

Improving the MAC Error Exponent Using Distributed Structure

Eli Haim
Dept. of EE-Systems, TAU
Tel Aviv, Israel
Email: elih@eng.tau.ac.il

Yuval Kochman
EECS Dept., MIT
Cambridge, MA 02139, USA
Email: yuvalko@mit.edu

Uri Erez*
Dept. of EE-Systems, TAU
Tel Aviv, Israel
Email: uri@eng.tau.ac.il

Abstract—Structured codes have been utilized in deriving the best known achievable rate regions in certain network scenarios. In this paper we demonstrate that structure can be also beneficial in terms of error exponents even in cases where there is no capacity gain. We use distributed structure, i.e., different users use codes which satisfy a nesting condition. Specifically, for the scalar Gaussian multiple-access channel we obtain an improvement over the best known achievable exponent, given by Gallager, for certain rate pairs.

I. INTRODUCTION

Structured codes have been known to achieve better rates than random ones in some distributed scenarios. This was first discovered by Körner and Marton [1], and was extended in recent works, see e.g. [2], [3]. This work sheds new light on the role of structure: even in the case of a Gaussian multiple-access (MAC) channel, where structure is not required in order to achieve the capacity region, the analysis suggests that it is needed in order to improve the error probability, asymptotically measured by the error exponent.

The error exponent of the additive white Gaussian noise (AWGN) channel was introduced by Shannon, who showed that above the critical rate the exponent is given by the *random-coding exponent*, i.e., it is achieved by random codes uniformly distributed over the surface of a sphere. Gallager [4] extended this result to general input-constrained channels. Below the critical rate, the random-coding error exponent lower-bounds the error exponent. In an even lower rate region, the error exponent can be improved by using expurgation.

In order to find codes with good error exponent for the Gaussian MAC channel, Gallager [5] derived the error exponent of the ensemble of codes where the codebook of each user is uniformly distributed over a spherical shell, similar to the single-user case. Clearly, the sum of such two codebooks does not result in a spherical-shell one. Thus, Gallager's exponent reflects a loss with respect to the single-user case.

In this work we improve the exponent by considering codebooks that are jointly structured (nested) in a way that their sum, seen as a single-user codebook, has good properties. Specifically, without structure, standard expurgation, i.e., simply eliminating pairs of codewords, is not possible since the codebooks must be independent. In the distributed structure

approach introduced in this work, the sum-codebook inherently gains the expurgation since it uses lattices. We compare the error exponent of this approach with the spherical-shells code [5], and show that in a certain rate-pair region, it results in a *strictly* larger error exponent.

It is worth noting that in a related recent work, Nazari et al. [6] give lower bounds on the error exponents of *discrete* memoryless MAC channels. In particular, they use expurgation in only one of the codebooks, and show that it is strictly larger than previous known bounds.

II. CHANNEL MODEL AND EXPONENTS

A. Single-User Channel

Let us first recall some results for a single-user AWGN channel. Consider the following single-user AWGN channel:

$$Y = X + Z, \quad (1)$$

where X is the input to the channel and is subject to the power constraint:

$$\frac{1}{n} \sum_{j=1}^n x_j^2 \leq P, \quad (2)$$

where n is the codeword length. $Z \sim \mathcal{N}(0, N)$ is additive noise, statistically independent of X . The capacity of this channel is given by $C(A) \triangleq 1/2 \log(1 + A)$, where $A \triangleq P/N$ is the signal to noise ratio (SNR). The error-exponent of this channel is defined as

$$E^{(\text{SU})}(R, A) = \limsup_{n \rightarrow \infty} -\frac{1}{n} \log P_n(\mathcal{E}), \quad (3)$$

where $P_n(\mathcal{E})$ is the minimal possible error-probability of codes with length n , and R is the rate.

The best known achievable error exponent of this channel, denoted by $\underline{E}^{(\text{SU})}(R, A)$, is given as follows: the expurgated error exponent $E_{\text{ex}}^{(\text{SU})}(R, A)$ at the expurgation region, and the random-coding error exponent $E_r^{(\text{SU})}(R, A)$ at the rest of the region (see [4, Section 7]). The expurgated exponent is larger than the random-coding exponent below some rate $R_{\text{ex}}(A)$ (the expurgation region). Above the critical rate $R_{\text{cr}}(A)$, the random-coding exponent is known to be optimal.

