Structured Dirty-Paper Coding using Low-Density Lattices

Sang Hyun Lee, Ankit Ghiya, Sriram Vishwanath
Department of ECE
University of Texas at Austin
Austin, TX, USA
Email: {shlee, aghiya, sriram}@ece.utexas.edu

Sung Soo Hwang, Sunghwan Kim
Samsung Electronics
Suwon, Gyeonggi-do, Korea
Email: {sungsoo.hwang, sunghwan007.kim}@samsung.com

Abstract—This paper studies dirty-paper coding in a Gaussian broadcast channel with two receivers. It finds that an approximate version of dirty-paper coding using low-density lattices can be implemented with a complexity that is polynomial-time on average in the block length. The main difference between this paper and prior work is that a non-binary LDPC-based lattice codebook is used for each user, and one codebook is aligned with the other. The low-density nature enables tractable encoding and decoding algorithms, and the alignment gives structure to the overall signal transmitted and it enables us to perform the encoding and decoding efficiently.

Index Terms—Dirty-paper coding, Nested lattice codes, LDPC codes

I. INTRODUCTION

The broadcast channel is one of the most important channel settings in multi-user information theory [1]. For the multiple-antenna Gaussian broadcast channel (and as a special case, for the single antenna broadcast channel), it is now well known that “dirty-paper” coding achieves the entire capacity region [2]-[4]. However, one of the big stumbling blocks for this channel has been the perceived impracticality of dirty-paper coding. This is for two reasons: First, dirty-paper coding requires accurate knowledge of the channel state information for all the channels at the transmitter, and second, even with the state known, it can be shown that the encoding and decoding process required by dirty-paper coding mechanisms (both based on binning [5] and structured coding arguments [4]) have an exponential complexity in the block length. Thus, multiple papers have been subsequently written approximating dirty-paper coding using both linear and non-linear mechanisms such as Tomlinson-Harashima precoding [6]-[7], zero-forcing and MMSE coding [8]. However, results for cellular networks have shown that dirty-paper coding can have large gains over strategies that substitute for it [9], and thus it is essential that we determine a mechanism for performing dirty-paper coding without attempting to bypass it.

In this paper, we focus on the encoding and decoding aspect of dirty-paper coding. In other words, assuming that the channel state is known perfectly at the transmitter, we simplify the dirty-paper coding techniques in [4], [10] using aligned lattices to implement it with a complexity that is polynomial-time on average in the block length. This means that, for slowly fading environments with perfect channel state feedback, dirty-paper coding might in fact be a viable choice, and is one step closer to being practical than previously thought.

This paper is organized as follows. The next section presents the system model. In Section III, we present the main encoding strategy using lattice codes. In Section IV, we present the decoding strategy to be used for this setting. In Section V, we present belief-propagation framework for the encoding and decoding strategies. In Section VI, we demonstrate simulation results. Finally, with Section VII, we conclude this paper.

II. SYSTEM MODEL

This paper uses the following notation. $T$ is used to denote matrix transpose. Boldface is used for all vectors which are assumed to be column vectors unless specified otherwise. For a lattice $L$ as defined in [11], $V_L$ is used to denote its Voronoi region. $\mod$ is used to denote a modulo operation with respect to a lattice (as defined in [11]). $U[S]$ is used to denote either a discrete or a continuous-valued uniform distribution over support $S$.

The system considered is a multiple-input single-output (MISO) broadcast channel as depicted by Figure 1. For the

---

1This work is supported by a grant from Samsung Electronics.

sake of simplicity, only two receivers are assumed in the system.\(^3\) The channel is mathematically characterized by

\[
Y_1 = h_1^T X + N_1, \\
Y_2 = h_2^T X + N_2.
\]

where \(X\) is a transmitted signal, \(h_1\) and \(h_2\) represent the channel state information for both receivers, respectively, and \(N_1\) and \(N_2\) are the additive Gaussian noises with variance \(N\) for both receivers, respectively. Here, all symbols are assumed to be real-valued, and the extension to the complex case is straightforward. Also, the transmitter is limited to a power of \(P\). The main assumption made in this paper is that the channel state information \(h_1\) and \(h_2\) are known to the transmitter and receivers exactly. The capacity region of this channel is already known to be achieved by dirty-paper coding (along with time sharing) [2]. Traditionally, dirty-paper coding is implemented using a Gel’fand-Pinsker-style binning argument [14]. However, in recent work, lattice codes have been used to perform this operation [4]. Specifically, it shows that nested lattice codes can be used to perform dirty-paper coding for the point-to-point Gaussian noise channel with additive Gaussian state, which has been subsequently generalized to any state distribution in [10]. The encoding and decoding scheme introduced in [4] for the Gaussian noise channel with additive Gaussian state is described next.

