, and $N'' \sim \mathcal{N}(0, 1)$. Furthermore, these three random variables are mutually independent. Let $M, N, K_a \rightarrow \infty$ with β, μ , and α_ℓ held constant. Then,

$$V_N'' \xrightarrow{D} \mathbb{P}[A'' = 1 \mid B'']. \quad (60)$$

Proof. The proof follows from [13, Claim 1]. See for details. \square

Remark 2. Note that, in contrast to the previous case, the equivalent scalar channel in the common codebook case is a single fading channel, with fading coefficient G not known to the receiver. The large-system characterization of the PUPE for this scenario can again be carried out along the lines of [15]. However, the presence of G precludes a closed-form expression. Specifically, in the large-system limit, the PUPE is given by

$$\epsilon = \frac{1-p}{p} \mathbb{P}_1 \left[\ln \frac{d\mathbb{P}_0}{d\mathbb{P}_1} \geq \theta \right] \quad (61)$$

where θ is determined by imposing that

$$\mathbb{P}_0 \left[\ln \frac{d\mathbb{P}_0}{d\mathbb{P}_1} \geq \theta \right] + \frac{1-p}{p} \mathbb{P}_1 \left[\ln \frac{d\mathbb{P}_0}{d\mathbb{P}_1} \geq \theta \right] = 1. \quad (62)$$

Here, $\mathbb{P}_0 = \mathcal{N}(0, 1)$ and $\mathbb{P}_1 = \gamma_1 \mathcal{N}(g_1, 1) + \gamma_2 \mathcal{N}(g_2, 1)$.

V. NUMERICAL RESULTS

We evaluate the minimum energy per bit $NP/(2B)$ required to achieve a PUPE of 0.01 as a function of the number of active users K_a for the case in which each user map messages of $B = 128$ bits to codewords of length $N = 30\,000$. Throughout, we set $g_1 = 1$, $g_2 = 0.8$, and $K_{a2} = 2K_{a1}$. In Fig. 1, we depict

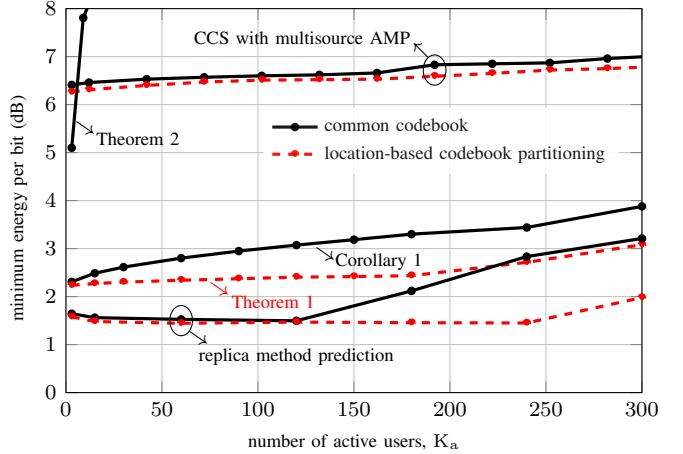


Fig. 1. Minimum energy per bit to achieve target PUPE of 0.01 vs. number of active users K_a .

the random-coding bound with location-based codebook partitioning in Theorem 1 as well as those corresponding to common codebook with joint decoding (Corollary 1) and common codebook with interference-cancellation decoding (Theorem 2). In the figure, we also depict the replica method predictions, obtained via the expressions given in Remark 1 and Remark 2. We also use the normalization with respect to the effective number of bits suggested in [15]. Finally, we provide simulation results for a CCS scheme [8] in which the decoder operates according to the multisource-AMP framework proposed in [10]. Specifically, in the resulting scheme, each message is divided into 16 blocks of 16 bits each. The CCS inner decoder performs multisource-AMP signal reconstruction, while the outer decoder stitches together the reconstructed signals, to ensure that they form valid codewords. To do so, we assume that the inner decoder produces a list of candidate messages of size $K_a + 10$.

As shown in the figure, for the channel model considered in the paper, location-based codeword partitioning results in a consistent reduction of the minimum energy per bit (although this reduction is marginal when K_a is small) across all types of curves depicted in the figure (random-coding bounds, replica-method predictions, performance of CCS schemes). Note also that, for the scenario considered in this section, i.e., $K_{a2} = 2K_{a1}$ with $g_2 < g_1$, interference cancellation exhibits poor performance (6 dB gap from the location-based codeword partitioning bound for $K_a = 12$).

VI. CONCLUSION

For a Gaussian UMA channel characterized by heterogeneous path loss, we showed that location-based codebook partitioning outperforms, in terms of the minimum energy per bit required to meet a specific PUPE, the conventional UMA framework, which utilizes a common codebook for all users. These gains were validated through finite-blocklength random coding bounds, replica method large-system limit predictions, and empirical performance of a coding scheme based on CCS and multisource-AMP.

We anticipate that the energy efficiency gains from location-based codebook partitioning will be even more pronounced in wireless network architectures featuring distributed access points (distributed MIMO). Indeed, in such systems, the access points are located so as to ensure uniform quality of service, which should amplify the benefit of the location-based codebook partitioning, as illustrated in [10] for the case of multisource-AMP decoders. Such extension, as well as the inclusion of small-scale fading will be considered in future works.

REFERENCES

- [1] A. E. Kalor, G. Durisi, S. Coleri, S. Parkvall, W. Yu, A. Mueller, and P. Popovski, "Wireless 6G connectivity for massive number of devices and critical services," *Proc. IEEE*, Nov. 2024.
- [2] Y. Polyanskiy, "A perspective on massive random-access," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Aachen, Germany, Jun. 2017, pp. 2523–2527.
- [3] K.-H. Ngo, A. Lancho, G. Durisi, and A. Graell i Amat, "Unsourced multiple access with random user activity," *IEEE Trans. Inf. Theory*, vol. 69, no. 7, pp. 4537–4558, Jul. 2023.
- [4] S. S. Kowshik, K. Andreev, A. Frolov, and Y. Polyanskiy, "Energy efficient coded random access for the wireless uplink," *IEEE Trans. Commun.*, vol. 68, no. 8, pp. 4694–4708, Jun. 2020.
- [5] K. Andreev, P. Rybin, and A. Frolov, "Unsourced random access," *Foundations and Trends® in Commun. and Inf. Theory*, vol. 22, no. 5–6, pp. 605–842, Aug. 2025.
- [6] A. Fengler, P. Jung, and G. Caire, "SPARCs for unsourced random access," *IEEE Trans. Inf. Theory*, vol. 67, no. 10, pp. 6894–6915, Oct. 2021.
- [7] V. K. Amalladinne, A. Vem, D. K. Soma, K. R. Narayanan, and J. Chamberland, "A coupled compressive sensing scheme for unsourced multiple access," in *Proc. IEEE Int. Conf. Acoustics, Speech and Signal Proc. (ICASSP)*, Calgary, AB, Canada, Apr. 2018, pp. 6628–6632.
- [8] V. K. Amalladinne, J. F. Chamberland, and K. R. Narayanan, "A coded compressed sensing scheme for unsourced multiple access," *IEEE Trans. Inf. Theory*, vol. 66, no. 10, pp. 6509–6533, Oct. 2020.
- [9] V. K. Amalladinne, A. K. Pradhan, C. Rush, J.-F. Chamberland, and K. R. Narayanan, "Unsourced random access with coded compressed sensing: Integrating AMP and belief propagation," *IEEE Trans. Inf. Theory*, vol. 68, no. 4, pp. 2384–2409, Apr. 2022.
- [10] B. Çakmak, E. Gkiouzepi, M. Opper, and G. Caire, "Joint message detection and channel estimation for unsourced random access in cell-free user-centric wireless networks," *IEEE Trans. Inf. Theory*, vol. 71, no. 5, pp. 3614–3643, May 2025.
- [11] S. F. Edwards and P. W. Anderson, "Theory of spin glasses," *Journal of Physics F: Metal Physics*, vol. 5, no. 5, p. 965, May 1975.
- [12] T. Tanaka, "A statistical-mechanics approach to large-system analysis of CDMA multiuser detectors," *IEEE Trans. Inf. Theory*, vol. 48, no. 11, pp. 2888–2910, Nov. 2002.
- [13] D. Guo and S. Verdú, "Randomly spread CDMA: Asymptotics via statistical physics," *IEEE Trans. Inf. Theory*, vol. 51, no. 6, pp. 1983–2010, Jun. 2005.
- [14] D. Guo, "Performance of synchronous multirate CDMA via statistical physics," in *Proc. Int. Symp. Inf. Theory (ISIT)*, Adelaide, SA, Australia, Sept. 2005, pp. 199–203.
- [15] Y. Polyanskiy, "Remarks on massive random access," 2020, DLR-MIT-TUM Workshop, Munich, Germany, Feb. 2020.
- [16] Y. Ohnishi and J. Honorio, "Novel change of measure inequalities with applications to PAC-Bayesian bounds and Monte Carlo estimation," in *Proc. Int. Conf. Artificial Intelligence and Statistics (AISTATS)*. Virtual Conference: PMLR, Apr. 2021, pp. 1711–1719.
- [17] M. H. DeGroot and M. J. Schervish, *Probability and Statistics*, 4th ed. Boston, MA, USA: Pearson, 2012.
- [18] R. G. Gallager, *Information theory and reliable communication*. New York, USA: Wiley, 1968.
- [19] Y. Kabashima, "Introduction to the replica method." [Online]. Available: https://ithems.riken.jp/download/file/18/Intro_RM_rev.pdf
- [20] A. Dembo and O. Zeitouni, *Large Deviations Techniques and Applications*, 2nd ed. Springer Berlin, Heidelberg, 2009.
- [21] P. Billingsley, *Probability and Measure*, 3rd ed. New York: Wiley, 1995.

APPENDIX A
MATHEMATICAL PRELIMINARIES FOR THE RANDOM
CODING BOUNDS

The following results will be used in the proofs of Theorems 1, and 2.

Lemma 1 (Change of measure [16, Lemma 4]). *Let p and q be two probability measures. Consider a random variable X supported on \mathcal{H} and a function $f: \mathcal{H} \rightarrow [0, 1]$. It holds that*

$$\mathbb{E}_p[f(X)] \leq \mathbb{E}_q[f(X)] + d_{\text{TV}}(p, q) \quad (63)$$

where $d_{\text{TV}}(p, q)$ denotes the total variation distance between p and q .

Lemma 2 (Chernoff bound [17, Th. 6.2.7]). *For a random variable X with moment-generating function $\mathbb{E}[e^{tX}]$ defined for all $|t| \leq b$, it holds for all $\lambda \in [0, b]$ that*

$$\mathbb{P}[X \leq x] \leq e^{\lambda x} \mathbb{E}[e^{-\lambda X}]. \quad (64)$$

Corollary 2 (Chernoff joint bound). *For two random variables X_1 and X_2 with joint moment-generating function $\mathbb{E}[e^{t_1 X_1 + t_2 X_2}]$ defined for all $|t_1| \leq b_1$ and $|t_2| \leq b_2$, it holds for all $\lambda_1 \in [0, b_1]$, $\lambda_2 \in [0, b_2]$ that*

$$\mathbb{P}[X_1 \leq x_1, X_2 \leq x_2] \leq e^{\lambda_1 x_1 + \lambda_2 x_2} \mathbb{E}[e^{-\lambda_1 X_1 - \lambda_2 X_2}]. \quad (65)$$

Lemma 3 (Gallager's ρ -trick [18, p. 136]). *It holds that $\mathbb{P}[\cup_i A_i] \leq (\sum_i \mathbb{P}[A_i])^\rho$ for every $\rho \in [0, 1]$.*

Lemma 4 (Moment-generating function of quadratic forms of a Gaussian vector). *Let $\mathbf{X} \in \mathbb{R}^N$ and $\mathbf{X} \sim \mathcal{N}(\boldsymbol{\mu}, \Sigma)$. Let $\mathbf{A} \in \mathbb{R}^{N \times N}$ be a symmetric matrix and $\mathbf{b} \in \mathbb{R}^N$. For every $\gamma \in \mathbb{R}$ such that $\Sigma^{-1} + 2\gamma\mathbf{A} \succ \mathbf{0}$, it holds that*

$$\begin{aligned} & \mathbb{E}[\exp(-\gamma(\mathbf{X}^T \mathbf{A} \mathbf{X} + 2\mathbf{b}^T \mathbf{X}))] \\ &= \det(\mathbf{I}_N + 2\gamma\Sigma\mathbf{A})^{-1/2} \\ & \cdot \exp(2\gamma^2(\mathbf{A}\boldsymbol{\mu} + \mathbf{b})^T(\Sigma^{-1} + 2\gamma\mathbf{A})^{-1}(\mathbf{A}\boldsymbol{\mu} + \mathbf{b}) \\ & \quad - \gamma(\boldsymbol{\mu}^T \mathbf{A} \boldsymbol{\mu} + 2\mathbf{b}^T \boldsymbol{\mu})). \end{aligned} \quad (66)$$

In particular, for $\gamma = -1$ and $\boldsymbol{\mu} = \mathbf{0}$, it holds that

$$\begin{aligned} & \mathbb{E}[\exp(\mathbf{X}^T \mathbf{A} \mathbf{X} + 2\mathbf{b}^T \mathbf{X})] \\ &= \det(\mathbf{I}_N - 2\Sigma\mathbf{A})^{-1/2} \exp(2\mathbf{b}^T(\Sigma^{-1} - 2\mathbf{A})^{-1}\mathbf{b}), \end{aligned} \quad (67)$$

given that $\Sigma^{-1} \succ 2\mathbf{A}$; for $\Sigma = \sigma^2 \mathbf{I}_N$, $\mathbf{A} = \mathbf{I}_N$, and $\mathbf{b} = \mathbf{0}$, it holds that

$$\mathbb{E}[e^{-\gamma\|\mathbf{X}\|^2}] = (1 + 2\gamma\sigma^2)^{-N/2} \exp\left(-\frac{\gamma\|\boldsymbol{\mu}\|^2}{1 + 2\gamma\sigma^2}\right), \quad (68)$$

for every $\gamma > -\frac{1}{2\sigma^2}$.

