Finite-Blocklength and Error-Exponent Analyses for LDPC Codes in Point-to-Point and Multiple Access Communication

Yuxin Liu and Michelle Effros
Dept. of Elec. Eng., California Institute of Technology, Pasadena, CA 91125, USA. Emails: {yuxinl, effros}@caltech.edu

***Abstract*—This paper applies error-exponent and dispersion-style analyses to derive finite-blocklength achievability bounds for low-density parity-check (LDPC) codes over the point-to-point channel (PPC) and multiple access channel (MAC). The error-exponent analysis applies Gallager's error exponent to bound achievable symmetrical and asymmetrical rates in the MAC. The dispersion-style analysis begins with a generalization of the random coding union (RCU) bound from random code ensembles with i.i.d. codewords to random code ensembles in which codewords may be statistically dependent; this generalization is useful since the codewords of random linear codes such as LDPC codes are dependent. Application of the RCU bound yields finite-blocklength error bounds and asymptotic achievability results for both i.i.d. random codes and LDPC codes. For discrete, memoryless channels, these results show that LDPC codes achieve first- and second-order performance that is optimal for the PPC and identical to the best prior results for the MAC.**

I. Introduction

This paper (see [1] for an extended version) presents achievability bounds for the finite-blocklength performance of low-density parity-check (LDPC) codes over the point-to-point channel (PPC) and the multiple access channel (MAC). Proofs employ two types of analyses.

1) Error-exponent analyses generalize the techniques in [2] to demonstrate that average error probability ϵ decays exponentially in blocklength n with an error exponent bounded below by Gallager's error exponent. This technique yields tighter bounds when ϵ is very small.
2) Dispersion-style analyses generalize [3], bounding the log size of the codebook achievable for a given average error probability ϵ and blocklength n. This method yields tighter bounds when n is very small.

LDPC codes [4] are linear codes whose sparse parity-check matrices enable low complexity decoding strategies. While [4] includes some early analyses of code performance for LDPC codes, the results derived here build more directly on tools originally developed for general linear codes.

In [5, Section 6.2], Gallager describes a random coset parity-check matrix code ensemble. Each element of the parity-check matrix is chosen uniformly and independently from $\{0, 1\}$. The coset ensemble is formed by adding the same random vector to all codewords defined by the parity-check matrix. For PPCs with non-binary input alphabets, a "quantization" mapping maps one or more binary vectors to each channel input symbol. Gallager shows that the proposed code can achieve the capacity of an arbitrary discrete, memoryless PPC (DM-PPC) under maximum likelihood (ML) decoding.

In [6], Davey and MacKay generalize binary LDPC codes to finite field $\mathrm{GF}(q), q > 2$, showing empirically that q-ary codes can significantly improve binary code performance for binary-input PPCs under belief propagation decoding.

The standard $\mathrm{GF}(q)$ LDPC code ensemble employs a random Tanner graph that maps the vector of variable-node edge sockets to a random permutation of the vector of check-node edge sockets; edge weights are independent and identically distributed (i.i.d.) uniform on $\mathrm{GF}(q) \setminus \{0\}$. For the DM-PPC under ML decoding, [2] derives the first upper bound on the average error probability using Gallager's error exponent, showing that under sufficiently large connectivity and blocklength the random code has a high probability of achieving vanishing error probability at rates arbitrarily close to the channel capacity. Independently of [2], the authors in [7] analyze the performance over modulo-additive PPCs of two different $\mathrm{GF}(q)$-LDPC code ensembles under ML decoding. The error exponents for most codes in their design are bounded below asymptotically by the random coding error exponent [7].

While many studies focus on asymptotic LDPC behavior, the increasing prevalence of short blocklength codes (e.g., 5G codes, whose current blocklengths typically range from 100 to 20,000), motivate interest in finite-blocklength analyses.

In [8], Di et al. analyze the finite-blocklength performance of LDPC codes over the binary erasure channel (BEC), where finite-blocklength analysis boils down to a combinatorial problem. The paper derives the exact average bit- and block-erasure probability for a given regular ensemble of LDPC codes under iterative decoding and presents upper bounds on the average bit- and block-erasure probability for standard binary LDPC ensembles and the random parity-check ensemble under ML decoding. Similar studies include [9]–[13], which extend this approach to binary-input PPCs that may not be symmetric. While these analyses are non-asymptotic, they yield expressions that are either difficult to evaluate or empirical in nature.

Yang and Meng [14] study Gallager's independent, uniform parity-check ensemble and the standard binary LDPC

This material is based upon work supported in part by the National Science Foundation under Grant No. 1817241. The work of Y. Liu is supported in part by the Oringer Fellowship Fund in Information Science and Technology.

code ensemble under modified Feinstein's threshold decoding. Noting that codewords under these ensembles are not pairwise independent and therefore that Shannon-style random coding arguments do not apply, they derive new achievability bounds for memoryless binary-input, output-symmetric PPCs, demonstrating that Gallager's parity-check ensemble bound is asymptotically tight up to the second order and that the standard LDPC code ensemble is capacity achieving.

Less is known about LDPC codes over MACs [15]–[17].

This paper bounds the finite-blocklength performance of the standard $\mathrm{GF}(q)$ LDPC code ensemble under ML decoding using both the error-exponent approach from [2] and the dispersion-style approach from [3]. The error exponent analysis extends the result of [2] from the DM-PPC to the discrete, memoryless MAC (DM-MAC), refining the result with a non-asymptotic expansion from [5, Exercise 5.23]. The dispersion-style analysis derives a finite-blocklength error bound and asymptotic third-order achievability results for the DM-PPC and DM-MAC when the codewords are i.i.d., generalizes the random coding union (RCU) bound [3, Th. 16] to enable application to code ensembles with dependent codewords, and derives an upper bound for the quantized coset LDPC code ensemble, showing that LDPC codes achieve first- and second-order performance that is optimal for the DM-PPC and matches best prior results for the DM-MAC.