The point-to-point Gaussian noise channel with additive Gaussian state (the channel model studied in [4]) has the form

\[
Y = X + S + N,
\]

where the transmitted message \(X\) has a power constraint \(P\), the additive state \(S\) is known non-causally to the transmitter, and the noise \(N\) is Gaussian with zero mean and variance \(N\). A “good” lattice \(\Lambda\) (in the sense of channel coding) is chosen as the “fine” lattice used to communicate the messages, which is nested\(^4\) with a “coarse” lattice \(L\) that represents the power constraint \((E||X||^2 \leq P)\). Given the lattice point \(\lambda \in \Lambda\) is communicated, the state \(S\) known to the transmitter and a scalar \(\alpha = P/(P+N)\), the encoding process follows:

\[
X = [\lambda - \alpha S - U] \mod L,
\]

where \(X\) is the dirty-paper-encoded message to be transmitted through the channel, and \(U\) is a dither chosen uniformly over the Voronoi region of the lattice \(L\). This is subsequently decoded by constructing:

\[
Y' = [\alpha Y + U] \mod L
\]

which is subsequently shown in [4] and [10] to be equivalent to

\[
Y' = [\lambda - (1-\alpha)U + \alpha N] \mod L.
\]

From \(Y'\), the lattice point \(\lambda\) is recovered using lattice decoding [4]. A straightforward application of this lattice-based encoding scheme to broadcast channels is still highly complex. This complexity is due to both the encoding and decoding processes in (3) and (4). Both of them require that the “mod” operation (with respect to a lattice) be performed on an arbitrary point in \(\mathbb{R}^n\). This process is equivalent to quantization with respect to the coarse lattice and is known to be \(NP\) in complexity, with some (approximate) techniques to accomplish this in existence [15]. Note that, although the dither \(U\) is constant for the entire communication, the additive state \(S\) changes from block to block, making the encoding in (3) exceedingly difficult to perform in real-time. On the decoding end, the operation in (4) suffers from the same issue as \(Y\) changes from block to block.

There are two main differences between dirty-paper coding when applied to Gaussian noise channel with state as in (2) and the multi-antenna broadcast channel. First, the channel input and outputs at each instant are vectors instead of scalars in (2). Secondly, the state \(S\) is (completely) controlled by the transmitter. If, in the dirty-paper coding scheme used for the broadcast channel, the additive state \(S\) has no structure (as done in [3]), then the encoding process will be identical in complexity to (3) and thus impractical.

The main focus of this work is to use low-density lattices and belief-propagation decoding at the transmitter and receivers [16], [17], [18], thus transforming the communication process to one that is polynomial-time in complexity in the block length.

### III. Approximate Dirty-Paper Encoding Strategy

In this section and next (Section IV), we describe the overall encoding and decoding strategies respectively to be used. Note that the simplified version (using belief-propagation decoding) is discussed in Section V. This section and the next are devoted to summarizing the theoretical aspects of this algorithm, and are based on the work in [4].

Without loss of generality, we choose Receiver 1 to have a dirty-paper-encoded codebook with a transmit power of \(\beta P\) for some \(0 \leq \beta \leq 1\). Traditionally, the codebook for Receiver 2 (transmitted with no dirty-paper encoding) is constructed first, and then the codebook for Receiver 1 (transmitted dirty-paper-encoded) is constructed using binning techniques [3]. In our case, we reverse this order with nested-lattice coding. First, we choose a “good” lattice \(\Lambda\) (in the sense of channel coding) for Receiver 1. This fine lattice \(\Lambda\) is nested with a coarse lattice \(L_1\) which represents the power constraint \(\beta P\).