Proof. Denote the quadratic form as $Q = \mathbf{X}^T \mathbf{A} \mathbf{X} + 2\mathbf{b}^T \mathbf{X}$. Using the density of $\mathbf{X} \sim \mathcal{N}(\boldsymbol{\mu}, \Sigma)$, we compute $\mathbb{E}[e^{-\gamma Q}]$ as

$$\begin{aligned} \mathbb{E}[e^{-\gamma Q}] &= \frac{1}{(2\pi)^{N/2} \det(\Sigma)^{1/2}} \\ & \cdot \int_{\mathbb{R}^n} \exp\left(-\frac{1}{2}(\mathbf{x} - \boldsymbol{\mu})^T \Sigma^{-1} (\mathbf{x} - \boldsymbol{\mu}) - \gamma \mathbf{x}^T \mathbf{A} \mathbf{x} - 2\gamma \mathbf{b}^T \mathbf{x}\right) d\mathbf{x}. \end{aligned} \quad (69)$$

We define $\mathbf{K} = \Sigma^{-1} + 2\gamma\mathbf{A}$ and $\mathbf{h} = \Sigma^{-1}\boldsymbol{\mu} - 2\gamma\mathbf{b}$. Since Σ^{-1} and \mathbf{A} are symmetric, \mathbf{K} is symmetric. The exponent on the right-hand side of (69) becomes $-\frac{1}{2}\mathbf{x}^T \mathbf{K} \mathbf{x} + \mathbf{h}^T \mathbf{x} - \frac{1}{2}\boldsymbol{\mu}^T \Sigma^{-1} \boldsymbol{\mu}$. Hence,

$$\begin{aligned} \mathbb{E}[e^{-\gamma Q}] &= \frac{\exp\left(-\frac{1}{2}\boldsymbol{\mu}^T \Sigma^{-1} \boldsymbol{\mu}\right)}{(2\pi)^{n/2} \det(\Sigma)^{1/2}} \\ & \cdot \int_{\mathbb{R}^n} \exp\left(-\frac{1}{2}\mathbf{x}^T \mathbf{K} \mathbf{x} + \mathbf{h}^T \mathbf{x}\right) d\mathbf{x}. \end{aligned} \quad (70)$$

Under the condition that \mathbf{K} is positive definite, the standard Gaussian integral identity yields

$$\begin{aligned} & \int_{\mathbb{R}^n} \exp\left(-\frac{1}{2}\mathbf{x}^T \mathbf{K} \mathbf{x} + \mathbf{h}^T \mathbf{x}\right) d\mathbf{x} \\ &= (2\pi)^{n/2} \det(\mathbf{K})^{-1/2} \exp\left(\frac{1}{2}\mathbf{h}^T \mathbf{K}^{-1} \mathbf{h}\right). \end{aligned} \quad (71)$$

Substituting this into (70) gives

$$\begin{aligned} \mathbb{E}[e^{-\gamma Q}] &= \det(\Sigma)^{-1/2} \det(\mathbf{K})^{-1/2} \\ & \cdot \exp\left(-\frac{1}{2}\boldsymbol{\mu}^T \Sigma^{-1} \boldsymbol{\mu} + \frac{1}{2}\mathbf{h}^T \mathbf{K}^{-1} \mathbf{h}\right), \end{aligned} \quad (72)$$

which leads to (66) after some simplifications of the determinant and exponent terms. The particular cases (67) and (68) follow straightforwardly from (66). \square

APPENDIX B
PROOF OF THEOREM 1

We analyze the PUPE achieved with the random-coding scheme introduced in Section III-A, averaged over the Gaussian code ensemble. We denote by \mathcal{W}_ℓ the set of messages transmitted by users in cluster $\ell \in \{1, 2\}$, and define $(\widehat{\mathcal{W}}_1, \widehat{\mathcal{W}}_2)$ as in (4). Furthermore, we denote by \mathcal{W}_{MD} the set of misdetected messages, i.e., $\mathcal{W}_{\text{MD}} = \widehat{\mathcal{W}} \setminus \widetilde{\mathcal{W}}$, and by \mathcal{W}_{FP} the set of false-positive messages, i.e., $\mathcal{W}_{\text{FP}} = \widetilde{\mathcal{W}} \setminus \widehat{\mathcal{W}}$. The PUPE can be expressed as

$$P_e = \mathbb{E}\left[\frac{|\mathcal{W}_{\text{MD}}|}{|\widetilde{\mathcal{W}}|}\right]. \quad (73)$$

A. Change of Measure

We apply Lemma 1 to the random variable $\frac{|\mathcal{W}_{\text{MD}}|}{|\widetilde{\mathcal{W}}|}$ to replace the measure under which the expectation is taken by the one under which: i) the active users transmit distinct messages, i.e., $|\widetilde{\mathcal{W}}| = K_a$ and $\widetilde{W}_1, \dots, \widetilde{W}_{K_a}$ are sampled uniformly without replacement from $[M]$; ii) $\mathbf{X}_{\ell,k} = \mathbf{C}_{\ell,W_k}$, $\forall \ell, k$, instead of $\mathbf{X}_{\ell,k} = \mathbf{C}_{\ell,W_k} \mathbb{1}\{\|\mathbf{C}_{\ell,W_k}\| \leq NP\}$. The total variation between the original measure and the new one is upper-bounded by

$$\begin{aligned} & \mathbb{P}\left[|\widetilde{\mathcal{W}}| < K_a\right] + \mathbb{P}[\exists k \in [K_a]: \|\mathbf{C}_{\ell,W_k}\| \geq NP] \\ & \leq 1 - \frac{M!}{M^{K_a}(M - K_a)!} + K_a \frac{\Gamma(N/2, NP/(2P'))}{\Gamma(N/2)} \end{aligned} \quad (74)$$

$$= p_0. \quad (75)$$

The inequality (74) follows from the same analysis as in [3, App. A-A]. We consider implicitly the new measure hereafter

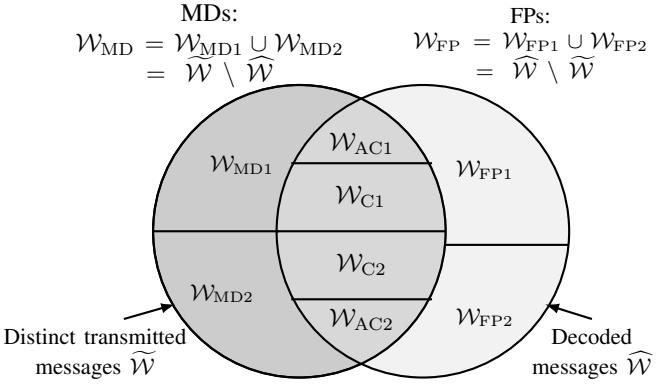


Fig. 2. A diagram depicting the relation between the sets of messages.

at a cost of adding p_0 to the original expectation in (73). Specifically, we expand this expectation as

$$P_e \leq \sum_{t=0}^{K_a} \frac{t}{K_a} \mathbb{P}[|\mathcal{W}_{MD}| = |\mathcal{W}_{FP}| = t] + p_0, \quad (76)$$

and next focus on upper-bounding $\mathbb{P}[|\mathcal{W}_{MD}| = |\mathcal{W}_{FP}| = t]$ under the new measure.

B. Message Sets

We further split the sets of misdetected messages, false-positive messages, and correctly decoded messages, as depicted in Fig. 2. We first split \mathcal{W}_{MD} into two sets \mathcal{W}_{MD1} and \mathcal{W}_{MD2} that contain the misdetected messages of users in clusters 1 and 2, respectively. Similarly, we split \mathcal{W}_{FP} into \mathcal{W}_{FP1} and \mathcal{W}_{FP2} . Recall that the decoded sets of messages for clusters 1 and 2 are $\widehat{\mathcal{W}}_1$ and $\widehat{\mathcal{W}}_2$, respectively. We denote $\mathcal{W}_{AC1} = \mathcal{W}_1 \cap \widehat{\mathcal{W}}_2$, which is the set of messages that are false positives from the perspective of cluster 2 but happen to coincide with messages transmitted by cluster 1. We refer to these messages as “accidentally correct” messages (hence the subscript AC). Similarly, we denote the set of accidentally correct messages for cluster 2 as $\mathcal{W}_{AC2} = \mathcal{W}_2 \cap \widehat{\mathcal{W}}_1$. Finally, we denote the sets of other correctly decoded messages as $\mathcal{W}_{C1} = \widehat{\mathcal{W}}_1 \setminus \mathcal{W}_{MD1} \setminus \mathcal{W}_{AC1}$ and $\mathcal{W}_{C2} = \widehat{\mathcal{W}}_2 \setminus \mathcal{W}_{MD2} \setminus \mathcal{W}_{AC2}$.

Exploiting symmetry, we assume without loss of generality that $\mathcal{W} = [K_a]$, $\mathcal{W}_1 = [K_{a1}]$, and thus $\mathcal{W}_2 = [K_{a1} + 1 : K_a]$. Denote the cardinality of the message sets as $t_{MD1} = |\mathcal{W}_{MD1}|$, $t_{FP1} = |\mathcal{W}_{FP1}|$, $t_{AC1} = |\mathcal{W}_{AC1}|$, and $t_{AC2} = |\mathcal{W}_{AC2}|$. Under the event $|\mathcal{W}_{MD}| = |\mathcal{W}_{FP}| = t$, we have that $|\mathcal{W}_{MD2}| = t - t_{MD1}$ and $|\mathcal{W}_{FP2}| = t - t_{FP1}$. As $\mathcal{W}_1 = \mathcal{W}_{C1} \cup \mathcal{W}_{AC1} \cup \mathcal{W}_{MD1}$, $\mathcal{W}_1 = \mathcal{W}_{C1} \cup \mathcal{W}_{AC2} \cup \mathcal{W}_{FP1}$, and $|\mathcal{W}_1| = |\widehat{\mathcal{W}}_1| = K_{a1}$, we obtain that

$$t_{FP1} + t_{AC2} = t_{MD1} + t_{AC1} = K_{a1} - t_{C1} \leq K_{a1}. \quad (77)$$

Similarly, we have that

$$t_{FP2} + t_{AC1} = t_{MD2} + t_{AC2} = K_{a2} - t_{C2} \leq K_{a2}. \quad (78)$$

Therefore, given t , t_{MD1} is upper-bounded by both t and K_{a1} , and lower-bounded as $t_{MD1} = t - t_{MD2} \geq t - K_{a2}$. That is,

t_{MD1} is bounded in \mathcal{T}_t defined in (24). Similarly, so is t_{FP1} . Furthermore, given t_{MD1} and t_{FP1} , t_{AC1} belongs to the set $\mathcal{T}'_{t,t_{MD1},t_{FP1}}$ defined in (25).

