Lattice Index Coding for the Broadcast Channel

Lakshmi Natarajan, Yi Hong, and Emanuele Viterbo
Department of Electrical & Computer Systems Engineering
Monash University, Clayton, VIC 3800, Australia
{lakshmi.natarajan, yi.hong, emanuele.viterbo}@monash.edu

***Abstract*—The index coding problem involves a sender with K messages to be transmitted across a broadcast channel, and a set of receivers each of which demands a subset of the K messages while having prior knowledge of a different subset as side information. We consider the specific instance of noisy index coding where the broadcast channel is Gaussian and every receiver demands all the messages from the source. We construct *lattice index codes* for this channel by encoding the K messages individually using K modulo lattice constellations and transmitting their sum modulo a shaping lattice. We introduce a design metric called *side information gain* that measures the advantage of a code in utilizing the side information at the receivers, and hence its quality as an index code. Based on the Chinese remainder theorem, we then construct lattice index codes for the Gaussian broadcast channel. Among all lattice index codes constructed using any densest lattice of a given dimension, our codes achieve the maximum side information gain.**

***Index Terms*—Chinese remainder theorem, Gaussian broadcast channel, index coding, lattice codes, side information.**

I. Introduction

The classical noiseless index coding problem consists of a sender with K independent messages $w_1, \dots, w_K$, and a noiseless binary broadcast channel, where each receiver demands a subset of the messages, while knowing the values of a different subset of messages as side information. The transmitter is required to broadcast a coded packet, at the least possible rate, to meet the demands of all the receivers (see [1]–[3] and references therein). In the noisy version of this problem, the messages are to be transmitted across a broadcast channel with additive white Gaussian noise (AWGN) at the receivers (see [4]–[8] and references therein). The exact capacity region (the achievable rates of the K messages) with general message demands and side informations is known only for the two-receiver case [4], [5].

In this paper, we consider the special case of noisy index coding where every receiver demands all the messages at the source. The capacity region of this class of channels follows from the results in [8]. Denote a receiver by the pair (SNR, S), where SNR is the signal-to-noise ratio, and $S \subset \{1, \dots, K\}$ is the index set of the messages $w_S = (w_k, k \in S)$ whose values are known at the receiver as side information. Note that this includes the case $S = \varnothing$, i.e., no side information. Let $R_1, \dots, R_K$ be the rates of the individual messages in bits per dimension (b/dim), i.e., the number of bits to be transmitted per each use of the broadcast channel. The source entropy is $R = R_1 + \cdots + R_K$, and the *side information rate* at (SNR, S) is $R_S \triangleq \sum_{k \in S} R_k$. The rate tuple $(R_1, \dots, R_K)$ is achievable if and only if [8]

$$\tfrac{1}{2}\log_2(1 + \mathsf{SNR}) > H(w_1, \dots, w_K \,|\, w_S) = R - R_S,$$

for every receiver (SNR, S). Consequently, at high message rates, the presence of the side information corresponding to S at a receiver reduces the minimum required SNR from approximately 2^{2R} to $2^{2(R-R_S)}$, or equivalently, by a factor of $R_S \times 20\log_{10} 2$ dB $\approx 6R_S$ dB. Hence, a capacity-achieving index code allows a receiver to transform each bit per dimension of side information into an apparent SNR gain of approximately 6 dB.

The notion of *multiple interpretation* was introduced in [9] as a property of error correcting codes that allows the receiver error performance to improve with the availability of side information. Binary multiple interpretation codes based on nested convolutional and cyclic codes were constructed in [10] and [11], respectively. These codes can be viewed as index codes for the noisy binary broadcast channel.