While practical LDPC code implementations typically employ sub-optimal iterative decoders, it is instructive to study how LDPC codes perform under ML decoding in order to understand the performance penalty of the low density encoder separately from that of the sub-optimal decoder. The main results are Theorems 1, 2, and 3, which bound the error performance of quantized coset LDPC codes using Gallager's error exponent and Theorems 5, 7, 8, and 9, which give finite-blocklength error bounds and asymptotic achievability results for the PPC and MAC first for i.i.d. codes and then for quantized coset LDPC codes.

II. Notation

Let $[k] \triangleq \{1, 2, \ldots, k\}$. For ordered set $\mathcal{A}$ and alphabets $\mathcal{X}_i$, $i \in \mathcal{A}$, let $\mathcal{X}_\mathcal{A} \triangleq \prod_{i\in\mathcal{A}} \mathcal{X}_i$, and let $P_{X_\mathcal{A}}$ be the distribution on $\mathcal{X}_\mathcal{A}$. Given a scalar function $f(\cdot)$, a set $\mathcal{Z} \subseteq \mathbb{R}^n$, a vector $\boldsymbol{v} \in \mathbb{R}^n$, and a scalar $a \in \mathbb{R}$, $a\mathcal{Z} + \boldsymbol{v} \triangleq \{a\boldsymbol{z} + \boldsymbol{v}, \boldsymbol{z} \in \mathcal{Z}\}$ and $f(\boldsymbol{v}) \triangleq (f(v_i), i \in [n])$. For ordered sets $\mathcal{A}$ and $\mathcal{B}$ with $\mathcal{A} \cap \mathcal{B} = \emptyset$ and any $x_\mathcal{A} \in \mathcal{X}_\mathcal{A}, x_\mathcal{B} \in \mathcal{X}_\mathcal{B}$, and $y \in \mathcal{Y}$

$$i(x_\mathcal{A}; y) \triangleq \log \frac{P_{Y|X_\mathcal{A}}(y|x_\mathcal{A})}{P_Y(y)} \tag{1}$$

$$i(x_\mathcal{A}; y|x_\mathcal{B}) \triangleq \log \frac{P_{Y|X_\mathcal{A},X_\mathcal{B}}(y|x_\mathcal{A}, x_\mathcal{B})}{P_{Y|X_\mathcal{B}}(y|x_\mathcal{B})}. \tag{2}$$

The mutual informations, dispersions, conditional dispersions, and third centered moments of information are

$$\begin{aligned}
I(P_{X_\mathcal{A}}) &\triangleq \mathbb{E}[i(X_\mathcal{A}; Y)] \\
I(P_{X_\mathcal{A}}|P_{X_\mathcal{B}}) &\triangleq \mathbb{E}[i(X_\mathcal{A}; Y|X_\mathcal{B}))] \\
V(P_{X_\mathcal{A}}) &\triangleq \mathrm{Var}[i(X_\mathcal{A}; Y)] \\
V(P_{X_\mathcal{A}}|P_{X_\mathcal{B}}) &\triangleq \mathrm{Var}[i(X_\mathcal{A}; Y|X_\mathcal{B})] \\
V^Y(P_{X_\mathcal{A}}) &\triangleq \mathrm{Var}[i(X_\mathcal{A}; Y)|Y] \\
V^Y(P_{X_\mathcal{A}}|P_{X_\mathcal{B}}) &\triangleq \mathrm{Var}[i(X_\mathcal{A}; Y|X_\mathcal{B})|Y] \\
T(P_{X_\mathcal{A}}) &\triangleq \mathbb{E}[|i(X_\mathcal{A}; Y) - I(P_{X_\mathcal{A}})|^3] \\
T(P_{X_\mathcal{A}}|P_{X_\mathcal{B}}) &\triangleq \mathbb{E}[|i(X_\mathcal{A}; Y|X_\mathcal{B}) - I(P_{X_\mathcal{A}}|P_{X_\mathcal{B}})]|^3].
\end{aligned}$$

III. Quantized Coset LDPC Codes

For any prime power q and finite field $\mathrm{GF}(q)$, a quantized coset $\mathrm{GF}(q)$-LDPC code is defined by a standard LDPC encoder, a coset vector $\boldsymbol{v}$, and a quantizer. (See Fig. 1.)

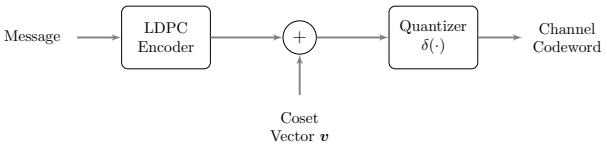

Fig. 1. Encoding of Quantized Coset LDPC Code

Definition 1: A **standard $\mathrm{GF}(q)$-LDPC code** is defined by a bipartite Tanner graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ with n variable nodes, r check nodes, and undirected edge set $\mathcal{E} \subseteq [n] \times [r]$. For each $(i, j) \in \mathcal{E}$, edge (i, j) connects the ith variable node and jth check node; edge weight $g_{i,j}$ is a constant in $\mathrm{GF}(q) \setminus \{0\}$. The neighborhood of $j \in [r]$ is $\mathcal{N}(j) \triangleq \{i : (i, j) \in \mathcal{E}\}$.

The n variable nodes hold a column vector $\boldsymbol{u}$ from $\mathrm{GF}(q)^n$; $\boldsymbol{u}$ is a **codeword** if it satisfies all check nodes, giving

$$\sum_{i\in\mathcal{N}(j)} g_{i,j} u_i = 0 \quad \forall j \in [r],$$

where the linear equation operates in $\mathrm{GF}(q)$. The set of all codewords constitute the code's **codebook**

$$\boldsymbol{c} = \{\boldsymbol{c}_1, \ldots, \boldsymbol{c}_M\} \subseteq \mathrm{GF}(q)^n.$$

Size $M = |\boldsymbol{c}|$ exceeds q^{nR} for **design rate** $R \triangleq 1 - \frac{r}{n}$ q-ary symbols per channel use if the parity-check matrix corresponding to the Tanner graph does not have full rank.