In the high SNR limit $A \gg 1$, $\underline{E}^{(\text{SU})}(R, A)$ approaches the

* This work was supported in part by the U.S. - Israel Binational Science Foundation under grant 2008/455.

Poltyrev exponent [7]:

$$E_P(\rho) \triangleq \begin{cases} 0, & \rho^2 \leq 1 \\ \frac{1}{2} [(\rho^2 - 1) - \log \rho^2], & 1 < \rho^2 \leq 2 \\ \frac{1}{2} \log \frac{e\rho^2}{4}, & 2 \leq \rho^2 \leq 4 \\ \frac{\rho^2}{8}, & \rho^2 \geq 4 \end{cases}, \quad (4)$$

where $\rho^2 = (1 + A) \exp\{-2R\}$. The boundaries $\rho^2 = 1$, $\rho^2 = 2$ and $\rho^2 = 4$ correspond to $C(A)$, $R_{\text{cr}}(A)$ and $R_{\text{ex}}(A)$, respectively.

B. MAC Channel

Consider a two-user memoryless Gaussian MAC channel:

$$Y = X_1 + X_2 + Z, \quad (5)$$

where X_1, X_2 are the inputs to the channel, and are subject to power constraints as in (2) with powers P_1 and P_2 respectively. The additive noise $Z \sim \mathcal{N}(0, N)$ is independent of the pair (X_1, X_2) . Without loss of generality, let $P_1 \geq P_2$.

We denote the SNRs by $A_i \triangleq P_i/N$ ($i = 1, 2$). Denote the codebook of user i by \mathcal{C}_i , and its rate by $R_i = 1/n \log |\mathcal{C}_i|$.

The error event \mathcal{E} is defined as the event that at least one of the messages from the message pair is decoded in error. The error exponent of the MAC channel is defined as

$$E^{(\text{MAC})}(R_1, R_2, A_1, A_2) = \limsup_{n \rightarrow \infty} -\frac{1}{n} \log P_n(\mathcal{E}), \quad (6)$$

where $P_n(\mathcal{E})$ is the minimal possible error probability for codes of length n , when the rate-pair is (R_1, R_2) .

The best known achievable error-exponent of this channel is given by Gallager [5], using spherical shell codebooks. We denote this error exponent by $E_r^{(\text{G})}(R_1, R_2, A_1, A_2)$. It is given by the minimum between three exponents: two of the exponents, $E_{r_1}^{(\text{G})}(R_1, A_1)$ and $E_{r_2}^{(\text{G})}(R_2, A_2)$ are the single-user random-coding error exponents. The third one, $E_{r_3}^{(\text{G})}(R_1 + R_2, A_1, A_2)$ reflects the exponent of the probability that both codewords are decoded in error. Obviously, the exponent is upper-bounded by any of these three. In the sequel, we upper bound the exponent by $E_r^{(\text{G})}$, given by [5]:

$$\begin{aligned} \overline{E_r^{(\text{G})}}(R, A_1, A_2) &\triangleq E_{r_3}^{(\text{G})}(R, A_1, A_2) \\ &= (1 + \rho) \log \frac{e\sqrt{\theta_1\theta_2}}{1 + \rho} - \frac{\theta_1 + \theta_2}{2} \\ &\quad + \frac{\rho}{2} \log \left(1 + \frac{A_1}{\theta_1} + \frac{A_2}{\theta_2} \right) - \rho R, \end{aligned} \quad (7)$$

where $R \triangleq R_1 + R_2$, and the right-hand expression of (7) is optimized over $\rho \in [0, 1]$ and over r_i for:

$$\theta_i \triangleq (1 + \rho)(1 - 2r_i P_i), \quad \theta_i \in [0, 1 + \rho]. \quad (8)$$

C. Single-User Bounds on MAC Error Exponents

Definition 1 (Associated single user channel): For a given MAC channel (5), we denote its *associated single-user channel* by the single-user channel (1)-(2) with $P \triangleq P_1 + P_2$.