C. Pairwise Error Event

We express the received signal as

$$\begin{aligned} \mathbf{Y} &= g_1[c_1(\mathcal{W}_{MD1}) + c_1(\mathcal{W}_{AC1}) + c_1(\mathcal{W}_{C1})] \\ &\quad + g_2[c_2(\mathcal{W}_{MD2}) + c_2(\mathcal{W}_{AC2}) + c_2(\mathcal{W}_{C2})] + \mathbf{Z}. \end{aligned} \quad (79)$$

Furthermore, the sums of the codewords corresponding to the decoded message sets ($\widehat{\mathcal{W}}_1, \widehat{\mathcal{W}}_2$) are expressed as

$$c_1(\widehat{\mathcal{W}}_1) = c_1(\mathcal{W}_{FP1}) + c_1(\mathcal{W}_{AC2}) + c_1(\mathcal{W}_{C1}), \quad (80)$$

$$c_2(\widehat{\mathcal{W}}_2) = c_2(\mathcal{W}_{FP2}) + c_2(\mathcal{W}_{AC1}) + c_2(\mathcal{W}_{C2}). \quad (81)$$

The pairwise error event $\widehat{\mathcal{W}} \rightarrow \widehat{\mathcal{W}}$ occurs when

$$\|\mathbf{Y} - g_1 c_1(\widehat{\mathcal{W}}_1) - g_2 c_2(\widehat{\mathcal{W}}_2)\| < \|\mathbf{Z}\|. \quad (82)$$

Using (79), (80), and (81), we obtain that (82) is equivalent to

$$\begin{aligned} &\|\mathbf{Z} + g_1 c_1(\mathcal{W}_{MD1}) + g_2 c_2(\mathcal{W}_{MD2}) \\ &\quad - g_1 c_1(\mathcal{W}_{FP1}) - g_2 c_2(\mathcal{W}_{FP2}) \\ &\quad + g_1 c_1(\mathcal{W}_{AC1}) - g_2 c_2(\mathcal{W}_{AC1}) \\ &\quad - g_1 c_1(\mathcal{W}_{AC2}) + g_2 c_2(\mathcal{W}_{AC2})\| \leq \|\mathbf{Z}\|. \end{aligned} \quad (83)$$

We denote by $F(\mathcal{W}_{MD\ell}, \mathcal{W}_{FP\ell}, \mathcal{W}_{AC\ell}, \ell \in \{1, 2\})$ the set of $(\mathcal{W}_{MD\ell}, \mathcal{W}_{FP\ell}, \mathcal{W}_{AC\ell}, \ell \in \{1, 2\})$ such that (83) holds.

D. Error-Exponent Analysis

By writing the event $|\mathcal{W}_{MD}| = |\mathcal{W}_{FP}| = t$ as a union of the pairwise error events $F(\mathcal{W}_{MD\ell}, \mathcal{W}_{FP\ell}, \mathcal{W}_{AC\ell}, \ell \in \{1, 2\})$, we have that

$$\begin{aligned} &\mathbb{P}[|\mathcal{W}_{MD}| = |\mathcal{W}_{FP}| = t] \\ &= \mathbb{P} \left[\bigcup_{t_{MD1} \in \mathcal{T}_t} \bigcup_{t_{FP1} \in \mathcal{T}_t} \bigcup_{t_{AC1} \in \mathcal{T}'_{t,t_{MD1},t_{FP1}}} \right. \\ &\quad \bigcup_{\mathcal{W}_{MD1} \subset \binom{[K_{a1}]}{t_{MD1}}} \bigcup_{\mathcal{W}_{MD2} \subset \binom{[K_{a1}+1:K_a]}{t-t_{MD1}}} \\ &\quad \bigcup_{\mathcal{W}_{FP1} \subset \binom{[K_{a1}+1:M]}{t_{FP1}}} \bigcup_{\mathcal{W}_{FP2} \subset \binom{[K_{a1}+1:M] \setminus \mathcal{W}_{FP1}}{t-t_{FP1}}} \\ &\quad \bigcup_{\mathcal{W}_{AC1} \subset \binom{[K_{a1}]\setminus \mathcal{W}_{MD1}}{t_{AC1}}} \bigcup_{\mathcal{W}_{AC2} \subset \binom{[K_{a1}+1:K_a]\setminus \mathcal{W}_{MD2}}{t_{AC1}+t_{MD1}-t_{FP1}}} \\ &\quad \left. F(\mathcal{W}_{MD\ell}, \mathcal{W}_{FP\ell}, \mathcal{W}_{AC\ell}, \ell \in \{1, 2\}) \right] \\ &\leq \sum_{t_{MD1} \in \mathcal{T}_t} \sum_{t_{FP1} \in \mathcal{T}_t} \sum_{t_{AC1} \in \mathcal{T}'_{t,t_{MD1},t_{FP1}}} \\ &\quad \mathbb{P} \left[\bigcup_{\mathcal{W}_{MD1} \subset \binom{[K_{a1}]}{t_{MD1}}} \bigcup_{\mathcal{W}_{MD2} \subset \binom{[K_{a1}+1:K_a]}{t-t_{MD1}}} \right. \\ &\quad \bigcup_{\mathcal{W}_{FP1} \subset \binom{[K_{a1}+1:M]}{t_{FP1}}} \bigcup_{\mathcal{W}_{FP2} \subset \binom{[K_{a1}+1:M] \setminus \mathcal{W}_{FP1}}{t-t_{FP1}}} \\ &\quad \left. \mathcal{W}_{AC1} \subset \binom{[K_{a1}]\setminus \mathcal{W}_{MD1}}{t_{AC1}} \mathcal{W}_{AC2} \subset \binom{[K_{a1}+1:K_a]\setminus \mathcal{W}_{MD2}}{t_{AC1}+t_{MD1}-t_{FP1}} \right. \\ &\quad \left. F(\mathcal{W}_{MD\ell}, \mathcal{W}_{FP\ell}, \mathcal{W}_{AC\ell}, \ell \in \{1, 2\}) \right] \end{aligned} \quad (84)$$

$$F(\mathcal{W}_{MD\ell}, \mathcal{W}_{FP\ell}, \mathcal{W}_{AC\ell}, \ell \in \{1, 2\}) \Big]. \quad (85)$$

Given $c_\ell(\mathcal{W}_{MD\ell})$, $c_\ell(\mathcal{W}_{FP\ell})$, $\ell \in \{1, 2\}$, and Z , it holds for every $\lambda > 0$ that

$$\begin{aligned} & \mathbb{P}[F(\mathcal{W}_{MD\ell}, \mathcal{W}_{FP\ell}, \mathcal{W}_{AC\ell}, \ell \in \{1, 2\})] \\ & \leq \exp(\lambda \|Z\|^2) \mathbb{E}_{\mathcal{W}_{AC1}, \mathcal{W}_{AC2}} [\exp(-\lambda \|Z\|^2 \\ & \quad + g_1 c_1(\mathcal{W}_{MD1}) + g_2 c_2(\mathcal{W}_{MD2}) \\ & \quad - g_1 c_1(\mathcal{W}_{FP1}) - g_2 c_2(\mathcal{W}_{FP2}) + g_1 c_1(\mathcal{W}_{AC1}) \\ & \quad - g_2 c_2(\mathcal{W}_{AC1}) - g_1 c_1(\mathcal{W}_{AC2}) + g_2 c_2(\mathcal{W}_{AC2})\|)^2)] \quad (86) \\ & = \exp(\lambda \|Z\|^2)(1 + 2\lambda(g_1^2 + g_2^2)(t_{AC1} + t_{AC2})P')^{-N/2} \\ & \quad \cdot \exp(-\lambda \|Z\|^2 + g_1 c_1(\mathcal{W}_{MD1}) + g_2 c_2(\mathcal{W}_{MD2}) \\ & \quad - g_1 c_1(\mathcal{W}_{FP1}) - g_2 c_2(\mathcal{W}_{FP2})\|)^2) \\ & \quad \cdot (1 + 2\lambda(g_1^2 + g_2^2)(t_{AC1} + t_{AC2})P')^{-1}), \quad (87) \end{aligned}$$

where we have applied the Chernoff bound in Lemma 2 in (86) and then used (66) in Lemma 4 to compute the expectation. Note that $(g_1^2 + g_2^2)(t_{AC1} + t_{AC2})$ is equal to κ_{AC} defined in (21). Next, we apply Gallager's ρ -trick in Lemma 3 to get that, given $c_\ell(\mathcal{W}_{MD\ell})$, $c_\ell(\mathcal{W}_{FP\ell})$, $\ell \in \{1, 2\}$, and Z , it holds for every $\rho_1 \in [0, 1]$ that

$$\begin{aligned} & \mathbb{P}\left[\bigcup_{\mathcal{W}_{AC1} \subset ([K_{a1}] \setminus \mathcal{W}_{MD1})} \bigcup_{\mathcal{W}_{AC2} \subset ([K_{a1+1:K_a}] \setminus \mathcal{W}_{MD2})} F(\mathcal{W}_{MD\ell}, \mathcal{W}_{FP\ell}, \mathcal{W}_{AC\ell}, \ell \in \{1, 2\})\right] \\ & \leq \binom{K_{a1} - t_{MD1}}{t_{AC1}}^{\rho_1} \binom{K_a - K_{a1} - t + t_{MD1}}{t_{AC1} + t_{MD1} - t_{FP1}}^{\rho_1} \\ & \quad \cdot (1 + 2\lambda\kappa_{AC}P')^{-N\rho_1/2} \\ & \quad \cdot \exp\left(\mu_1(\|Z\|^2 - \|Z + g_1 c_1(\mathcal{W}_{MD1}) + g_2 c_2(\mathcal{W}_{MD2})\|^2 - g_1 c_1(\mathcal{W}_{FP1}) - g_2 c_2(\mathcal{W}_{FP2})\|)\right) \end{aligned}$$

where μ_1 is defined by (19). By taking the expectation over \mathcal{W}_{FP1} and \mathcal{W}_{FP2} using (66) in Lemma 4, we obtain that, for given $c_\ell(\mathcal{W}_{MD\ell})$, $\ell \in \{1, 2\}$, and given Z ,

$$\begin{aligned} & \mathbb{P}\left[\bigcup_{\mathcal{W}_{AC1} \subset ([K_{a1}] \setminus \mathcal{W}_{MD1})} \bigcup_{\mathcal{W}_{AC2} \subset ([K_{a1+1:K_a}] \setminus \mathcal{W}_{MD2})} F(\mathcal{W}_{MD\ell}, \mathcal{W}_{FP\ell}, \mathcal{W}_{AC\ell}, \ell \in \{1, 2\})\right] \\ & \leq \binom{K_{a1} - t_{MD1}}{t_{AC1}}^{\rho_1} \binom{K_a - K_{a1} - t + t_{MD1}}{t_{AC1} + t_{MD1} - t_{FP1}}^{\rho_1} \\ & \quad \cdot \exp\left(\lambda\rho_1\|Z\|^2 - \mu_1\|Z + g_1 c_1(\mathcal{W}_{MD1}) + g_2 c_2(\mathcal{W}_{MD2})\|^2 - (1 + 2\mu_1(g_1^2 t_{FP1} + g_2^2 t_{FP2})P')^{-1} - Na_1\right) \quad (88) \end{aligned}$$

where

$$\begin{aligned} a_1 &= \frac{\rho_1}{2} \ln(1 + 2\lambda\kappa_{AC}P') \\ &+ \frac{1}{2} \ln(1 + 2\mu_1(g_1^2 t_{FP1} + g_2^2 t_{FP2})P'). \quad (89) \end{aligned}$$