In this work, we propose *lattice index codes* $\mathscr{C}$ for the AWGN broadcast channel, in which the K messages are individually mapped to K modulo lattice constellations, and the transmit symbol is generated as the sum of the individual symbols modulo a shaping lattice. Given the value of w_S as side information, the optimal decoder restricts its choice of symbols to a subset of $\mathscr{C}$, thereby increasing the minimum squared Euclidean distance between the valid codewords. We use this squared distance gain, normalized by the side information rate R_S, as the design metric, and call it the *side information gain* of the code $\mathscr{C}$. We first motivate our results using a simple one-dimensional lattice code (Section II), and then show that $20\log_{10} 2 \approx 6$ dB/b/dim is an upper bound on the side information gain of lattice index codes constructed from densest lattices (Section III). This upper bound characterizes the maximum squared distance gain, and is independent of the information theoretic result of [8], which characterizes the SNR gain asymptotically in both the code dimension and probability of error. Based on the Chinese remainder theorem, we construct lattice index codes for the AWGN channel with side information gain $20\log_{10} 2$ dB/b/dim (Section IV). These codes have the maximum side information gain among all lattice index codes whose underlying lattice is densest in its dimension.

This work was supported by the Australian Research Council under Grant Discovery Project No. DP130100103 and the 2013 Monash Faculty of Engineering Seed Funding Scheme.

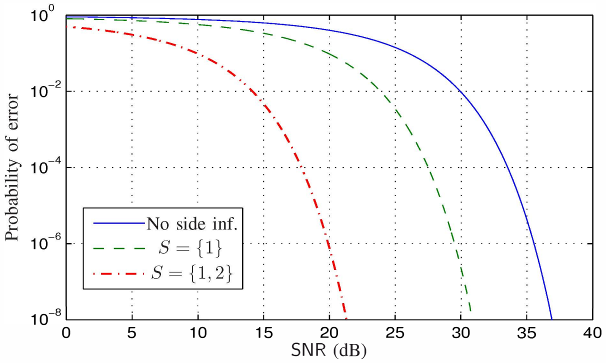

Fig. 1. Performance of the code of Example 1 for three different receivers.

Notation: The symbol S^{c} denotes the complement of the set S, and $\varnothing$ is the empty set.

II. Motivating Example

In this section, we illustrate the key idea behind our construction using a simple one-dimensional lattice index code $\mathscr{C} \subset \mathbb{Z}$ (Example 1). Let $w_1, \dots, w_K$ be K independent messages at the source with alphabets $\mathcal{W}_1, \dots, \mathcal{W}_K$, respectively. The transmitter jointly encodes the information symbols $w_1, \dots, w_K$, to a codeword $x \in \mathscr{C}$, where $\mathscr{C} \subset \mathbb{R}^n$ is an n-dimensional constellation. The rate of the k^{th} message is $R_k = {}^1\!/\!{}_n \log_2 |\mathcal{W}_k|$ b/dim, $k = 1, \dots, K$. Given the channel output $y = x + z$, where z is the additive white Gaussian noise, and the side information $w_S = a_S$, i.e., $w_k = a_k$ for $k \in S$, the maximum-likelihood decoder at the receiver (SNR, S) restricts its search to the subcode $\mathscr{C}_{a_S} \subset \mathscr{C}$ obtained by expurgating all the codewords in $\mathscr{C}$ that correspond to $w_S \neq a_S$. Denote the minimum distance between any two points in $\mathscr{C}$ by d_0. Let d_{a_S} be the minimum distance of the subcode $\mathscr{C}_{a_S}$, and d_S be the minimum of d_{a_S} over all possible values a_S of side information w_S. Then the minimum squared distance gain corresponding to the side information index set S is $10 \log_{10} \left({}^{d_S^2}\!/\!{}_{d_\bullet^2}\right)$ dB.