Any codebook pair $(\mathcal{C}_1, \mathcal{C}_2)$ for the MAC channel can be used to construct a *corresponding codebook* for its associated

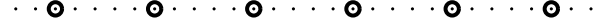


Fig. 1. One-dimensional example: the circles are points of the codebook of the first user. The dots are the superposition of the two codebooks ($|\mathcal{C}_1| = 2L_1 = 6, |\mathcal{C}_2| = 2L_2 + 1 = 5$).

single-user channel, by the Minkowski sum codebook $\mathcal{C} = \mathcal{C}_1 + \mathcal{C}_2$. However, not every single-user codebook \mathcal{C} can be decoupled in such a manner.

Therefore, for any given ensemble of codebook-pairs for the MAC channel, a *corresponding codebook ensemble* can be constructed for its associated single-user channel, both having the same error exponent.

Thus, the error-exponent of the associated single-user channel upper-bounds the error exponent of the MAC channel:

$$E^{(\text{MAC})}(R_1, R_2, A_1, A_2) \leq E^{(\text{SU})}(R_1 + R_2, A_1 + A_2). \quad (9)$$

The exponent $E_r^{(\text{G})}(R_1, R_2, A_1, A_2)$ is strictly smaller than the single-user exponent. Moreover, it is strictly smaller than the *random coding* error exponent.

In this work, we construct an ensemble of codebook pairs for the MAC channel, such that the corresponding ensemble for the associated single-user channel has a “good” error exponent. For a certain range of rate-pairs and SNRs, the ensemble achieves a better error exponent than the error exponent of the spherical-shells ensemble $E_r^{(\text{G})}(R_1, R_2, A_1, A_2)$. The exponent $\underline{E}^{(\text{SU})}(R_1 + R_2, A_1 + A_2)$ is used as a benchmark for the error exponent which we obtain. Above the critical rate it is an upper-bound.

III. ONE-DIMENSIONAL MOTIVATION

In this section we present the basic idea of distributed structure by a one-dimensional example, and demonstrate how it can result in improved error probability. Suppose that the users transmit using pulse-amplitude modulation (PAM) constellations, where the constellation of the second user has support that is smaller than the distance between any two points of the first. Moreover, their Minkowski sum should have a constant distance between every two adjacent points. Specifically, $\mathcal{C}_1 = \{\pm 1, \pm 3, \dots, \pm(2L_1 - 1)\}$ (where $L_1 \in \mathbb{N}$), and $\mathcal{C}_2 = \{0, \pm 2/(2L_2 + 1), \pm 4/(2L_2 + 1), \dots, \pm 2L_2/(2L_2 + 1)\}$, where $L_2 \in \mathbb{N}$. The transformation $c = c_1 + c_2$ where $c_1 \in \mathcal{C}_1, c_2 \in \mathcal{C}_2$ is bijective, i.e., the codeword pair can be resolved from their sum without ambiguity (see Figure 1). Thus, from the point of view of the receiver, the sum-constellation may have resulted from the transmission of a single user. Indeed, it is a PAM constellation with $|\mathcal{C}_1| \cdot |\mathcal{C}_2|$ points, where the distance between its points is equal to that of \mathcal{C}_2 . The error probability can be calculated directly from here.

Note that if the constellations were designed independently, e.g. by using PAM constellations with distances that do not result in a PAM constellation, some points would have been closer, resulting in higher error probability. In the high-dimensional case we strive to preserve this distance uniformity behavior. We will thus require that the decoding (Voronoi) region of the corresponding single-user codebook, as seen by the receiver, remains the same as the Voronoi region of \mathcal{C}_2 .

Extending this example to higher dimensions will preserve this distance property, but will result in a shaping loss. Therefore, in addition to the distance properties between the codebook points, we want the corresponding codebook of the associated single-channel to have “good” shaping.

IV. PRELIMINARIES: LATTICES

This section presents mathematical background which is required for the code construction and its error-probability analysis. For a more thorough treatment of lattices, the reader may refer to [8] and the references therein.

A lattice Λ is a discrete subgroup of the Euclidean space \mathbb{R}^n with the ordinary vector addition operation. A coset of Λ is any translate of it, i.e., $\mathbf{x} + \Lambda$, where $\mathbf{x} \in \mathbb{R}^n$.