Note that $g_1^2 t_{FP1} + g_2^2 t_{FP2}$ is equal to κ_{FP} defined in (23). Now we apply Gallager's ρ -trick again to obtain that, given $c_\ell(\mathcal{W}_{MD\ell})$, $c_\ell(\mathcal{W}_{FP\ell})$, $\ell \in \{1, 2\}$, given Z and for every $\rho_2 \in [0, 1]$,

$$\begin{aligned} & \mathbb{P}\left[\bigcup_{\mathcal{W}_{FP1} \subset ([K_{a1+1:M}] \setminus \mathcal{W}_{FP1})} \bigcup_{\mathcal{W}_{FP2} \subset ([K_{a+1:M}] \setminus \mathcal{W}_{FP2})} \bigcup_{\mathcal{W}_{AC1} \subset ([K_{a1}] \setminus \mathcal{W}_{MD1})} \bigcup_{\mathcal{W}_{AC2} \subset ([K_{a1+1:K_a}] \setminus \mathcal{W}_{MD2})} F(\mathcal{W}_{MD\ell}, \mathcal{W}_{FP\ell}, \mathcal{W}_{AC\ell}, \ell \in \{1, 2\})\right] \quad (90) \end{aligned}$$

$$\begin{aligned} & \leq \binom{M - K_a}{t_{FP1}}^{\rho_2} \binom{M - K_a - t_{FP1}}{t - t_{FP1}}^{\rho_2} \\ & \quad \cdot \binom{K_{a1} - t_{MD1}}{t_{AC1}}^{\rho_1\rho_2} \binom{K_a - K_{a1} - t + t_{MD1}}{t_{AC1} + t_{MD1} - t_{FP1}}^{\rho_1\rho_2} \\ & \quad \cdot \mathbb{E}_{c_1(\mathcal{W}_{MD1}), c_2(\mathcal{W}_{MD2})} \left[\exp\left(\lambda\rho_1\rho_2\|Z\|^2 - \mu_2\|Z + g_1 c_1(\mathcal{W}_{MD1}) + g_2 c_2(\mathcal{W}_{MD2})\|^2 - N\rho_2 a_1\right) \right] \quad (91) \end{aligned}$$

$$\begin{aligned} & = \binom{M - K_a}{t_{FP1}}^{\rho_2} \binom{M - K_a - t_{FP1}}{t - t_{FP1}}^{\rho_2} \\ & \quad \cdot \binom{K_{a1} - t_{MD1}}{t_{AC1}}^{\rho_1\rho_2} \binom{K_a - K_{a1} - t + t_{MD1}}{t_{AC1} + t_{MD1} - t_{FP1}}^{\rho_1\rho_2} \\ & \quad \cdot (1 + 2\mu_2(g_1^2 t_{MD1} + g_2^2 t_{MD2})P')^{-N/2} \\ & \quad \cdot \exp\left(\left(\lambda\rho_1\rho_2 - \frac{\mu_2}{1 + 2\mu_2(g_1^2 t_{MD1} + g_2^2 t_{MD2})P'}\right)\|Z\|^2 - N\rho_2 a_1\right) \quad (92) \end{aligned}$$

$$\begin{aligned} & = \binom{M - K_a}{t_{FP1}}^{\rho_2} \binom{M - K_a - t_{FP1}}{t - t_{FP1}}^{\rho_2} \\ & \quad \cdot \binom{K_{a1} - t_{MD1}}{t_{AC1}}^{\rho_1\rho_2} \binom{K_a - K_{a1} - t + t_{MD1}}{t_{AC1} + t_{MD1} - t_{FP1}}^{\rho_1\rho_2} \\ & \quad \cdot \exp(b\|Z\|^2 - N\rho_2 a_1 - Na_2), \quad (93) \end{aligned}$$

where we used (66) in Lemma 4 to obtain the first equality, and we define μ_2 by (20) and

$$b = \lambda\rho_1\rho_2 - \frac{\mu_2}{1 + 2\mu_2(g_1^2 t_{MD1} + g_2^2 t_{MD2})P'}, \quad (94)$$

$$a_2 = \frac{1}{2} \ln(1 + 2\mu_2(g_1^2 t_{MD1} + g_2^2 t_{MD2})P'). \quad (95)$$

Note that $g_1^2 t_{MD1} + g_2^2 t_{MD2}$ is equal to κ_{MD} defined in (22). We now apply Gallager's ρ -trick the third time to obtain that, given Z and for every $\rho_3 \in [0, 1]$,

$$= \mathbb{P}\left[\bigcup_{\mathcal{W}_{MD1} \subset ([K_{a1}] \setminus \mathcal{W}_{MD1})} \bigcup_{\mathcal{W}_{MD2} \subset ([K_{a1+1:K_a}] \setminus \mathcal{W}_{MD2})}\right]$$

$$\left[\begin{array}{l} \bigcup_{\mathcal{W}_{\text{FP1}} \subset \binom{[\text{K}_a+1:\text{M}]}{t_{\text{FP1}}}} \bigcup_{\mathcal{W}_{\text{FP2}} \subset \binom{[\text{K}_a+1:\text{M}] \setminus \mathcal{W}_{\text{FP1}}}{t-t_{\text{FP1}}}} \\ \bigcup_{\mathcal{W}_{\text{AC1}} \subset \binom{[\text{K}_a+1:\text{M}]}{t_{\text{AC1}}}} \bigcup_{\mathcal{W}_{\text{AC2}} \subset \binom{[\text{K}_a+1:\text{K}_a] \setminus \mathcal{W}_{\text{MD2}}}{t_{\text{AC1}}+t_{\text{MD1}}-t_{\text{FP1}}}} \\ F(\mathcal{W}_{\text{MD}\ell}, \mathcal{W}_{\text{FP}\ell}, \mathcal{W}_{\text{AC}\ell}, \ell \in \{1, 2\}) \end{array} \right] \quad (96)$$

$$\leq \binom{\text{K}_a}{t_{\text{MD1}}}^{\rho_3} \binom{\text{K}_a}{t-t_{\text{MD1}}}^{\rho_3} \\ \cdot \binom{M-\text{K}_a}{t_{\text{FP1}}}^{\rho_2 \rho_3} \binom{M-\text{K}_a-t_{\text{FP1}}}{t-t_{\text{FP1}}}^{\rho_2 \rho_3} \\ \cdot \binom{\text{K}_a-t_{\text{MD1}}}{t_{\text{AC1}}}^{\rho_1 \rho_2 \rho_3} \binom{\text{K}_a-\text{K}_a-t+t_{\text{MD1}}}{t_{\text{AC1}}+t_{\text{MD1}}-t_{\text{FP1}}}^{\rho_1 \rho_2 \rho_3} \\ \cdot \mathbb{E}_{\mathbf{Z}} [\exp(b\|\mathbf{Z}\|^2 - N\rho_2 \rho_3 a) - N\rho_3 a_1] \quad (97)$$

$$= \binom{\text{K}_a}{t_{\text{MD1}}}^{\rho_3} \binom{\text{K}_a}{t-t_{\text{MD1}}}^{\rho_3} \\ \cdot \binom{M-\text{K}_a}{t_{\text{FP1}}}^{\rho_2 \rho_3} \binom{M-\text{K}_a-t_{\text{FP1}}}{t-t_{\text{FP1}}}^{\rho_2 \rho_3} \\ \cdot \binom{\text{K}_a-t_{\text{MD1}}}{t_{\text{AC1}}}^{\rho_1 \rho_2 \rho_3} \binom{\text{K}_a-\text{K}_a-t+t_{\text{MD1}}}{t_{\text{AC1}}+t_{\text{MD1}}-t_{\text{FP1}}}^{\rho_1 \rho_2 \rho_3} \\ \cdot (1-2b\rho_3)^{-N/2} \exp(-N\rho_2 \rho_3 a_1 - N\rho_3 a_2), \quad (98)$$

where in the last equality, we use (66) in Lemma 4 to compute the expectation over \mathbf{Z} .

We conclude that $\mathbb{P}[\mathcal{W}_{\text{MD}}] = |\mathcal{W}_{\text{FP}}| = t$ is upper-bounded by the right-hand side of (98). We complete the proof by substituting this bound into (76).

APPENDIX C PROOF OF COROLLARY 1

When $\mathcal{C}_1 = \mathcal{C}_2$, we have that $c_1(\mathcal{W}) = c_2(\mathcal{W})$ for a given message set \mathcal{W} . The proof follows the same steps detailed in Appendix B, except that, in (87), the covariance matrix of $g_1 c_1(\mathcal{W}_{\text{AC1}}) - g_2 c_2(\mathcal{W}_{\text{AC1}}) - g_1 c_1(\mathcal{W}_{\text{AC2}}) + g_2 c_2(\mathcal{W}_{\text{AC2}})$ is given by $\kappa_{\text{AC}} \mathbf{P}' \mathbf{I}_N$ with κ_{AC} defined in (26).

APPENDIX D PROOF OF THEOREM 2

By performing the same change of measure as in Appendix B, we obtain the bound (76). We next focus on upper-bounding $\mathbb{P}[\mathcal{W}_{\text{MD}}] = |\mathcal{W}_{\text{FP}}| = t$ under the new measure and for the interference-cancellation decoder.

A. Pairwise Error Event

For this decoder, the pairwise error event $\widetilde{\mathcal{W}} \rightarrow \widehat{\mathcal{W}}$ implies that

$$\|\mathbf{Y} - g_1 c(\widehat{\mathcal{W}}_1)\| \leq \|\mathbf{Y} - g_1 c(\mathcal{W}_1)\|, \quad (99)$$

$$\|\mathbf{Y} - g_1 c(\widehat{\mathcal{W}}_1) - g_2 c(\widehat{\mathcal{W}}_2)\| \leq \|\mathbf{Y} - g_1 c(\widehat{\mathcal{W}}_1) - g_2 c(\mathcal{W}_2)\| \quad (100)$$

where we recall that $c(\mathcal{W}) = \sum_{w \in \mathcal{W}} C_w$. Splitting message sets as in Appendix B, we express (99) and (100) as

$$\begin{aligned} & \| \underbrace{\mathbf{Z} + g_1 c(\mathcal{W}_{\text{MD1}}) + g_2 c(\mathcal{W}_{\text{MD2}}) - g_1 c(\mathcal{W}_{\text{FP1}}) + g_2 c(\mathcal{W}_{\text{C2}})}_{=\mathbf{A}} \\ & + g_1 c(\mathcal{W}_{\text{AC1}}) + (g_2 - g_1) c(\mathcal{W}_{\text{AC2}}) \| \\ & \leq \| \underbrace{\mathbf{Z} + g_2 c(\mathcal{W}_{\text{C2}}) + g_2 c(\mathcal{W}_{\text{MD2}})}_{=\mathbf{B}} + g_2 c(\mathcal{W}_{\text{AC2}}) \|, \end{aligned} \quad (101)$$

$$\begin{aligned} & \| \underbrace{\mathbf{Z} + g_1 c(\mathcal{W}_{\text{MD1}}) + g_2 c(\mathcal{W}_{\text{MD2}}) - g_1 c(\mathcal{W}_{\text{FP1}}) - g_2 c(\mathcal{W}_{\text{FP2}})}_{=\mathbf{C}} \\ & + (g_1 - g_2)(c(\mathcal{W}_{\text{AC1}}) - c(\mathcal{W}_{\text{AC2}})) \| \\ & \leq \| \underbrace{\mathbf{Z} + g_1 c(\mathcal{W}_{\text{MD1}}) - g_1 c(\mathcal{W}_{\text{FP1}})}_{=\mathbf{D}} \\ & + g_1 c(\mathcal{W}_{\text{AC1}}) - g_1 c(\mathcal{W}_{\text{AC2}}) \|, \end{aligned} \quad (102)$$

where we also defined the vectors \mathbf{A} , \mathbf{B} , \mathbf{C} , \mathbf{D} to make the notation more compact in the following. We denote by $F_{\text{IC}}(\mathcal{W}_{\text{MD}\ell}, \mathcal{W}_{\text{FP}\ell}, \mathcal{W}_{\text{AC}\ell}, \ell \in \{1, 2\})$ the set of $(\mathcal{W}_{\text{MD}\ell}, \mathcal{W}_{\text{FP}\ell}, \mathcal{W}_{\text{AC}\ell}, \ell \in \{1, 2\})$ such that (101) and (102) hold. Note that \mathcal{W}_{C2} is fully determined given $\mathcal{W} = [\text{K}_a+1 : \text{K}_a]$, \mathcal{W}_{MD2} , and \mathcal{W}_{AC2} . By writing the event $|\mathcal{W}_{\text{MD}}| = |\mathcal{W}_{\text{FP}}| = t$ as a union of the pairwise error events, we obtain a similar bound as in (85) with $F(\mathcal{W}_{\text{MD}\ell}, \mathcal{W}_{\text{FP}\ell}, \mathcal{W}_{\text{AC}\ell}, \ell \in \{1, 2\})$ replaced by $F_{\text{IC}}(\mathcal{W}_{\text{MD}\ell}, \mathcal{W}_{\text{FP}\ell}, \mathcal{W}_{\text{AC}\ell}, \ell \in \{1, 2\})$.