Following [18], [19], we do not transmit codewords from the LDPC encoder but instead apply quantized coset coding.

Definition 2: The **coset $GF(q)$-LDPC code** adds constant **coset vector $\boldsymbol{v}$** (component-wise in $\mathrm{GF}(q)$) to each codeword of an LDPC codebook $\boldsymbol{c}$, giving coset LDPC codebook

$$\boldsymbol{c} + \boldsymbol{v} = \{\boldsymbol{c}_i + \boldsymbol{v}, i \in [M]\}.$$

Definition 3: The **quantized coset $\mathrm{GF}(q)$-LDPC code** applies **quantizer** $\delta : \mathrm{GF}(q) \to \mathcal{U}$, where $\mathcal{U}$ is the channel input alphabet, to each codeword of an LDPC coset codebook $\boldsymbol{c} + \boldsymbol{v}$, giving quantized coset codebook

$$\delta(\boldsymbol{c} + \boldsymbol{v}) = \{\delta(\boldsymbol{c}_i + \boldsymbol{v}), i \in [M]\}.$$

The quantizer operates symbol-wise, mapping each symbol from $GF(q)$ to a symbol from $\mathcal{U}$ as

$$\delta(\boldsymbol{c}_i + \boldsymbol{v}) \triangleq [\delta(\boldsymbol{c}_i[j] + \boldsymbol{v}[j])]_{j\in[n]} = [\delta((\boldsymbol{c}_i + \boldsymbol{v})[j])]_{j\in[n]}.$$

Quantizer δ allows a code on $\mathrm{GF}(q)$ to approximate any rational probability mass function P_U for which $P_U(u)$ is an

integer multiple N_u of $1/q$ for all $u \in \mathcal{U}$. This is achieved by mapping N_u elements to each channel input symbol $u \in \mathcal{U}$.

We consider a random ensemble of quantized coset $\mathrm{GF}(q)$-LDPC codes. In our Tanner graphs, all left and right nodes have degrees λ and ρ, respectively. Edges with weights chosen i.i.d. uniform on $\mathrm{GF}(q) \setminus \{0\}$ map the vector of variable-node edge sockets to a random permutation of the vector of check-node edge sockets. If the parity-check matrix corresponding to the Tanner graph is not full-rank, the code design restricts the operational rate to equal the design rate by choosing exactly q^{nR} codewords for use in coding. We use $\mathrm{LDPC}(\lambda, \rho; n)$ to denote the single-user ensemble from the random (λ, ρ) LDPC graph after uniform random codeword selection.

IV. Error Exponent Bound for LDPC codes in MAC

To simplify notation, the following arguments treat a symmetrical K-transmitter DM-MAC (S-DM-K-MAC) and a general 2-transmitter DM-MAC (DM-2-MAC) under ML decoding. Both arguments generalize to the DM-K-MAC ($K \geq 2$).

For the S-DM-K-MAC, all transmitters employ the same random codebook from the $\mathrm{LDPC}(\lambda, \rho; n)$ ensemble, each offset by an independent random coset vector $\boldsymbol{v}_k, k \in [K]$, and followed by the same quantizer $\delta(\cdot)$. We denote the MAC ensemble before and after applying the random coset matrix $\boldsymbol{v} = [\boldsymbol{v}_1 \boldsymbol{v}_2 \cdots \boldsymbol{v}_K]$ and quantizer δ by $\mathrm{LDPC}_K(\lambda, \rho; n)$ and $\mathrm{LDPC}_K(\lambda, \rho, \delta; n)$, respectively.

For a fixed LDPC graph with $M = q^{nR}$ codewords, the **single-transmitter codebook** for each transmitter $k \in [K]$ is denoted by $\boldsymbol{c}_{(k)} = \{\boldsymbol{c}_1, \ldots, \boldsymbol{c}_M\} \subseteq \mathrm{GF}(q)^n$. The **MAC codebook** is the set of codematrices $\boldsymbol{d} = \{\boldsymbol{d}_{\boldsymbol{m}} : \boldsymbol{m} \in [M]^K\} \subseteq \mathrm{GF}(q)^{n \times K}$, where $\boldsymbol{d}_{\boldsymbol{m}} = (\boldsymbol{c}_{m(1)}, \ldots, \boldsymbol{c}_{m(K)})$ for each $\boldsymbol{m} = (m(1), \ldots, m(K))$. The MAC coset codebook is $\boldsymbol{d} + \boldsymbol{v}$, and the quantized coset codebook is $\delta(\boldsymbol{d} + \boldsymbol{v})$.

We first describe the distribution over the types of codematrices. For any matrix $\boldsymbol{a} \in \mathrm{GF}(q)^{n \times K}$, let $\mathcal{T}_{\mathcal{Q}}^n(\boldsymbol{a})$ denote the **type** that results when we view $\boldsymbol{a}$ as a list of n elements from alphabet $\mathcal{Q} \stackrel{\triangle}{=} \mathrm{GF}(q)^K$. The **set of possible types** is

$$\mathcal{T}_{\mathcal{Q}}^n \stackrel{\triangle}{=} \{\mathcal{T}_{\mathcal{Q}}^n(\boldsymbol{a}) : \boldsymbol{a} \in \mathrm{GF}(q)^{n \times K}\} \subset \mathbb{Z}_+^{|\mathcal{Q}|}.$$

For any MAC codebook $\boldsymbol{d}$, the **spectrum of codebook** $\boldsymbol{d}$ is $\boldsymbol{S}_{\boldsymbol{d}}^n = (S_{\boldsymbol{d}}^n(\boldsymbol{t}) : \boldsymbol{t} \in \mathcal{T}_{\mathcal{Q}}^n)$, where for any type $\boldsymbol{t} \in \mathcal{T}_{\mathcal{Q}}^n$, the number of codematrices of type $\boldsymbol{t}$ in MAC codebook $\boldsymbol{d}$ is

$$S_{\boldsymbol{d}}^n(\boldsymbol{t}) = \sum_{\boldsymbol{m}} \mathbb{1}(\mathcal{T}_{\mathcal{Q}}^n(\boldsymbol{d}_{\boldsymbol{m}}) = \boldsymbol{t}). \tag{3}$$

The **ensemble-average spectrum** of random codebook $\boldsymbol{D}$ is $\overline{\boldsymbol{S}}^n = E_{\boldsymbol{D}}[\boldsymbol{S}_{\boldsymbol{D}}^n] = (\overline{S}^n(\boldsymbol{t}) : \boldsymbol{t} \in \mathcal{T}_{\mathcal{Q}}^n)$.