The fundamental Voronoi region of Λ , denoted by \mathcal{V} , is a set of minimum Euclidean norm coset-representatives of Λ . Every $\mathbf{x} \in \mathbb{R}^n$ can be uniquely expressed as $\mathbf{x} = \lambda + \mathbf{r}$, where $\lambda \in \Lambda$, $\mathbf{r} \in \mathcal{V}$. The nearest-neighbor quantizer of a point $\mathbf{x} \in \mathbb{R}^n$ is defined by:

$$Q(\mathbf{x}) = \lambda, \quad \text{if } \mathbf{x} \in \lambda + \mathcal{V} \text{ and } \lambda \in \Lambda. \quad (10)$$

A. Good Lattices

We define two notions of “good” lattices. Let r_{Λ}^{cov} denote the covering radius of Λ , i.e., the radius of the smallest ball containing the Voronoi region \mathcal{V} . Let $r_{\Lambda}^{\text{effec}}$ denote the effective radius of the Voronoi region, i.e., the radius of a sphere having the same volume as \mathcal{V} . We say that a sequence of lattices $\Lambda^{(n)} \in \mathbb{R}^n$, $n = 1, 2, \dots$, is *good for covering* if $\liminf_{n \rightarrow \infty} r_{\Lambda^{(n)}}^{\text{cov}}/r_{\Lambda^{(n)}}^{\text{effec}} = 1$, for example Rogers-good lattices. Choosing a sequence of Rogers-good lattices with $r_{\Lambda^{(n)}}^{\text{cov}} = \sqrt{nP}$ results in $r_{\Lambda^{(n)}}^{\text{effec}} = \sqrt{n(P - \varepsilon_n)}$, where $\varepsilon_n \xrightarrow{n \rightarrow \infty} 0^+$. This implies that $\mathcal{V} \subset B_n(\sqrt{nP})$, where $B_n(r)$ is an n -dimensional sphere with radius r . Thus $1/n \sum_{i=1}^n x_i^2 \leq P$ for any point in $\mathbf{x} \in \mathcal{V}$.

A sequence of lattices $\Lambda^{(n)} \in \mathbb{R}^n$, $n = 1, 2, \dots$, is said to be *Polytyrev-good* if for an n -dimensional vector \mathbf{Z} with i.i.d. Gaussian entries with zero mean and power N :

$$\Pr(\mathbf{Z} \notin \mathcal{V}^{(n)}) < e^{-n[E_P(\rho_{\Lambda^{(n)}}) - o_n(1)]}, \quad (11)$$

where $\mathcal{V}^{(n)}$ is the Voronoi region of $\Lambda^{(n)}$, and $\rho_{\Lambda^{(n)}}$ is the *Voronoi-to-noise ratio*:

$$\rho_{\Lambda^{(n)}} \triangleq \frac{r_{\Lambda^{(n)}}^{\text{effec}}}{\sqrt{nN}} = \frac{[\text{Vol}(\mathcal{V}^{(n)})]^{1/n}}{\sqrt{2\pi eN}} + o_n(1). \quad (12)$$

The Polytyrev exponent $E_P(\rho)$ was defined in (4), and $o_n(1) \rightarrow 0$ as $n \rightarrow \infty$.

B. Nested Lattice Codes

Here we recall nested-lattice codes for a single-user AWGN channel. The construction of codes for the MAC channel is described in Section V.

We say that a coarse lattice Λ_0 is nested in a fine lattice Λ_1 if $\Lambda_0 \subseteq \Lambda_1$, i.e., Λ_0 is a sublattice of Λ_1 . We denote their fundamental Voronoi regions by \mathcal{V}_0 and \mathcal{V}_1 respectively, and the volumes of the Voronoi regions by V_0 and V_1 respectively.

A shift of Λ_0 by a point of Λ_1 is called a coset of Λ_0 relative to Λ_1 . For every such coset, there is a single point with minimal norm, which is called the coset leader. A nested-lattice code is the intersection of a fine lattice Λ_1 with the fundamental Voronoi region of a sublattice Λ_0 , i.e., $\mathcal{C} = \{\Lambda_1 \cap \mathcal{V}_0\}$. This is equal to the coset leaders of Λ_0 relative to Λ_1 . Thus, the number of codewords is equal to V_0/V_1 . We call $(V_0/V_1)^{1/n}$ the nesting ratio of the lattices. The code rate is thus equal to the logarithm of the nesting ratio: $R = 1/n \log(V_0/V_1)$.