The performance improvement at the receiver due to S is observed as a shift in the probability of error curve (versus SNR) to the left. The squared distance gain $10 \log_{10} \left({}^{d_S^2}\!/\!{}_{d_\bullet^2}\right)$ is a first-order estimate of this apparent SNR gain. Each bit per dimension of side information provides a gain of at least

$$\Gamma(\mathscr{C}) \triangleq \min_{\varnothing \subsetneq S \subsetneq \{1,\dots,K\}} \frac{10 \log_{10} \left({}^{d_S^2}\!/\!{}_{d_\bullet^2}\right)}{R_S}, \tag{1}$$

where $R_S = \sum_{k \in S} R_k$. We call $\Gamma(\mathscr{C})$ the *side information gain* of the code $\mathscr{C}$, and its unit is dB/b/dim. Using the normalization factor R_S in (1), we measure the distance gain with respect to the amount of side information available at a receiver. For $\mathscr{C}$ to be a good index code for the AWGN broadcast channel, we require that 1) $\mathscr{C}$ be a good point-to-point AWGN code, in order to minimize the SNR requirement at the receiver with no side information; and 2) $\Gamma(\mathscr{C})$ be large, so as to maximize the minimum gain from the availability of any amount of side information at the other receivers.

Example 1. Consider $K = 3$ independent messages w_1, w_2, and w_3 assuming values from $\mathcal{W}_1 = \{0, 1\}$, $\mathcal{W}_2 = \{0, 1, 2\}$ and $\mathcal{W}_3 = \{0, 1, 2, 3, 4\}$, respectively. The three messages are encoded to a code $\mathscr{C} \subset \mathbb{Z}$ using the function

$$x = 15w_1 + 10w_2 + 6w_3 \mod 30,$$

where the operation $a \bmod 30$ gives the unique remainder in $\mathscr{C} = \{-15, -14, \dots, 13, 14\}$ when the integer a is divided by 30. Using the Chinese remainder theorem [12], it is easy to verify that $\mathscr{C}$ is the set of all possible values that the transmit symbol x can assume. Since the dimension of $\mathscr{C}$ is $n = 1$, the rate of the k^{th} message is $R_k = \log_2 |\mathcal{W}_k|$ b/dim, i.e.,

$$R_1 = 1,\ R_2 = \log_2 3,\ \text{and}\ R_3 = \log_2 5 \text{ b/dim}.$$

With no side information ($S = \varnothing$), a receiver decodes the channel output to the nearest point in $\mathscr{C}$, with the corresponding minimum inter-codeword distance $d_0 = 1$. With $S = \{1\}$, the receiver knows the value of the first message $w_1 = a_1$. The decoder of this receiver restricts the choice of transmit symbols to the subcode

$$\mathscr{C}_{a_1} = \{15a_1 + 10w_2 + 6w_3 \mod 30 \,|\, w_2 \in \mathcal{W}_2, w_3 \in \mathcal{W}_3\}.$$

Any two points in this subcode differ by $10\Delta w_2 + 6\Delta w_3$, where Δw_2 and Δw_3 are integers, not both equal to zero. Since the greatest common divisor (gcd) of 10 and 6 is $\gcd(10, 6) = 2$, the minimum non-zero magnitude of $10\Delta w_2 + 6\Delta w_3$ is 2 [12]. Hence, the minimum distance corresponding to the side information index set $S = \{1\}$ is $d_S = 2$. The side information rate is $R_S = R_1 = 1$ b/dim, which equals $\log_2 d_S$.

When $S = \{1, 2\}$, the set of possible transmit symbols is

$$\mathscr{C}_{(a_1, a_2)} = \{15a_1 + 10a_2 + 6w_3 \mod 30 | w_3 \in \mathcal{W}_3\},$$

where $w_1 = a_1$ and $w_2 = a_2$ are known. The minimum distance of this subcode is $d_S = 6$, and the side information rate is $R_S = R_1 + R_2 = \log_2 6 = \log_2 d_S$ b/dim.