B. Error Exponent Analysis

We apply the Chernoff joint bound in Corollary 2 to bound the pairwise error probability as

$$\begin{aligned} & \mathbb{P}[F_{\text{IC}}(\mathcal{W}_{\text{MD}\ell}, \mathcal{W}_{\text{FP}\ell}, \mathcal{W}_{\text{AC}\ell}, \ell \in \{1, 2\})] \\ & = \mathbb{P} \left[\|\mathbf{A} + g_1 c(\mathcal{W}_{\text{AC1}}) + (g_2 - g_1) c(\mathcal{W}_{\text{AC2}})\|^2 \right. \\ & \quad \left. - \|\mathbf{B} + g_2 c(\mathcal{W}_{\text{AC2}})\|^2 \leq 0, \right. \\ & \quad \left. \|\mathbf{C} + (g_1 - g_2)(c(\mathcal{W}_{\text{AC1}}) - c(\mathcal{W}_{\text{AC2}}))\|^2 \right. \\ & \quad \left. - \|\mathbf{D} + g_1 c(\mathcal{W}_{\text{AC1}}) - g_1 c(\mathcal{W}_{\text{AC2}})\|^2 \leq 0 \right] \end{aligned} \quad (103)$$

$$\begin{aligned} & \leq \mathbb{E} \left[\exp \left(-\lambda_1 (\|\mathbf{A} + g_1 c(\mathcal{W}_{\text{AC1}}) + (g_2 - g_1) c(\mathcal{W}_{\text{AC2}})\|^2 \right. \right. \\ & \quad \left. \left. - \|\mathbf{B} + g_2 c(\mathcal{W}_{\text{AC2}})\|^2) \right. \right. \\ & \quad \left. \left. - \lambda_2 (\|\mathbf{C} + (g_1 - g_2)(c(\mathcal{W}_{\text{AC1}}) - c(\mathcal{W}_{\text{AC2}}))\|^2 \right. \right. \\ & \quad \left. \left. - \|\mathbf{D} + g_1 c(\mathcal{W}_{\text{AC1}}) - g_1 c(\mathcal{W}_{\text{AC2}})\|^2) \right) \right] \end{aligned} \quad (104)$$

for all $\lambda_1 > 0$ and $\lambda_2 > 0$.

1) *Expectation over $c(\mathcal{W}_{\text{AC1}})$ and $c(\mathcal{W}_{\text{AC2}})$ and the First Gallager- ρ Trick:* The exponent in (104) can be written as

$$\begin{aligned} & [c(\mathcal{W}_{\text{AC1}})^T \ c(\mathcal{W}_{\text{AC2}})^T] (\mathbf{U}_{\text{AC}} \otimes \mathbf{I}_N) \begin{bmatrix} c(\mathcal{W}_{\text{AC1}}) \\ c(\mathcal{W}_{\text{AC2}}) \end{bmatrix} \\ & + 2\mathbf{V}_{\text{AC}}^T \begin{bmatrix} c(\mathcal{W}_{\text{AC1}}) \\ c(\mathcal{W}_{\text{AC2}}) \end{bmatrix} + R_{\text{AC}} \end{aligned} \quad (105)$$

where

$$\mathbf{U}_{\text{AC}} = \begin{bmatrix} u_{\text{AC}}^{(1)} & u_{\text{AC}}^{(2)} \\ u_{\text{AC}}^{(2)} & u_{\text{AC}}^{(3)} \end{bmatrix}, \quad (106)$$

$$u_{AC}^{(1)} = -\lambda_1 g_1^2 - \lambda_2 g_2(g_2 - 2g_1), \quad (107)$$

$$u_{AC}^{(2)} = \lambda_1 g_1(g_1 - g_2) + \lambda_2 g_2(g_2 - 2g_1), \quad (108)$$

$$u_{AC}^{(3)} = -\lambda_1 g_1(g_1 - 2g_2) - \lambda_2 g_2(g_2 - 2g_1), \quad (109)$$

$$\mathbf{V}_{AC} = \begin{bmatrix} -\lambda_1 g_1 \mathbf{A} - \lambda_2(g_1 - g_2) \mathbf{C} + \lambda_2 g_1 \mathbf{D} \\ \lambda_1(g_1 - g_2) \mathbf{A} + \lambda_1 g_2 \mathbf{B} + \lambda_2(g_1 - g_2) \mathbf{C} - \lambda_2 g_1 \mathbf{D} \end{bmatrix}, \quad (110)$$

$$R_{AC} = -\lambda_1(\|\mathbf{A}\|^2 - \|\mathbf{B}\|^2) - \lambda_2(\|\mathbf{C}\|^2 - \|\mathbf{D}\|^2). \quad (111)$$

Note that $\begin{bmatrix} c(\mathcal{W}_{AC1}) \\ c(\mathcal{W}_{AC2}) \end{bmatrix} \sim \mathcal{N}(\mathbf{0}, \Sigma_{AC} \otimes \mathbf{I}_N)$ with $\Sigma_{AC} = \text{diag}(t_{AC1}P', t_{AC2}P')$. We apply (67) in Lemma 4 to compute the expectation in (104) over $c(\mathcal{W}_{AC1}), c(\mathcal{W}_{AC2})$ as

$$\begin{aligned} & \det(\mathbf{I}_2 - 2\Sigma_{AC}\mathbf{U}_{AC})^{-N/2} \\ & \cdot \exp(2\mathbf{V}_{AC}^T[(\Sigma_{AC}^{-1} - 2\mathbf{U}_{AC})^{-1} \otimes \mathbf{I}_N]\mathbf{V}_{AC} + R_{AC}) \end{aligned} \quad (112)$$

where we require λ_1, λ_2 to satisfy that $\Sigma_{AC}^{-1} \succ 2\mathbf{U}_{AC}$.

Now, we apply Gallager's ρ -trick in Lemma 3 to get that, given $c(\mathcal{W}_{MD\ell}), c(\mathcal{W}_{FP\ell}), \ell \in \{1, 2\}, c(\mathcal{W}_{C2})$, and Z , it holds for every $\rho_1 \in [0, 1]$ that

$$\begin{aligned} & \mathbb{P} \left[\bigcup_{\mathcal{W}_{AC1} \subset ([K_{a1}] \setminus \mathcal{W}_{MD1})} \bigcup_{\mathcal{W}_{AC2} \subset ([K_{a1+1:K_a}] \setminus \mathcal{W}_{MD2})} F_{IC}(\mathcal{W}_{MD\ell}, \mathcal{W}_{FP\ell}, \mathcal{W}_{AC\ell}, \ell \in \{1, 2\}) \right] \\ & \leq \binom{K_{a1} - t_{MD1}}{t_{AC1}}^{\rho_1} \binom{K_a - K_{a1} - t + t_{MD1}}{t_{AC1} + t_{MD1} - t_{FP1}}^{\rho_1} \\ & \cdot \det(\mathbf{I}_2 - 2\Sigma_{AC}\mathbf{U}_{AC})^{-N\rho_1/2} \\ & \cdot \exp(2\rho_1 \mathbf{V}_{AC}^T[(\Sigma_{AC}^{-1} - 2\mathbf{U}_{AC})^{-1} \otimes \mathbf{I}_N]\mathbf{V}_{AC} + \rho_1 R_{AC}). \end{aligned} \quad (113)$$

2) *Expectation over $c(\mathcal{W}_{FP1})$ and $c(\mathcal{W}_{FP2})$ and the Second Gallager- ρ Trick:* Next, we denote

$$\mathbf{E} = Z + g_1 c(\mathcal{W}_{MD1}) + g_2 c(\mathcal{W}_{MD2}) + g_2 c(\mathcal{W}_{C2}), \quad (114)$$

$$\mathbf{F} = Z + g_1 c(\mathcal{W}_{MD1}) + g_2 c(\mathcal{W}_{MD2}), \quad (115)$$

$$\mathbf{G} = Z + g_1 c(\mathcal{W}_{MD1}). \quad (116)$$

It follows that $\mathbf{A} = \mathbf{E} - g_1 c(\mathcal{W}_{FP1})$, $\mathbf{C} = \mathbf{F} - g_1 c(\mathcal{W}_{FP1}) - g_2 c(\mathcal{W}_{FP2})$, and $\mathbf{D} = \mathbf{G} - g_1 c(\mathcal{W}_{FP1})$. We can express the exponent in (113) as

$$\begin{aligned} & 2\rho_1 \mathbf{V}_{AC}^T[(\Sigma_{AC}^{-1} - 2\mathbf{U}_{AC})^{-1} \otimes \mathbf{I}_N]\mathbf{V}_{AC} + \rho_1 R_{AC} \\ & = [c(\mathcal{W}_{FP1})^T \ c(\mathcal{W}_{FP2})^T](\mathbf{U}_{FP} \otimes \mathbf{I}_N) \begin{bmatrix} c(\mathcal{W}_{FP1}) \\ c(\mathcal{W}_{FP2}) \end{bmatrix} \\ & + 2\mathbf{V}_{FP}^T \begin{bmatrix} c(\mathcal{W}_{FP1}) \\ c(\mathcal{W}_{FP2}) \end{bmatrix} + R_{FP} \end{aligned} \quad (117)$$

where

$$\mathbf{U}_{FP} = 2\rho_1 \Lambda_{FP} \mathbf{Q}_{FP} - \rho_1 \begin{bmatrix} \lambda_1 g_1^2 & \lambda_2 g_1 g_2 \\ \lambda_2 g_1 g_2 & \lambda_2 g_2^2 \end{bmatrix}, \quad (118)$$

$$\begin{aligned} \mathbf{V}_{FP} = & 2\rho_1 [\Lambda_{FP} \otimes \mathbf{I}_N] \mathbf{Q}_{FP} \\ & + \rho_1 \begin{bmatrix} \lambda_1 g_1 \mathbf{E} + \lambda_2 g_1 \mathbf{F} - \lambda_2 g_1 \mathbf{G} \\ \lambda_2 g_2 \mathbf{F} \end{bmatrix}, \end{aligned} \quad (119)$$

$$\begin{aligned} R_{FP} = & 2\rho_1 \mathbf{Q}_{FP}^T [(\Sigma_{AC}^{-1} - 2\mathbf{U}_{AC})^{-1} \otimes \mathbf{I}_N] \mathbf{Q}_{FP} \\ & - \rho_1 \lambda_1 (\|\mathbf{E}\|^2 - \|\mathbf{B}\|^2) - \rho_1 \lambda_2 (\|\mathbf{F}\|^2 - \|\mathbf{G}\|^2), \end{aligned} \quad (120)$$

with

$$\mathbf{Q}_{FP} = \begin{bmatrix} \lambda_1 g_1^2 - \lambda_2 g_1 g_2 & \lambda_2 g_2(g_1 - g_2) \\ -\lambda_1 g_1(g_1 - g_2) + \lambda_2 g_1 g_2 & -\lambda_2 g_2(g_1 - g_2) \end{bmatrix}, \quad (121)$$

$$\mathbf{Q}_{FP} = \begin{bmatrix} -\lambda_1 g_1 \mathbf{E} - \lambda_2(g_1 - g_2) \mathbf{F} + \lambda_2 g_1 \mathbf{G} \\ \lambda_1(g_1 - g_2) \mathbf{E} + \lambda_1 g_2 \mathbf{B} + \lambda_2(g_1 - g_2) \mathbf{F} - \lambda_2 g_1 \mathbf{G} \end{bmatrix}, \quad (122)$$

$$\Lambda_{FP} = \mathbf{Q}_{FP}^T (\Sigma_{AC}^{-1} - 2\mathbf{U}_{AC})^{-1}. \quad (123)$$

Note that $\begin{bmatrix} c(\mathcal{W}_{FP1}) \\ c(\mathcal{W}_{FP2}) \end{bmatrix} \sim \mathcal{N}(\mathbf{0}, \Sigma_{FP} \otimes \mathbf{I}_N)$ with $\Sigma_{FP} = \text{diag}(t_{FP1}P', t_{FP2}P')$. By applying (67) in Lemma 4 to compute the expectation of (113) over $c(\mathcal{W}_{FP1}), c(\mathcal{W}_{FP2})$, we obtain that, given $c(\mathcal{W}_{MD\ell}), \ell \in \{1, 2\}, c(\mathcal{W}_{C2})$, and Z ,

$$\begin{aligned} & \mathbb{P} \left[\bigcup_{\mathcal{W}_{AC1} \subset ([K_{a1}] \setminus \mathcal{W}_{MD1})} \bigcup_{\mathcal{W}_{AC2} \subset ([K_{a1+1:K_a}] \setminus \mathcal{W}_{MD2})} F_{IC}(\mathcal{W}_{MD\ell}, \mathcal{W}_{FP\ell}, \mathcal{W}_{AC\ell}, \ell \in \{1, 2\}) \right] \\ & \leq \binom{K_{a1} - t_{MD1}}{t_{AC1}}^{\rho_1} \binom{K_a - K_{a1} - t + t_{MD1}}{t_{AC1} + t_{MD1} - t_{FP1}}^{\rho_1} \\ & \cdot \det(\mathbf{I}_2 - 2\Sigma_{AC}\mathbf{U}_{AC})^{-N\rho_1/2} \\ & \cdot \det(\mathbf{I}_2 - 2\Sigma_{FP}\mathbf{U}_{FP})^{-N/2} \\ & \cdot \exp(2\mathbf{V}_{FP}^T[(\Sigma_{FP}^{-1} - 2\mathbf{U}_{FP})^{-1} \otimes \mathbf{I}_N]\mathbf{V}_{FP} + R_{FP}) \end{aligned} \quad (124)$$

under the condition that $\Sigma_{FP}^{-1} \succ 2\mathbf{U}_{FP}$.