V. DISTRIBUTED-STRUCTURE CODING

In this section we describe a code construction for the MAC channel, which is based on distributed structure. It consists of two codebooks, where each is a subset of a lattice, and their Minkowski sum forms a subset of the fine lattice. It has the property that every pair of codewords results in a different point of the fine lattice. In addition, the fine lattice is a good lattice for associated single-user channel. Hence, inherently from the code, the decoding is done jointly for the two users.

While the code presented here is sub-optimal in terms of the capacity region, for certain rate-pairs it improves on the best known error exponent in [5].

A. Codebooks Construction

Recall that $P_1 \geq P_2$. For clarity of derivation, we also assume that $P_2 \geq N$. We ignore other case, i.e. $P_2 < N$, since this results in $R_2 = 0$ for the proposed construction. That is, this is a degenerate case (under the code presented here), since it forms a single-user channel, as only the first user transmits.

The codebook generation uses a triplet of nested lattices: $\Lambda_0^{(n)} \subseteq \Lambda_1^{(n)} \subseteq \Lambda_2^{(n)}$, where the covering radii are given by:

$$r_{\mathcal{V}_0}^{\text{cov}} = \sqrt{nP_1}, \quad r_{\mathcal{V}_1}^{\text{cov}} = \sqrt{nP_2}, \quad r_{\mathcal{V}_2}^{\text{cov}} = \sqrt{n\tilde{N}},$$

where $\tilde{N} \in [N, P_2]$, and $\mathcal{V}_i^{(n)}$ is the fundamental Voronoi region of $\Lambda_i^{(n)}$. Each lattice is both Rogers-good and Polytyrev-good.¹ The existence of such good nested lattices for any choice of nesting ratios is shown in [9]. Denote the volume of $\mathcal{V}_i^{(n)}$ by $V_i^{(n)}$. Since the lattices are Rogers-good, we have:

$$V_0^{(n)} = [2\pi e(P_1 - \varepsilon_{1,n})]^{n/2}, \quad V_1^{(n)} = [2\pi e(P_2 - \varepsilon_{2,n})]^{n/2},$$

where $\varepsilon_{i,n} \rightarrow 0^+$ as $n \rightarrow \infty$. See Figure 2 for an illustration of the nested lattices.

The codebook of the second user is given by the coset-leaders of $\Lambda_2^{(n)}$ relative to $\Lambda_1^{(n)}$: $\mathcal{C}_2^{(n)} = \{\Lambda_2^{(n)} \cap \mathcal{V}_1^{(n)}\}$. The rate of the second user is given by the nesting ratio:

$$R_2^{(n)} = \frac{1}{n} \log \frac{V_1}{V_2} \xrightarrow{n \rightarrow \infty} \alpha \cdot \frac{1}{2} \log \frac{P_2}{N} \triangleq R_2, \quad (13)$$

where $\alpha \triangleq (\log \tilde{A}_2)/(\log A_2) \in [0, 1]$, and $\tilde{A}_2 \triangleq P_2/\tilde{N}$. The codebook of the first user is constructed by the coset-leaders

¹Less restrictive constraints on the goodness of the lattices may suffice.

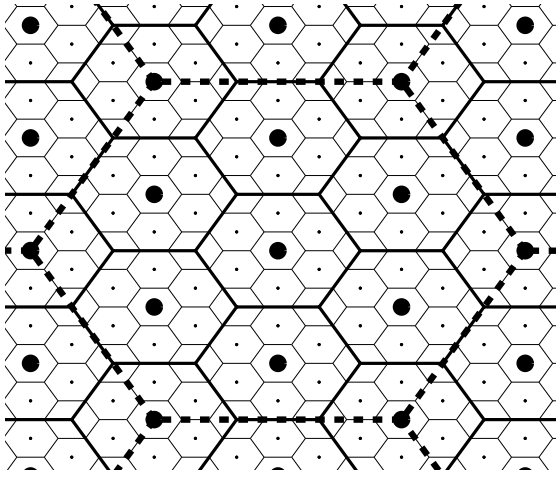


Fig. 2. Nested lattice with ratio 3:3: The thick-dashed line is the Voronoi partition of Λ_0 , where the region in the center is \mathcal{V}_0 , which is the shaping region of the first user. The thick points are the points of Λ_1 , and the thick-solid line is its Voronoi partition. The thick-solid line region in the center is \mathcal{V}_1 , which is the shaping region of the second user. The thin dots (together with the thick ones) are the points of Λ_2 , and the thin-solid line is its Voronoi partition.