Given a DM-K-MAC $(\mathcal{X} = \mathcal{U}^K, P_{Y|X}, \mathcal{Y})$ and quantizer $\delta(\cdot)$, let $\boldsymbol{\mathcal{D}} = (\mathcal{D}(g) : g \in \mathcal{Q})$, where $\mathcal{D}(g)$ is the extension of the Bhattacharyya parameter to non-binary channels

$$\mathcal{D}(g) \stackrel{\triangle}{=} \frac{1}{q^K} \sum_{g' \in \mathcal{Q}} \sum_{y} \sqrt{P_{Y|X}(y|\delta(g')) P_{Y|X}(y|\delta(g'+g))}.$$

For any type $\boldsymbol{t} \in \mathcal{T}_{\mathcal{Q}}^n$, define

$$\boldsymbol{\mathcal{D}}^{\boldsymbol{t}} \stackrel{\triangle}{=} \prod_{g \in \mathcal{Q}} \mathcal{D}(g)^{t(g)}, \;\; B(n, \boldsymbol{t}) \stackrel{\triangle}{=} \frac{n!}{\prod_{g \in \mathcal{Q}} t_g!}. \tag{4}$$

Theorem 1: Let $P_{Y|X}$ be the transition probability for an S-DM-K-MAC $(\mathcal{X} = \mathcal{U}^K, P_{Y|X}, \mathcal{Y})$. Let $(C, \ldots, C)$ be the MAC's maximal symmetrical rate vector, and fix $\boldsymbol{R} = (R, \ldots, R)$ with $R < C$. Let P_U be a pmf on $\mathcal{U}$ with $P_U(u) = N_u/q$ for each $u \in \mathcal{U}$, and let $\delta : \mathrm{GF}(q) \to \mathcal{U}$ be a quantization matched to P_U. Consider the $\mathrm{LDPC}_K(\lambda, \rho, \delta; n)$ ensemble of blocklength n, rate $\boldsymbol{R}$, and ensemble-average spectrum $\overline{\boldsymbol{S}}^n$. For any set $\mathrm{T} \subseteq \mathcal{T}_{\mathcal{Q}}^n$ and blocklength n, the ensemble-average error probability under ML decoding is

$$E[P_e^{(n)}] \leq \sum_{\boldsymbol{t} \in \mathrm{T}} \overline{S}^n(\boldsymbol{t}) \boldsymbol{\mathcal{D}}^{\boldsymbol{t}} + q^{-nE_p(KR + (\log \alpha_{\text{MAC}})/n)}, \tag{5}$$

where $E_p(\cdot)$ is Gallager's error exponent under $P_X = P_U^K$

$$E_p(R) \stackrel{\triangle}{=} \max_{0 \leq \rho \leq 1} [E_0(\rho, P_X) - \rho R]$$

$$E_0(\rho, P_X) \stackrel{\triangle}{=} -\log \sum_y \left[\sum_{x \in \mathcal{U}^K} P_X(x) P_{Y|X}(y|x)^{1/(1+\rho)} \right]^{1+\rho}$$

$$\alpha_{\text{MAC}} \stackrel{\triangle}{=} \max_{\boldsymbol{t} \in \mathrm{T}^c} \frac{\overline{S}^n(\boldsymbol{t})}{(M^K - 1) B(n, \boldsymbol{t}) q^{-nK}}.$$

Here $\mathrm{T}^c \stackrel{\triangle}{=} \mathcal{T}_{\mathcal{Q}}^n \setminus \mathrm{T} \setminus \{\mathcal{T}_{\mathcal{Q}}^n(\boldsymbol{0})\}$, where $\mathcal{T}_{\mathcal{Q}}^n(\boldsymbol{0})$ is the type of the all zero codematrix, and $M = q^{nR}$.

Optimizing over T for each blocklength n makes the bound as tight as possible. Applying expurgation [2] to remove codes with minimum distance less than σn gives Theorem 2.

Theorem 2: Fix $\epsilon^* > 0$. Under the definitions of Theorem 1, for large enough ρ and n and a matched choice of λ, the ensemble-average error probability for expurgated ensemble $\mathrm{LDPC}_K - \mathrm{Ex}_\sigma(\lambda, \rho, \delta; n)$ under ML decoding satisfies

$$E_{\text{ex}}[P_e^{(n)}] \leq q^{-nE_p(KR + \epsilon^*)}.$$

Bounding ϵ^* as a function of κ, where $\kappa = \frac{\rho}{n}$, bounds the code's density-performance tradeoff. If $\kappa < \frac{q-1}{q}$ decays no more quickly than $\boldsymbol{\Theta}(\frac{\log n}{n})$, then the minimal achievable rate offset ϵ^* decays as $O(\frac{\log n}{n})$. (See [1, Th. 2].) Selecting P_U to approximate the capacity-achieving input distribution makes $E_p(R) > 0$ for any $R < C$. When the capacity-achieving input distribution is not an integer multiple of $\frac{1}{q}$ for some small q, then a large q may be required to make this approximation accurate. Thus by Theorem 2, our proposed code design is asymptotically capacity achieving for ρ and q large enough.