It is known that optimal covariances \(\Sigma_1\) and \(\Sigma_2\) satisfying the power constraints \(tr[\Sigma_1] \leq \beta P\) and \(tr[\Sigma_2] \leq (1-\beta)P\) respectively exist such that the rate pairs \((R_1, R_2)\) lie on the boundary of the capacity region. An algorithmic framework for determining these optimal covariances is given in [3]. Also in [3], it is shown that the optimal choice of \(\Sigma_1\) and \(\Sigma_2\) for MISO broadcast channels is unit-rank matrices for the entire capacity region. This allows us to rewrite them in the form:

\[
\Sigma_1 = \beta Paa^T \\
\Sigma_2 = \beta Pbb^T
\]
for some vectors \( \mathbf{a} \) and \( \mathbf{b} \) respectively, where \( \bar{\beta} = 1 - \beta \). Now we introduce the notation:

\[
\begin{align*}
    h_{11} &= h_1^T \mathbf{a} \\
    h_{12} &= h_1^T \mathbf{b} \\
    h_{21} &= h_2^T \mathbf{a} \\
    h_{22} &= h_2^T \mathbf{b}.
\end{align*}
\]

**Lattice construction:** We know from [4], [13] that a nested-lattice ensemble \((\Lambda, L_1)\) exists with a fundamental volume such that, on average, the rate achieved by this ensemble for Receiver 1 with no interference present is at least

\[
\frac{1}{2} \log \left( \frac{h_{11}^2 P}{h_{22}^2 \beta P} \right).
\]

This, in essence, is the maximum rate seen without any interference by Receiver 1 when using the transmit covariance \( \Sigma_1 \) for its codebook generation and lies on the capacity region boundary for the channel with the appropriate choice for \( \Sigma_1 \) [3].

Next, we generate a codebook for Receiver 2. The desired rate for Receiver 2 is

\[
\frac{1}{2} \log \left( \frac{h_{12}^2 \beta P}{h_{22}^2 \beta P + N} \right).
\]

We take the lattice \( \Lambda \) and scale each element by \( \frac{h_{12}}{h_{22}} \) to generate a new lattice \( \tilde{\Lambda} = \frac{h_{12}}{h_{22}} \Lambda \). We find a sublattice of \( \tilde{\Lambda} \) given by \( \Gamma \) which is subsequently nested in a coarse lattice \( \Lambda \leq \tilde{\Lambda} \) representing the power constraint \( \beta P \) for Receiver 2. This nested pair \((\Gamma, L_2)\) are constructed such that the resulting rate for Receiver 2 is (9).

The nested lattices \((\Lambda, L_1)\) for Receiver 1 and \((\Gamma, L_2)\) for Receiver 2 are thus constructed so as to have very specific properties.

- They are "good" lattices for communication by themselves, ensuring that they can be used for encoding and decoding in a point-to-point communication.
- Important: Lattices \( \Gamma \) and \( \Lambda \) are related by a scaling factor. This relationship essentially the overall signal transmitted to have structure. In particular, the overall signal is a linear combination of two (possibly dithered) lattice points from the same lattice.

**Communication:** We desire to communicate lattice points \( \lambda \in \Lambda \) to Receiver 1 and \( \gamma \in \Gamma \) to Receiver 2. First, we choose:

\[
\mathbf{V} = [\gamma] \mod L_2,
\]

We now construct the dirty-paper-encoded output for Receiver 1 as follows:

\[
\mathbf{U} = [\lambda - h_{12} \mathbf{V} - \Delta_1] \mod L_1,
\]

where the dither \( \Delta_1 \) is a discrete-valued random variable uniformly distributed over \( \Lambda \cap V_L \). By construction, \( \mathbf{V} \) is an element of \( \Lambda \). Thus, \( \lambda - \alpha_1 h_{12} \mathbf{V} \) is an element of \( \Lambda \). Ultimately, the transmitted vector at time \( i \) is given by

\[
\mathbf{X}_i = aU_i + bV_i,
\]

where \( U_i \) and \( V_i \) denote the \( i \)th entries of vectors \( \mathbf{U} \) and \( \mathbf{V} \), respectively. Note that the dither \( \Delta_1 \) is constant for the entire duration of transmission.

**IV. Decoding Strategy**

Before we describe the decoding strategy based on belief propagation that we plan to use, we provide a brief description of the strategy used in [4] and [10] generalized to MISO broadcast channels. As the work in [4] and [10] forms the basis for our paper, this background is essential for us to proceed further.