of Λ_1 relative to Λ_0 : $\mathcal{C}_1^{(n)} = \{\Lambda_1^{(n)} \cap \mathcal{V}_0^{(n)}\}$. The rate of the first user results from the nesting ratio:

$$R_1^{(n)} = \frac{1}{n} \log \frac{V_0}{V_1} \xrightarrow{n \rightarrow \infty} \frac{1}{2} \log \frac{P_1}{P_2} \triangleq R_1. \quad (14)$$

Since $\Lambda_1^{(n)}$ and $\Lambda_2^{(n)}$ are Rogers-good lattices, as explained in Section IV-A, it follows that $\mathcal{C}_1^{(n)}$ and $\mathcal{C}_2^{(n)}$ satisfy the power constraints P_1 and P_2 respectively. Notice that the Minkowski sum of the two codebooks is a subset of the fine lattice $\Lambda_2^{(n)}$.

The maximal sum rate achieved by this construction is $1/2 \log A_1$. This reflects a loss in compare with the maximal sum rate of the channel, which is $1/2 \log(1 + A_1 + A_2)$.

B. Error Probability Analysis

In the following analysis we make some rather restrictive choices in the encoding-decoding process we consider. Some choices are necessary, while others simplify the derivation. Even with these choices, we improve the best known achievable exponent. In Section VII we present an assumption under which the best known achievable single-user exponent may be achieved (and above the critical rate it is optimal).

We analyze the error probability of the code by averaging over an ensemble of codes, which is described in [9]. This ensemble builds on *Construction A* [10].

The Minkowski sum of the codebook pair, which is a subset of the fine lattice $\Lambda_2^{(n)}$, can be interpreted as the corresponding codebook of the associated single-user channel. Thus, we can use a lattice decoder for joint decoding of the message pair. A lattice decoder is simply a lattice quantizer (10). The error-exponent of this ensemble when using lattice decoder is given by the Poltyrev exponent (4) with ρ given by (12) (see [11]):

$$\rho_{\Lambda^{(n)}}^2 = \frac{\left(V_1^{(n)}\right)^{2/n}}{e^{2R_2^{(n)}} \cdot 2\pi eN} \xrightarrow{n \rightarrow \infty} \frac{2\pi eP_2}{e^{2R_2} \cdot 2\pi eN} = e^{(1-\alpha) \log A_2}.$$

We conclude that the error exponent of the code is lower-bounded by:

$$E_r^{(\text{struct})}(R_1, R_2, A_1, A_2) \triangleq E_P \left(e^{\frac{1}{2}(1-\alpha) \log A_2} \right). \quad (15)$$

Note that the exponent is positive whenever $A_2 > 1$ (as we assumed).

VI. PERFORMANCE COMPARISON

In this section we show that the sub-optimal encoding-decoding scheme above outperforms the spherical-shells exponent for some rate pairs.

For given A_1, A_2 and R_1 , Figure 3 compares the spherical-shells error-exponent $E_{r_3}^{(G)}$ (7) with the distributed-structure error exponent (15). We can see that below a certain rate R_2 , distributed structure has a strictly larger error exponent than the spherical-shells one. These exponents are also compared with $\underline{E}^{(\text{SU})}(R_1 + R_2, A_1 + A_2)$, which is used here as a benchmark. Figure 3(a) shows a high SNR case, where the second user has half of the power of the first user. The error exponent of the distributed structure code is strictly larger than the one of the spherical-shells codebooks in part of the rate region. Figure 3(b) shows a high SNR case, where the second user is much weaker than the first one; therefore it is almost a single user case. Figure 3(c) shows a low SNR case, where the second user loses since it is not equal to the single-user capacity $C(\tilde{A}_2)$. Figure 3(d) shows a case, where the second user is much weaker than the first one, and therefore the first user loses rate since it is not equal to the single-user capacity $C(A_1)$. In the last two cases, the error exponent of the distributed structure code is lower than the one of the spherical-shells code.