Given distribution $P_{Y|X_1,X_2} P_{X_1} P_{X_2}$, let

$$\mathcal{R}(P_{X_1}, P_{X_2}) = \{(R_1, R_2) : R_1 < I(X_1; Y|X_2), \\ R_2 < I(X_2; Y|X_1), R_1 + R_2 < I(X_1, X_2; Y)\}.$$

Theorem 3: For DM-2-MAC $(\mathcal{X} = \mathcal{X}_1 \times \mathcal{X}_2, P_{Y|X_1,X_2}, \mathcal{Y})$, let P_{X_i} be a pmf on $\mathcal{X}_i$ with $P_{X_i}(x_i) = N_{x_i}/q$ for all $x_i \in \mathcal{X}_i$. Let $\delta_i : \mathrm{GF}(q) \to \mathcal{X}_i$ be the quantizer for P_{X_i}, $i \in \{1, 2\}$. If transmitter i employs ensemble $\mathrm{LDPC}(\lambda_i, \rho_i, \delta_i; n)$ with independent coset vector $\boldsymbol{v}_i$ such that rate vector $(R_1, R_2) \in \mathcal{R}(P_{X_1}, P_{X_2})$, then for any blocklength n, the ensemble-average error probability under ML decoding is

$$E[P_e^{(n)}] \leq q^{-nE_{p_1}(R_1 + \frac{\log \alpha_1}{n})} + q^{-nE_{p_2}(R_2 + \frac{\log \alpha_2}{n})} \\ + q^{-nE_{p_{12}}(R_1 + R_2 + \frac{\log \alpha_{12}}{n})}, \tag{6}$$

where $E_{p_1}(\cdot), E_{p_2}(\cdot)$, and $E_{p_{12}}(\cdot)$ are Gallager's error exponents for the input distribution P_{X_1}, P_{X_2}, and $P_X = P_{X_1}P_{X_2}$ (see [1, Th. 4] for details), $\alpha_{12} = \alpha_1\alpha_2$, and

$$\alpha_i = \max_{\boldsymbol{t}\in\mathcal{T}_q^n\setminus\{\mathcal{T}_q^n(\mathbf{0})\}} \frac{\overline{S}_i^n(\boldsymbol{t})}{(M_i-1)B(n,\boldsymbol{t})q^{-n}},\ i\in\{1,2\}. \quad (7)$$

Here $\overline{S}_i^n(\boldsymbol{t})$ is the LDPC$(\lambda_i,\rho_i;n)$ ensemble-average number of type-$\boldsymbol{t}$ vectors and $M_i = q^{nR_i}$ for $i\in\{1,2\}$.

From [20], all error exponents, $E_{p_1}(R_1), E_{p_2}(R_2)$, and $E_{p_{12}}(R_1+R_2)$, are positive when rate pair $(R_1,R_2)\in\mathcal{R}(P_{X_1},P_{X_2})$. However, restricting the ensemble from standard i.i.d. random codes to LDPC codes incurs rate offset penalties $\frac{\log\alpha_1}{n}$, $\frac{\log\alpha_2}{n}$, and $\frac{\log\alpha_{12}}{n}$ in R_1, R_2, and R_1+R_2. Again, under expurgation these rate offsets become arbitrarily small with large enough n, ρ_1, and ρ_2. Therefore, the proposed quantized coset-shifted LDPC MAC codes can achieve any rate pair in $\mathcal{R}(P_{X_1},P_{X_2})$. Taking the union of $\mathcal{R}(P_{X_1},P_{X_2})$ over all P_{X_1},P_{X_2} achievable with increasing values of prime power q and incorporating time sharing [21] then achieves any rate pair in the convex closure of $\cup_{P_{X_1}P_{X_2}}\mathcal{R}(P_{X_1},P_{X_2})$.

To understand how our LDPC error exponent analysis compares to other results, consider for a moment the DM-PPC. In [3, Th. 50], Polyanskiy et al. bound the achievable rate R with error probability ϵ and blocklength n as

$$R \geq C - \sqrt{\frac{V_{\min}}{n}}Q^{-1}(\epsilon) + O\left(\frac{1}{n}\right), \quad (8)$$

where $V_{\min} \leq 2\log_2^2(\min\{|\mathcal{X}|,|\mathcal{Y}|\}) - C^2$ is the minimal channel dispersion over all capacity-C-achieving channel input distributions [3]. In [5, Exercise 5.23] and [5, Th. 5.6.2., Corollary 1], Gallager gives the achievability result

$$R \geq C - \sqrt{\frac{8/e^2 + 2(\log_e|\mathcal{Y}|)^2 - 2R_{cr}^2}{n}\log_e\frac{1}{\epsilon}} \quad (9)$$

for the i.i.d. random code, where R_{cr} is the critical rate [5, Eq. (5.6.30)]. Comparing (8) with (9), the dispersion-style analysis gives a tighter coefficient for the $\sqrt{1/n}$ term, but the error-exponent analysis is more accurate at very small ϵ.

The error exponent analysis gives a sub-optimal $\sqrt{1/n}$ term even for i.i.d.-P_X codes. Specializing our analysis to the PPC, we find a penalty for using LDPC codes instead of i.i.d. P_X codes is a rate offset $\frac{\log\alpha}{n}$ in the error exponent, which is $O(\frac{\log n}{n})$ for large enough ρ after expurgation (see [1, Th. 2]).

V. Random Coding Union (RCU) Bound for I.I.D. and LDPC codes in PPC and MAC Communication

A. RCU Bound for the I.I.D. Code on the PPC

Theorem 4 generalizes [3, Th. 16] from i.i.d. to identically distributed (not necessarily independent) codewords.