At time \( i \), Receiver 1 observes the channel given by

\[
\begin{align*}
    \frac{1}{h_{11}} Y_{1i} &= \frac{1}{h_{11}} \left( h_1^T \mathbf{a} U_i + h_1^T \mathbf{b} V_i + N_{1i} \right) \\
    &= U_i + \frac{h_{12}}{h_{11}} V_i + \frac{1}{h_{11}} N_{1i}.
\end{align*}
\]

The dirty-paper decoding for Receiver 1 requires the construction of:

\[
\begin{align*}
    Y'_1 &= \left[ \frac{1}{h_{11}} \mathbf{Y}_1 + \Delta_1 \right] \mod L_1 \\
    &= \left[ \lambda - \frac{h_{12}}{h_{11}} \mathbf{V} - \Delta_1 \right] + \frac{h_{12}}{h_{11}} \mathbf{V} + N_1 \mod L_1 \\
    &= \left[ \lambda + \frac{1}{h_{11}} N_1 \right] \mod L_1.
\end{align*}
\]

Meanwhile, Receiver 2 observes

\[
\begin{align*}
    Y'_2 &= \frac{1}{h_{22}} Y'_2 = h_2^T \mathbf{b} \mathbf{V} + h_2^T \mathbf{a} \mathbf{U} + N_2 \\
    &= \mathbf{V} + \frac{h_{21}}{h_{22}} \mathbf{U} + \frac{1}{h_{22}} N_2.
\end{align*}
\]

Receivers 1 and 2 use lattice decoding on \( \mathbf{Y}'_1 \) and \( \mathbf{Y}'_2 \) respectively to determine the corresponding messages. Note that the encoding and lattice-decoding steps specified above are not practically feasible in general as they are equivalent to lattice quantization, which is well-known to be \( \mathcal{N} \mathcal{P} \). In the next section, we describe how the encoding and decoding steps can be approximated to render them tractable using a polynomial-time algorithm.

**V. Dirty-Paper Coding Using Low-Density Lattices**

To render the steps in the encoding and decoding (12) – (15) possible, we use the framework of low-density lattices [16], [17]. In particular, in this work we use low-density Construction-A lattices as used in [17]. A majority of Construction-A lattices are known to be "good" [12], and thus we focus on this ensemble in generating our low-density lattice. Next, we do the following:

1) The encoding in (12) is performed using matrix inversion and belief propagation. Note that the encoding, has, in general, exponential complexity. This combination of channel inversion with belief propagation thus only approximates the steps in the encoding process.

2) The lattice decoding steps in (14) and (15) is performed using belief propagation. This is similar to the belief propagation used to decode non-binary low-density parity-check (LDPC) codes [16], [18], [19].
Fig. 2. Performance of structured dirty-paper coding as a function of block length

This combination of channel inversion and belief propagation renders the encoding and decoding steps tractable. In the next step, we present simulation results using these steps.

VI. SIMULATION RESULTS

To demonstrate the performance of low-density lattices for the broadcast channel, we choose a set of nested lattices \((\Lambda, L_1)\) for Receiver 1 and \((\Gamma, L_2)\) for Receiver 2 such that the resulting rate equals \(R = \frac{1}{6} \log_2 p\) for each receiver. The encoding and decoding for Receiver 2 are the same as that for a conventional point-to-point system (examples of which can be found in [16], [17]), and so we focus here on determining the efficacy of the dirty-paper-coding process conducted for Receiver 1. Fig. 2 presents the symbol-error rate versus SNR for Receiver 1 for \(p = 3\) for block lengths 300 and 3000. We use (non-binary) \((3, 6)\)-regular and \((4, 6)\)-regular LDPC codes for fine and coarse lattices, respectively. We see that the performance of our code for block length equal to 3000 and symbol-error rates of \(10^{-5}\) or less is within 5 dB from point-to-point channel capacity [13]. Note that this is significantly better than treating interference either entirely or in-part as noise. In this simulation setting, the effective channel gain parameters are set to \(h_{11} = 4, h_{12} = 4, h_{21} = 4\) and \(h_{22} = 8\). Mapping of messages to codewords is performed following the same procedure as in [18]. Decoding is performed using belief propagation and an error is declared if the belief-propagation decoder does not converge after 500 iterations. We observed that, on an average, very few iterations (approximately 3) were needed for the belief-propagation decoder to converge for SNR of 6 dB or greater. The gap between the capacity limit and current performance results from multiple factors: First, the encoding algorithm is currently performed using matrix inversion which may not be very efficient. Secondly, the shaping factor \(\alpha\) (as in (3)) is set to one in our encoding and decoding procedures for simplicity.

VII. CONCLUSION

In this paper, we present a mechanism for approximating dirty-paper coding using (low-density) lattices. Using a combination of matrix-inversion based encoding and belief-propagation-based decoding, we find that we can construct nested lattices and precode for interference in a MISO broadcast channel.

In future work, we plan on reducing the gap between current performance and the AGN capacity limit by improving the low density lattice encoding mechanism.

ACKNOWLEDGMENT

We thank Dr. Giuseppe Caire for useful discussions and comments.

REFERENCES