Now, we apply Gallager's ρ -trick again to get that, given $c(\mathcal{W}_{MD\ell}), \ell \in \{1, 2\}, c(\mathcal{W}_{C2})$, and Z , and for every $\rho_2 \in [0, 1]$, it holds that

$$\begin{aligned} & \mathbb{P} \left[\bigcup_{\mathcal{W}_{FP1} \subset ([K_{a1+1:M}] \setminus \mathcal{W}_{FP1})} \bigcup_{\mathcal{W}_{FP2} \subset ([K_{a1+1:M}] \setminus \mathcal{W}_{FP1})} \right. \\ & \quad \left. \bigcup_{\mathcal{W}_{AC1} \subset ([K_{a1}] \setminus \mathcal{W}_{MD1})} \bigcup_{\mathcal{W}_{AC2} \subset ([K_{a1+1:K_a}] \setminus \mathcal{W}_{MD2})} F_{IC}(\mathcal{W}_{MD\ell}, \mathcal{W}_{FP\ell}, \mathcal{W}_{AC\ell}, \ell \in \{1, 2\}) \right] \end{aligned} \quad (125)$$

$$\begin{aligned} & \leq \binom{M - K_a}{t_{FP1}}^{\rho_2} \binom{M - K_a - t_{FP1}}{t - t_{FP1}}^{\rho_2} \\ & \cdot \binom{K_{a1} - t_{MD1}}{t_{AC1}}^{\rho_1 \rho_2} \binom{K_a - K_{a1} - t + t_{MD1}}{t_{AC1} + t_{MD1} - t_{FP1}}^{\rho_1 \rho_2} \\ & \cdot \det(\mathbf{I}_2 - 2\Sigma_{AC}\mathbf{U}_{AC})^{-N\rho_1 \rho_2/2} \\ & \cdot \det(\mathbf{I}_2 - 2\Sigma_{FP}\mathbf{U}_{FP})^{-N\rho_2/2} \\ & \cdot \exp(2\rho_2 \mathbf{V}_{FP}^T[(\Sigma_{FP}^{-1} - 2\mathbf{U}_{FP})^{-1} \otimes \mathbf{I}_N]\mathbf{V}_{FP} + \rho_2 R_{FP}). \end{aligned} \quad (126)$$

3) *Expectation over $c(\mathcal{W}_{MD1})$ and $c(\mathcal{W}_{MD2})$ and the Third Gallager- ρ Trick:* We express the exponent in (126) as

$$2\rho_2 \mathbf{V}_{FP}^T [(\Sigma_{FP}^{-1} - 2\mathbf{U}_{FP})^{-1} \otimes \mathbf{I}_N] \mathbf{V}_{FP} + \rho_2 R_{FP} = [c(\mathcal{W}_{MD1})^T \ c(\mathcal{W}_{MD2})^T] (\mathbf{U}_{MD} \otimes \mathbf{I}_N) \begin{bmatrix} c(\mathcal{W}_{MD1}) \\ c(\mathcal{W}_{MD2}) \end{bmatrix} \quad (127)$$

$$+ 2\mathbf{V}_{MD}^T \begin{bmatrix} c(\mathcal{W}_{MD1}) \\ c(\mathcal{W}_{MD2}) \end{bmatrix} + R_{MD} \quad (128)$$

where

$$\mathbf{U}_{MD} = 2\rho_2 \Lambda_{MD} \mathbf{Q}_{MD} + 2\rho_2 \rho_1 \Lambda_{M} \mathbf{M} \\ - \rho_2 \rho_1 \begin{bmatrix} \lambda_1 g_1^2 & (\lambda_1 + \lambda_2) g_1 g_2 \\ (\lambda_1 + \lambda_2) g_1 g_2 & \lambda_2 g_2^2 \end{bmatrix}, \quad (129)$$

$$\mathbf{M} = \begin{bmatrix} -\lambda_1 g_1^2 + \lambda_2 g_1 g_2 & -\lambda_1 g_1 g_2 - \lambda_2 g_2 (g_1 - g_2) \\ \lambda_1 g_1 (g_1 - g_2) - \lambda_2 g_1 g_2 & \lambda_1 g_1 g_2 + \lambda_2 g_2 (g_1 - g_2) \end{bmatrix}, \quad (130)$$

$$\mathbf{Q}_{MD} = 2\rho_1 \Lambda_{FP} \mathbf{M} + \rho_1 \begin{bmatrix} \lambda_1 g_1^2 & (\lambda_1 + \lambda_2) g_1 g_2 \\ \lambda_2 g_1 g_2 & \lambda_2 g_2^2 \end{bmatrix}, \quad (131)$$

$$\mathbf{V}_{MD} = 2\rho_2 (\Lambda_{MD} \otimes \mathbf{I}_N) \mathbf{Q}_{MD} + 2\rho_2 \rho_1 (\Lambda_M \otimes \mathbf{I}_N) \mathbf{M} \\ - \rho_2 \rho_1 \mathbf{R}, \quad (132)$$

$$\mathbf{Q}_{MD} = 2\rho_1 (\Lambda_{FP} \otimes \mathbf{I}_N) \mathbf{M} + \rho_1 \mathbf{R}, \quad (133)$$

$$\mathbf{M} = \left(\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix} \otimes \mathbf{I}_N \right) \mathbf{R}, \quad (134)$$

$$\mathbf{R} = \left(\begin{bmatrix} \lambda_1 g_1 & \lambda_1 g_1 g_2 \\ \lambda_2 g_2 & 0 \end{bmatrix} \otimes \mathbf{I}_N \right) \begin{bmatrix} \mathbf{Z} \\ c(\mathcal{W}_{C2}) \end{bmatrix}, \quad (135)$$

$$R_{MD} = 2\rho_2 \mathbf{Q}_{MD}^T [(\Sigma_{FP}^{-1} - 2\mathbf{U}_{FP})^{-1}] \mathbf{Q}_{MD} \\ + 4\rho_1 \rho_2 \mathbf{M}^T (\Sigma_{AC}^{-1} - 2\mathbf{U}_{AC})^{-1} \mathbf{M}, \quad (136)$$

with

$$\Lambda_{MD} = \mathbf{Q}_{MD}^T (\Sigma_{FP}^{-1} - 2\mathbf{U}_{FP})^{-1}, \quad (137)$$

$$\Lambda_M = \mathbf{M}^T (\Sigma_{AC}^{-1} - 2\mathbf{U}_{AC})^{-1}. \quad (138)$$

Note that $\begin{bmatrix} c(\mathcal{W}_{MD1}) \\ c(\mathcal{W}_{MD2}) \end{bmatrix} \sim \mathcal{N}(\mathbf{0}, \Sigma_{MD} \otimes \mathbf{I}_N)$ with $\Sigma_{MD} = \text{diag}(t_{MD1} P', t_{MD2} P')$. By applying (67) in Lemma 4 to compute the expectation of (126) over $c(\mathcal{W}_{MD1}), c(\mathcal{W}_{MD2})$, we obtain that, given $c(\mathcal{W}_{C2})$ and \mathbf{Z} ,

$$\begin{aligned} & \mathbb{P} \left[\bigcup_{\mathcal{W}_{FP1} \subset ([K_a+1:M] \setminus t_{FP1})} \bigcup_{\mathcal{W}_{FP2} \subset ([K_a+1:M] \setminus \mathcal{W}_{FP1})} \right. \\ & \quad \bigcup_{\mathcal{W}_{AC1} \subset ([K_a+1:K_a] \setminus \mathcal{W}_{MD1})} \bigcup_{\mathcal{W}_{AC2} \subset ([K_a+1:K_a] \setminus \mathcal{W}_{MD1} \setminus t_{FP1})} \\ & \quad F_{IC}(\mathcal{W}_{MD\ell}, \mathcal{W}_{FP\ell}, \mathcal{W}_{AC\ell}, \ell \in \{1, 2\}) \Big] \\ & \leq \binom{K_{a1} - t_{MD1}}{t_{AC1}}^{\rho_1} \binom{K_a - K_{a1} - t + t_{MD1}}{t_{AC1} + t_{MD1} - t_{FP1}}^{\rho_1} \\ & \quad \cdot \det(\mathbf{I}_2 - 2\Sigma_{AC} \mathbf{U}_{AC})^{-N\rho_1\rho_2/2} \\ & \quad \cdot \det(\mathbf{I}_2 - 2\Sigma_{FP} \mathbf{U}_{FP})^{-N\rho_2/2} \\ & \quad \cdot \det(\mathbf{I}_2 - 2\Sigma_{MD} \mathbf{U}_{MD})^{-N/2} \end{aligned}$$

$$\cdot \exp(2\mathbf{V}_{MD}^T [(\Sigma_{MD}^{-1} - 2\mathbf{U}_{MD})^{-1} \otimes \mathbf{I}_N] \mathbf{V}_{MD} + \rho_3 R_{MD}) \quad (139)$$

under the condition that $\Sigma_{MD}^{-1} \succ 2\mathbf{U}_{MD}$.

We now apply Gallager's ρ -trick the third time to obtain that, given $c(\mathcal{W}_{C2})$ and Z , and for every $\rho_3 \in [0, 1]$,

$$\begin{aligned} & = \mathbb{P} \left[\bigcup_{\mathcal{W}_{MD1} \subset ([K_{a1}] \setminus t_{MD1})} \bigcup_{\mathcal{W}_{MD2} \subset ([K_{a1+1:K_a}] \setminus t_{MD1})} \right. \\ & \quad \bigcup_{\mathcal{W}_{FP1} \subset ([K_{a+1:M}] \setminus t_{FP1})} \bigcup_{\mathcal{W}_{FP2} \subset ([K_{a+1:M}] \setminus \mathcal{W}_{FP1})} \\ & \quad \bigcup_{\mathcal{W}_{AC1} \subset ([K_{a1}] \setminus \mathcal{W}_{MD1})} \bigcup_{\mathcal{W}_{AC2} \subset ([K_{a1+1:K_a}] \setminus \mathcal{W}_{MD2})} \\ & \quad F_{IC}(\mathcal{W}_{MD\ell}, \mathcal{W}_{FP\ell}, \mathcal{W}_{AC\ell}, \ell \in \{1, 2\}) \Big] \\ & \leq \binom{K_{a1}}{t_{MD1}}^{\rho_3} \binom{K_{a2}}{t - t_{MD1}}^{\rho_3} \\ & \quad \cdot \binom{M - K_a}{t_{FP1}}^{\rho_2 \rho_3} \binom{M - K_a - t_{FP1}}{t - t_{FP1}}^{\rho_2 \rho_3} \\ & \quad \cdot \binom{K_{a1} - t_{MD1}}{t_{AC1}}^{\rho_1 \rho_2 \rho_3} \binom{K_a - K_{a1} - t + t_{MD1}}{t_{AC1} + t_{MD1} - t_{FP1}}^{\rho_1 \rho_2 \rho_3} \\ & \quad \cdot \det(\mathbf{I}_2 - 2\Sigma_{AC} \mathbf{U}_{AC})^{-N\rho_1 \rho_2 \rho_3/2} \\ & \quad \cdot \det(\mathbf{I}_2 - 2\Sigma_{FP} \mathbf{U}_{FP})^{-N\rho_2 \rho_3/2} \\ & \quad \cdot \det(\mathbf{I}_2 - 2\Sigma_{MD} \mathbf{U}_{MD})^{-N\rho_3/2} \\ & \quad \cdot \exp(2\rho_3 \mathbf{V}_{MD}^T [(\Sigma_{MD}^{-1} - 2\mathbf{U}_{MD})^{-1} \otimes \mathbf{I}_N] \mathbf{V}_{MD} + \rho_3 R_{MD}). \end{aligned} \quad (140)$$