If one is not satisfied with the numerical optimization of $E_{r_3}^{(G)}$ (7), an analytical comparison can be carried out by using the following symmetric-powers upper-bound:

$$E_{r_3}^{(G)}(R_1 + R_2, A_1, A_2) \leq E_{r_3}^{(G)}(R_1 + R_2, A_1, A_1).$$

This bound has an explicit expression given in [5, Section II-C, Equation (2.48)-(2.55)]. The distributed structure exponent is even higher than this bound, for some rate pairs.

While for general (i.e., non-structured) infinite constellations, Poltyrev's exponent (4) in the range of squared Voronoi-to-noise ratio larger than 4 is achieved by expurgation, for (infinite) lattices it is inherently achieved by the ensemble, since all codewords have the same error probability [7]. We note that the distributed structure code is superior to the spherical-shells in (part of) the expurgation region of Poltyrev's exponent ($\rho^2 \geq 4$). This may imply that the "inherent expurgation" of lattices contributes to some of the gain of this code over the spherical-shells one.

VII. DISCUSSION: TOWARDS OPTIMAL DISTRIBUTED STRUCTURE

In this section we outline a direction that may allow to establish that a distributed structure approach can be optimal; More specifically, in order to achieve the single-user error exponent, provided (an assumption that we do not know to