Theorem 4: (RCU allowing dependence) Given a PPC and marginal distribution P_X, consider a code ensemble with M codewords drawn according to $P_{X(1),X(2),\ldots,X(M)}$ such that

$$P_{X(i)} = P_X,\ \forall i\in[M] \quad (10)$$

$$P_{X(\mathcal{A})} = P_{X(\mathcal{B})},\ \forall\mathcal{A},\mathcal{B}\subseteq[M] \text{ s.t. } |\mathcal{A}| = |\mathcal{B}|. \quad (11)$$

Let $P_{X\bar{X}Y}(a,b,c) = P_{X\bar{X}}(a,b)P_{Y|X}(c|a)$, $P_{X\bar{X}}(a,b) = P_{X(1)X(2)}(a,b)$. Under ML decoding, ensemble average error probability ϵ satisfies

$$\epsilon \leq \mathbb{E}\left[\min\{1,(M-1)\Pr[i(\bar{X};Y)\geq i(X;Y)|X,Y]\}\right].$$

Similar to [22, Th. 5], applying Theorem 4, the Berry-Esséen inequality, and [3, Lemma 47] gives Theorem 5, which improves the third-order term of [3, Theorem 49].

Theorem 5: (Random coding finite-blocklength bound and asymptotic third-order-optimal achievability for the PPC). Consider a DM-PPC $P_{Y|X}$ and capacity achieving distribution P_X. If each symbol of each codeword is drawn i.i.d.-P_X and

$$I(P_X)>0, V(P_X)>0, V^Y(P_X)>0, T(P_X)<\infty, \quad (12)$$

then there exists a blocklength-n code with M codewords and average error probability ϵ such that for any $n\geq 1$

$$\epsilon \leq \mathbb{E}\left[\min\left\{1, M\frac{A(P_X)}{\sqrt{n}}\exp(-i(X^n;Y^n))\right\}\right], \quad (13)$$

and for large enough n

$$\frac{\log M}{n} \geq C - \sqrt{\frac{V(P_X)}{n}}Q^{-1}(\epsilon) + \frac{\log n}{2n} - O\left(\frac{1}{n}\right), \quad (14)$$

where $C_0 = 0.5583$ is the Berry-Esséen constant and

$$A(P_X) \triangleq 2\left(\frac{\log 2}{\sqrt{2\pi V(P_X)}} + 2\frac{C_0 T(P_X)}{V(P_X)^{3/2}}\right). \quad (15)$$

For proof details, see [1, Th. 11]. The achievability result in Theorem 5 is optimal up to the third order by [3, Th. 48].

B. RCU Bound for the I.I.D. Code on the 2-MAC

Theorem 6 extends the RCU bound to the 2-MAC.

Theorem 6: (RCU allowing dependence for the 2-MAC) Given P_{X_1} and P_{X_2}, consider an ensemble of 2-MAC codes with $M_1\times M_2$ codeword pairs drawn according to any $P_{X_1(1)\ldots X_1(M_1)}P_{X_2(1)\ldots X_2(M_2)}$ with

$$P_{X_i(m_i)} = P_{X_i},\ \forall i\in[2], m_i\in[M_i]$$
$$P_{X_i(\mathcal{A})} = P_{X_i(\mathcal{B})},\ \forall i\in[2],\mathcal{A},\mathcal{B}\subseteq[M_i] \text{ s.t. } |\mathcal{A}| = |\mathcal{B}|.$$

For all $(x_1,x_2,\bar{x}_1,\bar{x}_2,y)\in(\mathcal{X}_1\times\mathcal{X}_2)^2\times\mathcal{Y}$, let

$$P_{X_i\bar{X}_i}(x_i,\bar{x}_i) = P_{X_i(1)X_i(2)}(x_i,\bar{x}_i)\ \ \forall i\in[2]$$
$$P_{X_1X_2\bar{X}_1\bar{X}_2Y}(x_1,x_2,\bar{x}_1,\bar{x}_2,y) = \left(\prod_{i=1}^2 P_{X_i\bar{X}_i}(x_i,\bar{x}_i)\right)P_{Y|X_1,X_2}(y|x_1,x_2).$$

The ensemble average error probability under ML decoding is

$$\epsilon \leq \mathbb{E}[\min\{1, V_1+V_2+V_{12}\}], \quad (16)$$

where

$$V_{12} = (M_1-1)(M_2-1)\cdot\Pr[i(\bar{X}_1,\bar{X}_2;Y)\geq i(X_1,X_2;Y)|X_1,X_2,Y]$$
$$V_1 = (M_1-1)\Pr[i(\bar{X}_1;Y|X_2)\geq i(X_1;Y|X_2)|X_1,X_2,Y]$$
$$V_2 = (M_2-1)\Pr[i(\bar{X}_2;Y|X_1)\geq i(X_2;Y|X_1)|X_1,X_2,Y].$$

Theorem 7 presents an asymptotic achievability result based on Theorem 6. Our argument follows the source coding proof in [22, Th. 11] and is similar to [23]. Denote for brevity

$$E_1 \triangleq M_1 \frac{F_1}{\sqrt{n}} \exp(-i(X_1^n; Y^n|X_2^n)) \tag{17}$$

$$E_2 \triangleq M_2 \frac{F_2}{\sqrt{n}} \exp(-i(X_2^n; Y^n|X_1^n)) \tag{18}$$

$$E_{12} \triangleq M_1 M_2 \frac{F_{12}}{\sqrt{n}} \exp(-i(X_1^n, X_2^n; Y^n)), \tag{19}$$

where F_1, F_2, and F_{12} are extensions of $A(P_X)$ in (15), see [1, Th. 14] for details. Let $\boldsymbol{Z}$ be a mean-zero, covariance-$\boldsymbol{K}_{\boldsymbol{ZZ}}$ Gaussian random vector in $\mathbb{R}^d$, and define

$$Q_{\text{inv}}(\boldsymbol{K}_{\boldsymbol{ZZ}}, \epsilon) \triangleq \left\{ \boldsymbol{z} \in \mathbb{R}^d : \Pr[\boldsymbol{Z} \leq \boldsymbol{z}] \geq 1 - \epsilon \right\}. \tag{20}$$