4) *Expectation over Z and $c(\mathcal{W}_{C2})$:* We express the exponent in (141) as

$$\begin{aligned} & 2\rho_3 \mathbf{V}_{MD}^T [(\Sigma_{MD}^{-1} - 2\mathbf{U}_{MD})^{-1} \otimes \mathbf{I}_N] \mathbf{V}_{MD} + \rho_3 R_{MD} \\ & = [\mathbf{Z}^T \ c(\mathcal{W}_{C2})^T] (\mathbf{U}_{ZC} \otimes \mathbf{I}_N) \begin{bmatrix} \mathbf{Z} \\ c(\mathcal{W}_{C2}) \end{bmatrix} \end{aligned} \quad (142)$$

where

$$\begin{aligned} \mathbf{U}_{ZC} & = 2\rho_3 \mathbf{Q}_{ZC}^T (\Sigma_{MD}^{-1} - 2\mathbf{U}_{MD})^{-1} \mathbf{Q}_{ZC} \\ & + 2\rho_3 \rho_2 \Lambda_{ZCa}^T (\Sigma_{FP}^{-1} - 2\mathbf{U}_{FP})^{-1} \Lambda_{ZCa} \\ & + 4\rho_3 \rho_2 \rho_1 \Lambda_{ZCb}^T (\Sigma_{AC}^{-1} - 2\mathbf{U}_{AC})^{-1} \Lambda_{ZCb} \end{aligned} \quad (143)$$

with

$$\begin{aligned} \mathbf{Q}_{ZC} & = \rho_2 \rho_1 \left(-\mathbf{I}_2 + (4\Lambda_{MD} \Lambda_{FP} + 2\Lambda_M) \begin{bmatrix} -1 & 1 \\ 1 & -1 \end{bmatrix} + 2\Lambda_{MD} \right) \\ & \quad \cdot \begin{bmatrix} \lambda_1 g_1 & \lambda_1 g_1 g_2 \\ \lambda_2 g_2 & 0 \end{bmatrix}, \end{aligned} \quad (144)$$

$$\Lambda_{ZCa} = \rho_1 \left(\mathbf{I}_2 + 2\Lambda_{FP} \begin{bmatrix} -1 & 1 \\ 1 & -1 \end{bmatrix} \right) \begin{bmatrix} \lambda_1 g_1 & \lambda_1 g_1 g_2 \\ \lambda_2 g_2 & 0 \end{bmatrix}, \quad (145)$$

$$\Lambda_{ZCb} = \begin{bmatrix} -1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} \lambda_1 g_1 & \lambda_1 g_1 g_2 \\ \lambda_2 g_2 & 0 \end{bmatrix}. \quad (146)$$

Note that $\begin{bmatrix} \mathbf{Z} \\ c(\mathcal{W}_{C2}) \end{bmatrix} \sim \mathcal{N}(\mathbf{0}, \Sigma_{ZC} \otimes \mathbf{I}_N)$ with $\Sigma_{ZC} = \text{diag}(1, (K_{a2} - t_{MD2} - t_{AC2})P')$. By applying (67) in Lemma 4 to compute the expectation of (126) over \mathbf{Z} and $c(\mathcal{W}_{C2})$, we obtain that

$$\begin{aligned} &= \mathbb{P} \left[\bigcup_{\mathcal{W}_{MD1} \subset \binom{[K_{a1}]}{t_{MD1}}} \bigcup_{\mathcal{W}_{MD2} \subset \binom{[K_{a1}+1:K_a]}{t-t_{MD1}}} \right. \\ &\quad \bigcup_{\mathcal{W}_{FP1} \subset \binom{[K_{a1}+1:M]}{t_{FP1}}} \bigcup_{\mathcal{W}_{FP2} \subset \binom{[K_{a1}+1:M] \setminus \mathcal{W}_{FP1}}{t-t_{FP1}}} \\ &\quad \bigcup_{\mathcal{W}_{AC1} \subset \binom{[K_{a1}]}{t_{AC1}}} \bigcup_{\mathcal{W}_{AC2} \subset \binom{[K_{a1}+1:K_a]}{t_{AC1}+t_{MD1}-t_{FP1}}} \\ &\quad \left. F_{IC}(\mathcal{W}_{MD\ell}, \mathcal{W}_{FP\ell}, \mathcal{W}_{AC\ell}, \ell \in \{1, 2\}) \right] \quad (147) \end{aligned}$$

$$\begin{aligned} &\leq \left(\frac{K_{a1}}{t_{MD1}} \right)^{\rho_3} \left(\frac{K_{a2}}{t - t_{MD1}} \right)^{\rho_3} \\ &\quad \cdot \left(\frac{M - K_a}{t_{FP1}} \right)^{\rho_2 \rho_3} \left(\frac{M - K_a - t_{FP1}}{t - t_{FP1}} \right)^{\rho_2 \rho_3} \\ &\quad \cdot \left(\frac{K_{a1} - t_{MD1}}{t_{AC1}} \right)^{\rho_1 \rho_2 \rho_3} \left(\frac{K_a - K_{a1} - t + t_{MD1}}{t_{AC1} + t_{MD1} - t_{FP1}} \right)^{\rho_1 \rho_2 \rho_3} \\ &\quad \cdot \det(\mathbf{I}_2 - 2\sum_{AC} \mathbf{U}_{AC})^{-N\rho_1 \rho_2 \rho_3 / 2} \\ &\quad \cdot \det(\mathbf{I}_2 - 2\sum_{FP} \mathbf{U}_{FP})^{-N\rho_2 \rho_3 / 2} \\ &\quad \cdot \det(\mathbf{I}_2 - 2\sum_{MD} \mathbf{U}_{MD})^{-N\rho_3 / 2} \\ &\quad \cdot \det(\mathbf{I}_2 - 2\sum_{ZC} \mathbf{U}_{ZC})^{-N/2}, \quad (148) \end{aligned}$$

which is an upper-bound for $\mathbb{P}|\mathcal{W}_{MD}| = |\mathcal{W}_{FP}| = t$. Finally, by substituting this bound into (76) and rearranging the terms, we complete the proof.

APPENDIX E

MATHEMATICAL PRELIMINARIES FOR REPLICA ANALYSIS

We will make use of the definitions and results presented in this section for the proofs of Claim 1 and Claim 2. We will consider a generic channel model

$$\tilde{\mathbf{Y}} = \tilde{\mathcal{C}} \tilde{\mathbf{U}}^{(0)} + \tilde{\mathbf{Z}} \quad (149)$$

where $\tilde{\mathbf{Y}}, \tilde{\mathbf{Z}} \in \mathbb{R}^N$, $\tilde{\mathbf{U}}^{(0)}$ is a random (column) vector of length m' , $\tilde{\mathcal{C}} \in \mathbb{R}^{N \times m'}$, $\tilde{\mathcal{C}}$ has i.i.d. $\mathcal{N}(0, 1/N)$ entries, $\tilde{\mathbf{Z}} \sim \mathcal{N}(\mathbf{0}, \mathbf{I}_N)$, and will specialize the value of m' along with the definition of $\tilde{\mathbf{U}}^{(0)}$, to prove each claim. We fix $\beta = m'/N$.

First, we introduce the definition of the partition function.

Definition 2 (Partition Function). Fix positive integers ℓ and r , and a real number t . Let $\{\tilde{\mathbf{U}}^{(i)}, i \geq 1\}$ be an i.i.d. process, where $\tilde{\mathbf{U}}^{(i)} \stackrel{D}{=} \tilde{\mathbf{U}}^{(0)}$. Then, the partition function is defined as

$$\zeta^{(r)}(t; \tilde{\mathbf{Y}}, \tilde{\mathcal{C}}) = \mathbb{E} \left[e^{t \prod_{i=1}^{\ell} [\tilde{\mathbf{U}}^{(i)}]_1} \prod_{j=1}^r \mathbb{P} \left[\tilde{\mathbf{Y}} \mid \tilde{\mathbf{U}}^{(j)}, \tilde{\mathcal{C}} \right] \middle| \tilde{\mathbf{Y}}, \tilde{\mathcal{C}} \right]. \quad (150)$$

We have the following result.

Assumption 1 (Replica Trick for Moment Calculation). Let

$$\kappa(t, r) = \log \mathbb{E}_{\tilde{\mathbf{Y}}, \tilde{\mathcal{C}}} \left[\zeta^{(r)}(t; \tilde{\mathbf{Y}}, \tilde{\mathcal{C}}) \right] \quad (151)$$

denote the cumulant of the partition function in (150). Then, the ℓ^{th} moment of the random variable

$$V_N = \mathbb{P} \left[[\tilde{\mathbf{U}}^{(0)}]_1 = 1 \mid \tilde{\mathbf{Y}}, \tilde{\mathcal{C}} \right] \quad (152)$$

is given by

$$\mathbb{E}_{\tilde{\mathbf{Y}}, \tilde{\mathcal{C}}} [V_N^\ell] = \lim_{r \rightarrow 0} \lim_{t \rightarrow 0} \frac{d}{dt} \kappa(t, r). \quad (153)$$

Remark 3. In applying the replica trick in Assumption 1, we will compute in closed form $\mathbb{E}[\zeta^{(r)}]$ for $r \in \mathbb{N}$. We will then assume that the result holds for every $r \in \mathbb{R}$. This is a common practice in the application of the replica method (see [12] for such an application in the context of multiuser communication). A rigorous justification involves finding a unique analytic continuation of $\mathbb{E}[\zeta^{(r)}]$ from the set of positive integers to the entire real line; see, for instance, the discussion in [19].

Lemma 5. (Gaussian Integral Identity) Fix a positive integer r . For $i \in [0 : r]$, define

$$W_i = \sqrt{\frac{P}{MN}} \sum_{m=1}^M [\tilde{\mathcal{C}}]_m [\tilde{\mathbf{U}}^{(i)}]_m. \quad (154)$$

Then,

$$\int \mathbb{E}_{\tilde{\mathcal{C}}} \left[\prod_{j=0}^r e^{-\frac{(y - \sqrt{\beta} W_j)^2}{2}} \right] \frac{dy}{\sqrt{2\pi}} = e^{G^{(r)}(\mathcal{Q})} \quad (155)$$

where

$$\begin{aligned} G^{(r)}(\mathcal{Q}) &= -\frac{1}{2} \log \det(\mathbf{I}_{r+1} + \Sigma \mathcal{Q}) - \frac{1}{2} \log(1+r) \\ &\quad - \frac{r}{2} \log(2\pi). \end{aligned} \quad (156)$$

Here, Σ and \mathcal{Q} are $(r+1) \times (r+1)$ matrices with the (i, j) th entry given by $\beta \left(\mathbb{1}\{i=j\} - \frac{1}{r+1} \right)$ and $\mathbb{E}[W_i W_j]$, respectively.

The following lemma is used to evaluate the limiting value of the logarithm of the moment-generating function that arises in the analysis.

Lemma 6. (Varadhan's Integral Lemma, Theorem 4.3.1 [20]) Suppose that measures $\{\mu_n, n \geq 1\}$ satisfy the large deviation principle with a good rate function $I : \mathcal{X} \mapsto [0, \infty]$ (see [20, Section 1.2]), and let $\phi : \mathcal{X} \mapsto \mathbb{R}$ be a continuous function, where \mathcal{X} is a regular, topological space. Assume that, for some $\gamma > 1$,

$$\limsup_{n \rightarrow \infty} \frac{\log \mathbb{E} \left[e^{\gamma \phi(Z_n)} \right]}{n} < \infty. \quad (157)$$

Then,

$$\limsup_{n \rightarrow \infty} \frac{\log \mathbb{E} \left[e^{\frac{\gamma\phi(Z_n)}{n}} \right]}{n} = \sup_{x \in \mathcal{X}} (\phi(x) - I(x)). \quad (158)$$

Lemma 7 (Moment convergence implies convergence in distribution [21, Theorem 30.2]). *Let $\{X_n\}_{n \geq 1}$ be a sequence of real-valued random variables and X a real-valued random variable. Suppose that:*

- 1) *For every integer $k \geq 1$, the k th moment $\mathbb{E}[X_n^k]$ exists for all sufficiently large n .*
- 2) *For every integer $k \geq 1$,*

$$\lim_{n \rightarrow \infty} \mathbb{E}[X_n^k] = \mathbb{E}[X^k].$$

- 3) *The distribution of X is uniquely determined by its moments (equivalently, Carleman's condition [21, Theorem 30.1] is satisfied).*

Then X_n converges in distribution to X , i.e.,

$$X_n \xrightarrow{D} X.$$

APPENDIX F PROOF OF CLAIM 1

The proof follows the line of treatment outlined in Appendix G. The key difference involves modifying the definition of W_i in Lemma 5 to

$$\sqrt{\frac{Pg_1^2}{MN}} \sum_{m=1}^M [\tilde{\mathcal{C}}^{(1)}]_m [\tilde{\mathbf{U}}_1^{(i)}]_m + \sqrt{\frac{Pg_2^2}{MN}} \sum_{m=M+1}^{2M} [\tilde{\mathcal{C}}^{(2)}]_m [\tilde{\mathbf{U}}_2^{(i)}]_m \quad (159)$$

in conducting the central limit theorem analysis. Here, $\tilde{\mathcal{C}}^{(i)} \stackrel{D}{=} \tilde{\mathcal{C}}$, $\tilde{\mathcal{C}}^{(1)}$ and $\tilde{\mathcal{C}}^{(2)}$ are independent, and $\tilde{\mathbf{U}}_\ell^{(i)}$ has i.i.d. $\text{Ber}(\alpha_\ell \mu / \beta)$ entries. The rest of the proof is handled as in the proof of Proposition 1 in [14], which is built along the lines outlined in Appendix G.