Similarly, for every choice of $\varnothing \subsetneq S \subsetneq \{1, 2, 3\}$, we have $R_S = \log_2 d_S$, i.e., the minimum distance grows exponentially in the side information rate. As will be shown in Section IV, this property is satisfied by all the proposed lattice index codes. Using $R_S = \log_2 d_S$ and $d_0 = 1$ in (1), we see that the side information gain is $\Gamma = 20 \log_{10} 2 \approx 6$ dB/b/dim. In Section III-C we show that this is the maximum side information gain achievable by any index code $\mathscr{C} \subset \mathbb{Z}$ in which the messages are linearly encoded. Fig. 1 shows the performance of the code with $S = \varnothing$, $S = \{1\}$ and $S = \{1, 2\}$. At the probability of error of 10^{-4}, $S = \{1\}$ and $S = \{1, 2\}$ provide SNR gains of 6 dB and 15.6 dB over $S = \varnothing$. This is close to the corresponding squared distance gains of $10 \log_{10} \left(2^2\right)$ dB and $10 \log_{10} \left(6^2\right)$ dB, respectively. ■

Example 2. Labelling a given constellation $\mathscr{C}$ by set partitioning [13] is apparently a related problem, but it does not necessarily provide good index codes. In set partitioning with binary 'labels' $w_1, \dots, w_K$, the constellation $\mathscr{C}$ is recursively partitioned into two smaller signal sets with larger minimum

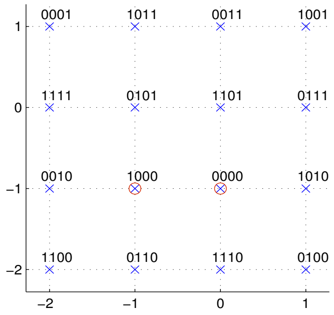

Fig. 2. A set partition labelling of 16-QAM. The two points marked with circles form the subcode for the side information $(w_2, w_3, w_4) = (0, 0, 0)$.

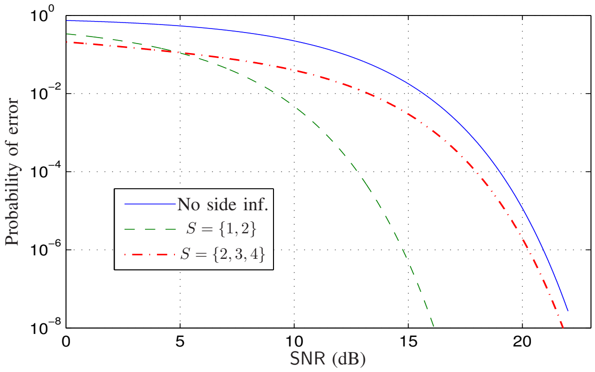

Fig. 3. Performance of set partition labelling.

distance. With $S = \{1, 2, \ldots, k\}$, for some $k < K$, the set of points with a given label $w_S = a_S$ forms one of the 2^k k^{th}-level partitions of $\mathscr{C}$. The minimum distance of the partition improves with increasing k. Fig. 2 shows one such labelling of 16-QAM with $K = 4$, where the knowledge of the value of the first k bits, $w_1, \ldots, w_k$, increases the minimum distance from $d_0 = 1$ to $d_S = \sqrt{2^k}$. However, this does not guarantee squared distance gain for every side information index set S. For instance, from Fig. 2, we observe that the side information $(w_2, w_3, w_4) = (0, 0, 0)$ does not provide any improvement in minimum distance. The performance of the code of Fig. 2 for $S = \varnothing$, $S = \{1, 2\}$ and $S = \{2, 3, 4\}$ is shown in Fig. 3. When the error rate is $P_e = 10^{-4}$, the knowledge of the first two bits provides an SNR gain of 6.2 dB. However, the SNR gain with $S = \{2, 3, 4\}$ is only 1 dB at $P_e = 10^{-4}$ and is smaller for diminishing P_e. ■

III. Lattice Index Codes

In this section, we review the necessary background on lattices and lattice codes based on [14]–[16], introduce lattice index codes, and then derive an upper bound on the side information gain of such codes constructed from the densest lattices.