Theorem 7: (Random coding finite-blocklength bound and third-order achievability for the DM-2-MAC). Consider a DM-2-MAC $(\mathcal{X}_1 \times \mathcal{X}_2, P_{Y|X_1,X_2}, \mathcal{Y})$. If each symbol of each codeword for transmitter i is drawn i.i.d.-P_{X_i}, $i \in \{1, 2\}$ and

$$V^Y(P_{X_1}|P_{X_2}) > 0, V^Y(P_{X_2}|P_{X_1}) > 0, V^Y(P_{X_1}, P_{X_2}) > 0$$
$$T(P_{X_1}|P_{X_2}) < \infty, T(P_{X_2}|P_{X_1}) < \infty, T(P_{X_1}, P_{X_2}) < \infty,$$

then there exists a blocklength-n MAC code with $M_1 \times M_2$ codewords and average error probability ϵ such that for each blocklength n,

$$\epsilon \leq \mathbb{E}\left[\min\left\{1, E_1 + E_2 + E_{12}\right\}\right], \tag{21}$$

and for large enough blocklength n

$$\bar{\boldsymbol{R}} \in \bar{\boldsymbol{I}} - \frac{Q_{\text{inv}}(\mathrm{V}, \epsilon)}{\sqrt{n}} + \frac{\log n}{2n}\mathbf{1} - O\left(\frac{1}{n}\right)\mathbf{1}, \tag{22}$$

where E_1, E_2, and E_{12} are defined in (17)-(19), Q_{inv} is defined in (20), $\bar{\boldsymbol{R}} = [R_1, R_2, R_1 + R_2]$, and $\bar{\boldsymbol{I}}$ and V are the expectation and covariance matrix of $[i(X_1; Y|X_2), i(X_2; Y|X_1), i(X_1, X_2; Y)]$.

C. RCU Bound for the LDPC Code Ensemble on the DM-PPC

We next apply Theorem 4 to the $\mathrm{LDPC}(\lambda, \rho, \delta; n)$ ensemble. The LDPC achievability result in Theorem 8, below, matches the bound for the unrestricted code design (Theorem 5) in its first- and second-order terms. The penalty $\frac{\log \alpha}{n}$ is $O(\frac{\log n}{n})$ for large enough ρ after expurgation (see [1, Appendix D]), where $\alpha = \alpha_1\Big|_{(\lambda_1,\rho_1)=(\lambda,\rho)}$ and α_1 is from (7). The question of whether the penalty in the third-order term results from the LDPC structure or the bounding technique is currently under investigation.

Theorem 8: (LDPC ensemble finite-blocklength bound, and second-order-optimal achievability for the DM-PPC). Consider a DMC with channel transition probability $P_{Y|X}$ and capacity achieving distribution P_X. There exist LDPC parameters (λ, ρ) for which the $\mathrm{LDPC}(\lambda, \rho, \delta; n)$ ensemble, with $\delta(\cdot)$ chosen to approximate P_X, contains at least one code with average error probability ϵ such that for any blocklength n

$$\epsilon \leq \mathbb{E}\left[\min\left\{1, \alpha M \frac{A(P_X)}{\sqrt{n}} \exp(-i(X^n; Y^n))\right\}\right], \tag{23}$$

and for large enough blocklength n and coding parameter q with $R = 1 - \frac{\lambda}{\rho} = \frac{\log M}{n}$

$$R \geq C - \sqrt{\frac{V(P_X)}{n}} Q^{-1}(\epsilon) + \frac{\log n}{2n} - \frac{\log \alpha}{n} - O\left(\frac{1}{n}\right) \tag{24}$$

provided the moment assumptions in (12) are satisfied.

Due to the difficulty of evaluating the exact value of α, expression (23) is only computable for small n (e.g., $n < 100$). However, expression (24) becomes increasingly accurate as n increases ($n \to \infty$). Analysis in [1, Th. 2] demonstrates $\frac{\log \alpha}{n}$ in (24) behaves as $O(\frac{\log n}{n})$ when $\rho = \kappa n$, provided that κ decays no more quickly than $\boldsymbol{\Theta}(\frac{\log n}{n})$.

A brief proof sketch follows; details appear in [1, Th. 15]. The proof for i.i.d. codes requires modification for use on the LDPC code ensemble due in part to the codeword dependence observed in all linear code ensembles. We replace the original RCU bound [3, Th. 16] by Theorem 4, which applies by the LDPC code ensemble's symmetry across codewords. While our achievability proof for i.i.d. codes (Theorem 5) relies on

$$\Pr[\bar{X}^n = \bar{x}^n | X^n, Y^n] = \Pr[\bar{X}^n = \bar{x}^n],$$

for the $\mathrm{LDPC}(\lambda, \rho, \delta; n)$ ensemble, we apply

$$\Pr[\bar{X}^n = \bar{x}^n | X^n, Y^n] \leq \alpha \Pr[\bar{X}^n = \bar{x}^n]. \tag{25}$$

Equation (25) provides a bound on the effect of the LDPC code ensemble's codeword dependence.

Although the symbols within a codeword are also not independent under the $\mathrm{LDPC}(\lambda, \rho; n)$ ensemble, they become independent after adding the uniformly distributed coset vector $\boldsymbol{v}$. Finally, applying the Berry-Esséen Theorem and [3, Lemma 47] gives the achievability bound in (24).

D. RCU Bound for the LDPC Code Ensemble on DM-2-MAC

Just as Theorem 8 extends the proof of Theorem 5 from i.i.d. to LDPC PPC code design, Theorem 9 extends Theorem 7 from i.i.d. to LDPC MAC code design.