APPENDIX G PROOF OF CLAIM 2

To establish the convergence in distribution of the random variables V_N , by Lemma 7, it suffices to show that the moments converge, i.e., $\mathbb{E}[V_N^\ell] \rightarrow \mathbb{E}[V^\ell]$ for all positive integers ℓ . To compute these moments, we invoke the replica method stated in Assumption 1.

The expectation of the partition function can be expressed as

$$\begin{aligned} & \mathbb{E}_{\tilde{\mathbf{Y}}, \tilde{\mathcal{C}}} \left[\zeta^{(r)}(t; \tilde{\mathbf{Y}}, \tilde{\mathcal{C}}) \right] \\ &= \mathbb{E} \left[\int e^{t \prod_{i=1}^{\ell} [\tilde{\mathbf{U}}^{(i)}]_1} \Pr \left[\tilde{\mathbf{y}} | \tilde{\mathbf{U}}, \tilde{\mathcal{C}} \right] \prod_{j=1}^r \Pr \left[\tilde{\mathbf{y}} | \tilde{\mathbf{U}}^{(j)}, \tilde{\mathcal{C}} \right] d\tilde{\mathbf{y}} \right] \end{aligned} \quad (160)$$

$$= \mathbb{E} \left[\int e^{t \prod_{i=1}^{\ell} [\tilde{\mathbf{U}}^{(i)}]_1} (2\pi)^{-\frac{n(r+1)}{2}} \prod_{j=0}^r e^{-\frac{\|\tilde{\mathbf{y}} - \tilde{\mathbf{c}} \tilde{\mathbf{U}}_j\|^2}{2}} d\tilde{\mathbf{y}} \right]. \quad (161)$$

We observe that, since the channel is memoryless, and the codebook $\tilde{\mathcal{C}}$ is i.i.d., the integrals over each of the coordinate of $\tilde{\mathbf{y}}$ are identical. Using this observation, we can express (161) as follows:

$$\begin{aligned} & \mathbb{E} \left[\zeta^{(r)}(t; \tilde{\mathbf{Y}}, \tilde{\mathcal{C}}) \right] = \\ & \mathbb{E} \left[e^{t \prod_{i=1}^{\ell} \tilde{\mathbf{U}}_1^{(i)}} \left\{ (2\pi)^{-\frac{r}{2}} \int \mathbb{E}_{\tilde{\mathcal{C}}} \left[\prod_{j=0}^r e^{-\frac{(\tilde{\mathbf{y}} - \sqrt{P}\tilde{\mathbf{c}}^T \tilde{\mathbf{U}}^{(j)})^2}{2}} \right] \frac{d\tilde{\mathbf{y}}}{\sqrt{2\pi}} \right\}^N \right]. \end{aligned} \quad (162)$$

We define W_i as in Lemma 5. Using the central limit theorem, Edgeworth expansion as argued in [12, Appendix B], and invoking Lemma 5, we conclude that

$$\mathbb{E} \left[\zeta^{(r)}(t; \tilde{\mathbf{Y}}, \tilde{\mathcal{C}}) \right] = \mathbb{E} \left[e^{t \prod_{i=1}^{\ell} [\tilde{\mathbf{U}}_1^{(i)} + G^{(r)}(\mathcal{Q}) + O(M^{-1})]} \right] \quad (163)$$

where $G^{(r)}(\mathcal{Q})$ is as defined in (156). We can further use Lemma 6 to obtain

$$\lim_{M \rightarrow \infty} \log \mathbb{E} \left[\zeta^{(r)}(t; \tilde{\mathbf{Y}}, \tilde{\mathcal{C}}) \right] = \sup_{\mathcal{Q}} \left[\frac{1}{\beta} G^{(r)}(\mathcal{Q}) - I^{(r)}(t; \mathcal{Q}) \right] \quad (164)$$

where

$$I^{(r)}(t; \mathcal{Q}) = \sup_{\tilde{\mathcal{Q}}} \left[\text{Tr}(\tilde{\mathcal{Q}} \mathcal{Q}) - \log M^{(r)}(\tilde{\mathcal{Q}}) \right] \quad (165)$$

is the rate function corresponding to the measure

$$\mathbb{E} \left[\prod_{i=0}^r \prod_{j \leq i} \delta \left(\sum_{m=1}^M [\tilde{\mathbf{U}}^{(i)}]_m [\tilde{\mathbf{U}}^{(j)}]_m - \frac{M\mathcal{Q}}{P} \right) e^{t \prod_{k=1}^{\ell} [\tilde{\mathbf{U}}^{(k)}]_1} \right] \quad (166)$$

and \mathcal{Q} is defined in Lemma 5. Also,

$$M^{(r)}(\tilde{\mathcal{Q}}) = \mathbb{E} \left[\exp \left(t \prod_{i=1}^{\ell} [\tilde{\mathbf{U}}^{(i)}]_1 \right) e^{\mathcal{U}'^T \tilde{\mathcal{Q}} \mathcal{U}'} \right] \quad (167)$$

where $\mathcal{U}' = [[\tilde{\mathbf{U}}^{(0)}]_1, \dots, [\tilde{\mathbf{U}}^{(r)}]_1]^T$.

We next substitute (165) to (164), which yield the following optimization problem.

$$\sup_{\mathcal{Q}} \inf_{\tilde{\mathcal{Q}}} \left[\frac{1}{\beta} G^{(r)}(\mathcal{Q}) - \text{Tr}(\tilde{\mathcal{Q}} \mathcal{Q}) + \log M^{(r)}(\tilde{\mathcal{Q}}) \right]. \quad (168)$$

Let

$$\begin{aligned} T^{(r)}(\mathcal{Q}, \tilde{\mathcal{Q}}) &= -\frac{1}{2\beta} \log \det(\mathbf{I}_r + \Sigma \mathcal{Q}) - \text{Tr}(\tilde{\mathcal{Q}} \mathcal{Q}) \\ &\quad + \log \mathbb{E} \left[e^{\mathcal{U}'^T \tilde{\mathcal{Q}} \mathcal{U}'} \right] - \frac{1}{2\beta} \log(1+r) \\ &\quad - \frac{r}{2\beta} \log(2\pi). \end{aligned} \quad (169)$$

Fix a \mathcal{Q} . Then, the infimum with respect to $\tilde{\mathcal{Q}}$ satisfies

$$\mathcal{Q} = \frac{\mathbb{E} \left[\mathcal{U}' \mathcal{U}'^T e^{\mathcal{U}'^T \tilde{\mathcal{Q}} \mathcal{U}'} \right]}{\mathbb{E} \left[e^{\mathcal{U}'^T \tilde{\mathcal{Q}} \mathcal{U}'} \right]}. \quad (170)$$

Let the solution of (170) be $\tilde{\mathcal{Q}}^*(\tilde{\mathcal{Q}})$. By defining the expectation with respect to the tilted measure

$$\mu(\tilde{\mathcal{Q}}) = \frac{e^{\mathcal{U}'^\top \tilde{\mathcal{Q}} \mathcal{U}'}}{\mathbb{E} [e^{\mathcal{U}'^\top \tilde{\mathcal{Q}} \mathcal{U}'}]} \quad (171)$$

we can rewrite (170) as

$$\mathcal{Q} = \mathbb{E} [\mathcal{U}' \mathcal{U}'^\top | \tilde{\mathcal{Q}}]. \quad (172)$$

Now, with $\tilde{\mathcal{Q}} = \tilde{\mathcal{Q}}^*(\mathcal{Q})$, the supremum of the function $T^{(r)}(\mathcal{Q}, \tilde{\mathcal{Q}}^*(\mathcal{Q}))$ satisfies

$$\tilde{\mathcal{Q}} = -\frac{(\mathbf{I}_r + \Sigma \mathcal{Q})^{-1} \Sigma}{\beta}. \quad (173)$$

Equations (170) and (173) together form saddle point equations.

Now, we assume that the solutions of the saddle point equations satisfy some symmetry assumption. Such a symmetry assumption is referred to as the *replica symmetry assumption*. The work of [13], among others, make such a symmetry assumption to solve the saddle point equations. Specifically, in our case, we will assume that the joint solutions to (170) and (173) have the following structure:

$$\mathcal{Q}^* = \begin{bmatrix} p & q & q & \cdots & q \\ q & p & q & \cdots & q \\ q & q & p & \cdots & q \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ q & q & q & \cdots & p \end{bmatrix}_{(r+1) \times (r+1)} \quad (174)$$

$$\tilde{\mathcal{Q}}^* = \begin{bmatrix} g & f & f & \cdots & f \\ f & g & f & \cdots & f \\ f & f & g & \cdots & f \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ f & f & f & \cdots & g \end{bmatrix}_{(r+1) \times (r+1)}. \quad (175)$$

Under replica symmetry assumption,

$$G^{(r)}(\mathcal{Q}^*) = -\frac{r}{2} \log(2\pi) - \frac{r-1}{2} \log(1+\beta(p-q)) - \frac{1}{2} \log(1+\beta(p-q)+r(p-q)). \quad (176)$$

Next, we evaluate the moment generating function $M^{(r)}(\tilde{\mathcal{Q}}^*)$ as

$$M^{(r)}(\tilde{\mathcal{Q}}^*) = \mathbb{E} \left[e^{(\sum_{i=0}^r [\tilde{\mathcal{U}}]_i)^2 f + (g-f) \sum_{i=0}^r [\tilde{\mathcal{U}}]_i^2} \right] \quad (177)$$

which can be expressed as

$$M^{(r)}(\tilde{\mathcal{Q}}^*) = \mathbb{E} \left[\sqrt{\frac{f}{\pi}} \int e^{-fu^2 + (2f \sum_{i=0}^r [\tilde{\mathcal{U}}]_i)u + (g-f) \sum_{i=0}^r [\tilde{\mathcal{U}}]_i^2} du \right]. \quad (178)$$

Now, the rate function admits the form

$$I^{(r)}(\mathcal{Q}^*) = (r+1)(pg + rqf)$$

$$-\log \mathbb{E} \left[\int \sqrt{\frac{f}{\pi}} \mathbb{E} \left[e^{-f(-(u-[U]_0)^2 + g[U]_0^2)} \right] \cdot \left(\mathbb{E} \left[e^{2f[U]_1 + (g-f)[U]_1^2} \right] \right)^r du \right] \quad (179)$$

Next, using the replica trick, we obtain

$$-\lim_{M \rightarrow \infty} \mathbb{E} \left[\frac{1}{M} \log \zeta^{(r)}(t; \tilde{Y}, \tilde{\mathcal{C}}) \right] = -\lim_{M \rightarrow \infty} \frac{1}{M} \lim_{r \rightarrow 0} \frac{d}{dt} \left[\beta^{-1} G^{(r)}(\mathcal{Q}^*) - I^{(r)}(t; \tilde{\mathcal{Q}}^*) \right] \Big|_{t=0}. \quad (180)$$

Using (173), we conclude that

$$f = \frac{1}{2(1+\beta(p-q))} \quad (181)$$

and

$$g = 0. \quad (182)$$

To establish convergence to the limiting random variable, we next express the parameters above in terms of the corresponding conditional expectations. This analysis follows the approach outlined in [13], leading to relationships analogous to those in [13, eq. (132)–(135)]. Carleman's condition for moment determinacy [21, Chapter 30, Theorem 30.1], are satisfied as the random variables involved are bounded in $[0, 1]$. These together prove the convergence in distribution to a limiting random variable. The expression for the limiting random variable involves calculation of the parameter by solving the final resultant saddle point equation

$$\frac{1}{\eta} = 1 + P\beta \mathbb{E} \left[\left([\tilde{U}]_1 - \mathbb{E} \left[[\tilde{U}]_1 | \sqrt{P}[\tilde{U}]_1 + \frac{1}{\sqrt{\eta}} N \right] \right)^2 \right] \quad (183)$$

with $N \sim \mathcal{N}(0, 1)$, and $\eta = d^2/f$.