A. *Lattices and lattice codes*

An n-dimensional *lattice* in $\mathbb{R}^n$ is a discrete additive subgroup $\Lambda = \{Gz \,|\, z \in \mathbb{Z}^n\}$, where the full-ranked matrix $G \in \mathbb{R}^{n \times n}$ is called the *generator matrix* of Λ. Since the difference between any two lattice points is also a lattice point, the *minimum distance* $d_{\min}(\Lambda)$ between any two points in Λ is the Euclidean length of the shortest non-zero vector of Λ. The *closest lattice point quantizer* $Q_\Lambda : \mathbb{R}^n \to \Lambda$ is

$$Q_\Lambda(x) = \lambda \text{ if } \|x - \lambda\| \leq \|x - \lambda'\| \text{ for every } \lambda' \in \Lambda,$$

where ties, if any, are broken systematically. The *fundamental Voronoi region* $\mathcal{V}_\Lambda$ is the set of all points in $\mathbb{R}^n$ that are mapped to 0 under Q_Λ. The volume of the fundamental region $\text{Vol}(\Lambda) = \int_{\mathcal{V}_\Lambda} dx$ is related to the generator matrix G as $\text{Vol}(\Lambda) = |\det G|$. The *packing radius* $r_\Lambda = {}^{d_{\min}(\Lambda)}\!/_2$ is the radius of the largest n-dimensional sphere contained in the Voronoi region $\mathcal{V}_\Lambda$. The *center density* of Λ is

$$\delta(\Lambda) = \frac{r_\Lambda^n}{\text{Vol}(\Lambda)} = \frac{\left({}^{d_{\min}(\Lambda)}\!/_2\right)^n}{\text{Vol}(\Lambda)}. \tag{2}$$

If Λ is scaled so that $r_\Lambda = 1$, then δ is the average number of lattice points per unit volume in $\mathbb{R}^n$. For the same values of average transmit power and minimum distance, a constellation carved from a lattice with a higher value of δ has a larger size, and hence, a higher coding gain. The densest lattices are known for dimensions $n = 1, 2, \ldots, 8$ and $n = 24$ [14], [17]. For $n = 1, \ldots, 8$, the densest lattices are $\mathbb{Z}, A_2, D_3, D_4, D_5, E_6, E_7$ and E_8, respectively, while the Leech lattice Λ_{24} is densest in 24 dimensions.

The *modulo*-Λ operation, $x \bmod \Lambda = x - Q_\Lambda(x) \in \mathcal{V}_\Lambda$, is the difference between a vector and its closest lattice point, and it satisfies the relation

$$(x_1 + x_2) \bmod \Lambda = (x_1 \bmod \Lambda + x_2) \bmod \Lambda. \tag{3}$$

Let $\Lambda_{\mathsf{s}} \subset \Lambda$ be a sub-lattice of Λ, and $\Lambda/\Lambda_{\mathsf{s}}$ be the quotient group of the cosets of Λ_{s} in Λ. Each coset of $\Lambda/\Lambda_{\mathsf{s}}$ can be identified by its unique representative contained in $\mathcal{V}_{\Lambda_{\mathsf{s}}}$. We will identify the group $\Lambda/\Lambda_{\mathsf{s}}$ with the group of coset leaders $\Lambda \cap \mathcal{V}_{\Lambda_{\mathsf{s}}} = \Lambda \bmod \Lambda_{\mathsf{s}}$, where addition is performed modulo Λ_{s}. Further, $|\Lambda/\Lambda_{\mathsf{s}}| = |\Lambda \bmod \Lambda_{\mathsf{s}}| = {}^{\text{Vol}(\Lambda_{\mathsf{s}})}\!/_{\text{Vol}(\Lambda)}$. The constellation $\Lambda/\Lambda_{\mathsf{s}}$ is called a *(nested) lattice code*, and Λ_{s} is its *shaping lattice* [15], [16].

B. *Lattice index codes*

Consider K lattices $\Lambda_1, \ldots, \Lambda_K$, with a common sub-lattice $\Lambda_{\mathsf{s}} \subset \Lambda_k$, $k = 1, \ldots, K$. We will use the lattice constellations $\Lambda_1/\Lambda_{\mathsf{s}}, \ldots, \Lambda_K/\Lambda_{\mathsf{s}}$ as the alphabets $\mathcal{W}_1, \ldots, \mathcal{W}_K$ of the K messages at the source.