Theorem 9: (Finite-blocklength bound and second-order best-prior achievability for the LDPC ensemble on the DM-2-MAC). Consider a DM-2-MAC $(\mathcal{X}_1 \times \mathcal{X}_2, P_{Y|X_1,X_2}, \mathcal{Y})$. Let transmitter i employ the $\mathrm{LDPC}(\lambda_i, \rho_i, \delta_i; n)$ ensemble with coset vector $\boldsymbol{v}_i$, and quantizer $\delta_i(\cdot)$ chosen to approximate P_{X_i} for $i \in \{1, 2\}$. Then there exist LDPC parameters (λ_1, ρ_1) and (λ_2, ρ_2) for which the $\mathrm{LDPC}(\lambda_1, \rho_1, \delta_1; n) \times \mathrm{LDPC}(\lambda_2, \rho_2, \delta_2; n)$ ensemble contains at least one MAC code with average error ϵ such that for any blocklength n

$$\epsilon \leq \mathbb{E}\left[\min\left\{1, \alpha_1 E_1 + \alpha_2 E_2 + \alpha_1 \alpha_2 E_{12}\right\}\right], \tag{26}$$

and for large enough n and coding parameter q

$$\bar{\boldsymbol{R}} \in \bar{\boldsymbol{I}} - \frac{Q_{\text{inv}}(\mathrm{V}, \epsilon)}{\sqrt{n}} + \frac{\log n}{2n}\mathbf{1} - \frac{\log \bar{\boldsymbol{\alpha}}}{n}\mathbf{1} - O\left(\frac{1}{n}\right)\mathbf{1}, \tag{27}$$

provided that the moment assumptions in Theorem 7 are satisfied. Here $\bar{\boldsymbol{\alpha}} = [\alpha_1, \alpha_2, \alpha_1\alpha_2]$, α_1 and α_2 are defined in (7), and the definitions of all other parameters are the same as those in Theorem 7.

REFERENCES

[1] Y. Liu and M. Effros. Finite-blocklength and error-exponent analysis for LDPC codes in point-to-point and multiple access communication. [Online]. Available: https://arxiv.org/abs/2005.06428

[2] A. Bennatan and D. Burshtein, "On the application of LDPC codes to arbitrary discrete-memoryless channels," *IEEE Trans. Inf. Theory*, vol. 50, no. 3, pp. 417–438, March 2004.

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

[4] R. Gallager, "Low-density parity-check codes," *IEEE Trans. Inf. Theory*, vol. 8, no. 1, pp. 21–28, 1962.

[5] R. Gallager, *Information Theory and Reliable Communication*. Springer, 1968, vol. 2.

[6] M. C. Davey and D. J. C. MacKay, "Low density parity check codes over gf(q)," in *Proc. IEEE Inf. Theory Workshop*, June 1998, pp. 70–71.

[7] U. Erez and G. Miller, "The ML decoding performance of LDPC ensembles over Z/sub q/," *IEEE Trans. Inf. Theory*, vol. 51, no. 5, pp. 1871–1879, May 2005.

[8] C. Di, D. Proietti, I. E. Telatar, T. Richardson, and R. Urbanke, "Finite-length analysis of low-density parity-check codes on the binary erasure channel," *IEEE Trans. Inf. Theory*, vol. 48, no. 6, pp. 1570–1579, June 2002.

[9] T. Richrdson, A. Shokrollahi, and R. Urbanke, "Finite-length analysis of various low-density parity-check ensembles for the binary erasure channel," in *Proc. IEEE Int. Symp. on Information Theory (ISIT)*, June 2002, p. 1.

[10] A. Amraoui, R. Urbanke, and A. Montanari, "Finite-length scaling of irregular LDPC code ensembles," in *Proc. IEEE Inf. Theory Workshop*, Aug 2005, pp. 5–10.

[11] A. Amraoui, A. Montanari, T. Richardson, and R. Urbanke, "Finite-length scaling for iteratively decoded LDPC ensembles," *IEEE Trans. Inf. Theory*, vol. 55, no. 2, pp. 473–498, Feb 2009.

[12] R. Yazdani and M. Ardakani, "Waterfall performance analysis of finite-length LDPC codes on symmetric channels," *IEEE Trans. Comm.*, vol. 57, no. 11, pp. 3183–3187, Nov 2009.

[13] Z. Mei, K. Cai, and G. Song, "Performance analysis of finite-length LDPC codes over asymmetric memoryless channels," *IEEE Trans. Veh. Technol.*, vol. 68, no. 11, pp. 11 338–11 342, Nov 2019.

[14] E. Yang and J. Meng, "New nonasymptotic channel coding theorems for structured codes," *IEEE Trans. Inf. Theory*, vol. 61, no. 9, pp. 4534–4553, Sep. 2015.

[15] A. Roumy and D. Declercq, "Characterization and optimization of LDPC codes for the 2-user Gaussian multiple access channel," *EURASIP J. Wirel. Comm. Netw.*, vol. 2007, no. 1, p. 074890, Jun 2007. [Online]. Available: https://doi.org/10.1155/2007/74890

[16] S. Sharifi, A. K. Tanc, and T. M. Duman, "LDPC code design for the two-user Gaussian multiple access channel," *IEEE Trans. on Wirel. Comm.*, vol. 15, no. 4, pp. 2833–2844, 2015.

[17] H. Yagi and H. V. Poor, "Coset codes for compound multiple access channels with common information," *IEEE Trans. Inf. Theory*, vol. 57, no. 6, pp. 3429–3448, 2011.

[18] P. Elias, "Coding for noisy channels," in *IRE Conv. Rec.*, vol. 3, Mar. 1955, pp. 37–46.

[19] A. Bennatan and D. Burshtein, "Design and analysis of nonbinary LDPC codes for arbitrary discrete-memoryless channels," *IEEE Trans. Inf. Theory*, vol. 52, no. 2, pp. 549–583, Feb 2006.

[20] Y.-S. Liu and B. L. Hughes, "A new universal random coding bound for the multiple-access channel," *IEEE Trans. Inf. Theory*, vol. 42, no. 2, pp. 376–386, 1996.

[21] T. Han and K. Kobayashi, "A new achievable rate region for the interference channel," *IEEE Trans. Inf. Theory*, vol. 27, no. 1, pp. 49–60, January 1981.

[22] S. Chen, M. Effros, and V. Kostina. Lossless source coding in the point-to-point, multiple access, and random access scenarios. [Online]. Available: https://arxiv.org/abs/1902.03366

[23] R. C. Yavas, M. Effros, and V. Kostina. Gaussian multiple and random access in the finite blocklength regime. [Online]. Available: https://arxiv.org/abs/2001.03867