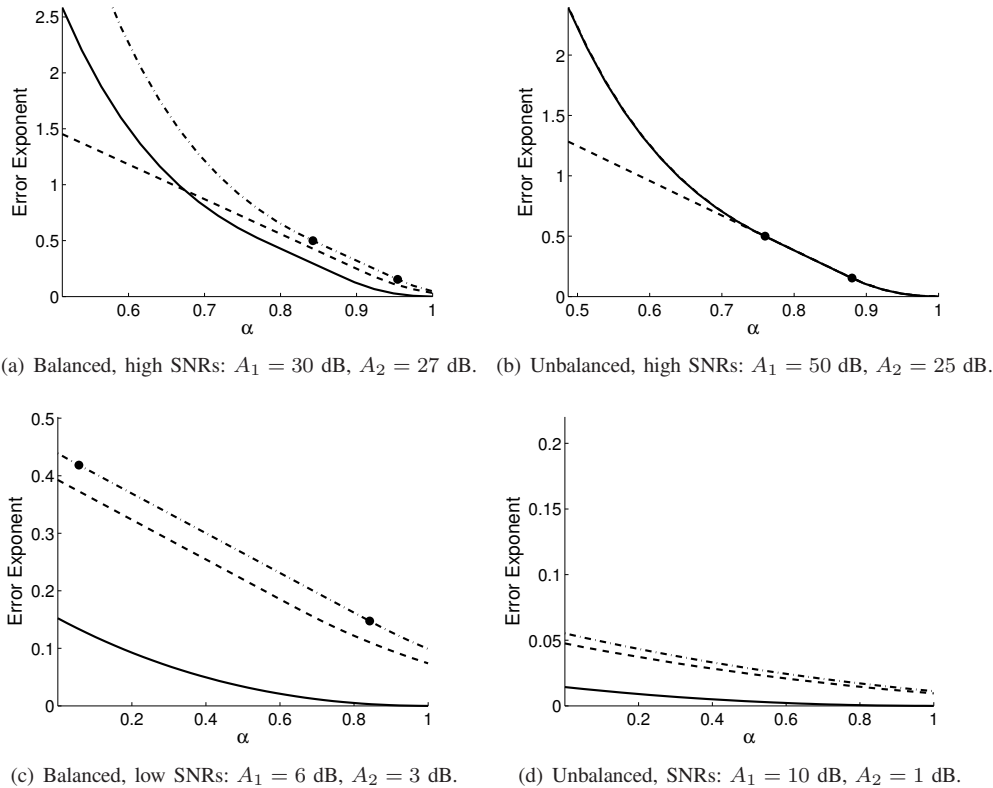


Fig. 3. Comparing the error exponent of the spherical-shells code $\overline{E}_r^{(G)}(R_1 + R_2, A_1, A_2)$ (dashed line) to the error-exponent of the distributed structure $E_r^{(\text{struct})}(R_1, R_2, A_1, A_2)$ (solid line). $\underline{E}^{(\text{SU})}(R_1 + R_2, A_1 + A_2)$ of the associated single user channel is shown by the dash-dot line of the associated single user channel. The two dots indicate the expurgation rate $R_{ex}(A_1 + A_2)$ and the critical rate $R_{cr}(A_1 + A_2)$. The horizontal axis is $\alpha = R_2 / (1/2 \log A_2)$, while R_1 is fixed according to Equation (14).

be true) that a nested-lattice construction with perfect tiling exists. To establish optimality, the following lemma may be of use. We omit the proof in this version.

Lemma 1: For a single-user AWGN channel, a uniformly random codebook over the fundamental Voronoi region of a Rogers-good lattice achieves the random coding error exponent.

This ensemble is different than Gallager's one [4, Chapter 7], since here the codewords are distributed uniformly over the entire sphere, and not only over a shell of the sphere.

It can further be shown that by replacing the uniformly random code with a good ensemble of lattices, $\underline{E}^{(\text{SU})}$ is achieved. Thus, a nested-lattice codebook can achieve $\underline{E}^{(\text{SU})}$.

In order to achieve a good single-user nested-lattice in a distributive manner, we require a Rogers-good and Poltyrev-good nested triple, such that it satisfies *perfect tiling*: the Voronoi region of each lattice tiles the Voronoi region of the coarser lattice, similar to the one-dimensional example in Section III. If this may be achieved, one obtains a an optimal lattice code, achieving the single-user error exponent $\underline{E}^{(\text{SU})}$. Even if perfect tiling is not possible, we expect that the results can be significantly improved. Furthermore, in conjunction with rate splitting one can generalize the scheme to achieve any rate-pair in the capacity region.

REFERENCES

- [1] J. Körner and K. Marton, "How to encode the modulo-two sum of binary sources," *IEEE Trans. Information Theory*, vol. IT-25, pp. 219–221, March 1979.
- [2] D. Krithivasan and S. Pradhan, "Lattices for distributed source coding: Jointly gaussian sources and reconstruction of a linear function," *IEEE Trans. Information Theory*, vol. 55, no. 12, pp. 5628–5651, 2009.
- [3] M. P. Wilson, K. R. Narayanan, H. D. Pfister, and A. Sprintson, "Joint physical layer coding and network coding for bidirectional relaying," *IEEE Trans. Information Theory*, vol. IT-56, pp. 5641–5654, Nov. 2010.
- [4] R. G. Gallager, *Information Theory and Reliable Communication*. John Wiley & Sons, 1968.
- [5] —, "A perspective on multiaccess channels," *IEEE Trans. Information Theory*, vol. 31, no. 2, pp. 124–142, mar. 1985.
- [6] A. Nazari, A. Anastopoulos, and S. S. Pradhan, "Error exponent for multiple-access channels: lower bounds," *CoRR*, vol. abs/1010.1303, 2010.
- [7] G. Poltyrev, "On coding without restrictions for the AWGN channel," *IEEE Trans. Information Theory*, vol. IT-40, pp. 409–417, March 1994.
- [8] R. Zamir, "Lattices are everywhere," in *Information Theory and Applications Workshop, 2009*, 2009, pp. 392–421.
- [9] D. Krithivasan and S. S. Pradhan, "A proof of the existence of good nested lattices," www.eecs.umich.edu/techreports/systems/cspl/cspl-384.pdf, 2007.
- [10] H.-A. Loeliger, "Averaging bounds for lattices and linear codes," *IEEE Trans. Information Theory*, vol. 43, no. 6, pp. 1767–1773, Nov. 1997.
- [11] U. Erez, S. Litsyn, and R. Zamir, "Lattices which are good for (almost) everything," *IEEE Trans. Information Theory*, vol. IT-51, pp. 3401–3416, Oct. 2005.