Definition 1. A *lattice index code* for K messages consists of K lattice constellations $\Lambda_1/\Lambda_{\mathsf{s}}, \ldots, \Lambda_K/\Lambda_{\mathsf{s}}$, and the injective linear encoder map $\rho : \Lambda_1/\Lambda_{\mathsf{s}} \times \cdots \times \Lambda_K/\Lambda_{\mathsf{s}} \to \mathscr{C}$ given by

$$\rho(x_1, \ldots, x_K) = (x_1 + \cdots + x_K) \bmod \Lambda_{\mathsf{s}}, \tag{4}$$

where $\mathscr{C}$ is the set of all possible values of the transmit symbol $x = \rho(x_1, \ldots, x_K)$. ■

The injectivity of ρ in Definition 1 ensures unique decodability of codewords. We now relate some properties of a lattice index code to those of its component lattices $\Lambda_1, \ldots, \Lambda_K$ and Λ_{s}.

The transmit codebook $\mathscr{C}$: Let $\Lambda = \Lambda_1 + \cdots + \Lambda_K$ be the lattice generated by the union of the lattices $\Lambda_1, \ldots, \Lambda_K$. It follows from (4) that $x_1 + \cdots + x_K \in \Lambda$, and hence $x \in \Lambda/\Lambda_{\sf s}$. On the other hand, every point in Λ is the sum of K lattice points, one each from $\Lambda_1, \ldots, \Lambda_K$. It follows from (3) that every point in the lattice constellation $\Lambda/\Lambda_{\sf s}$ is the $\bmod\ \Lambda_{\sf s}$ sum of K points, from $\Lambda_1/\Lambda_{\sf s}, \ldots, \Lambda_K/\Lambda_{\sf s}$, respectively. Hence, the transmit codebook is $\mathscr{C} = \Lambda/\Lambda_{\sf s}$.

Message rates: If Λ is an n-dimensional lattice, the rate of the k^{th} message is

$$R_k = \frac{1}{n}\log_2 |\Lambda_k/\Lambda_{\sf s}| = \frac{1}{n}\log_2 \frac{\text{Vol}(\Lambda_{\sf s})}{\text{Vol}(\Lambda_k)} \text{ b/dim.}$$

Minimum distance: Since $\mathscr{C} = \Lambda/\Lambda_{\sf s}$ is carved from the lattice Λ, the minimum inter-codeword distance with no side information is $d_0 = d_{\min}(\Lambda)$. Suppose that a receiver has side information of the messages with indices S, say $x_S = a_S$ (i.e., $x_k = a_k$, $k \in S$). The subcode decoded by this receiver is

$$\begin{aligned} \mathscr{C}_{a_S} &= \left(\sum_{k\in S} a_k + \sum_{k\in S^{\sf c}} \Lambda_k/\Lambda_{\sf s}\right) \bmod \Lambda_{\sf s} \\ &= \left(\sum_{k\in S} a_k + \sum_{k\in S^{\sf c}} \Lambda_k\right) \bmod \Lambda_{\sf s}, \end{aligned}$$

where we have used (3). Thus, $\mathscr{C}_{a_S}$ is a code carved from a translate of the lattice $\sum_{k\in S^{\sf c}} \Lambda_k$, and hence its minimum distance is $d_S = d_{\min}\left(\sum_{k\in S^{\sf c}} \Lambda_k\right)$.

Example 3. The code in Example 1 is a lattice index code with $K = 3$, $\Lambda_1 = 15\mathbb{Z}$, $\Lambda_2 = 10\mathbb{Z}$, $\Lambda_3 = 6\mathbb{Z}$, $\Lambda_{\sf s} = 30\mathbb{Z}$ and $\Lambda = 15\mathbb{Z} + 10\mathbb{Z} + 6\mathbb{Z} = \mathbb{Z}$. ■

C. An upper bound on the side information gain

With $S = \{1, \ldots, K-1\}$, the minimum distance is $d_S = d_{\min}\left(\sum_{k\in S^{\sf c}} \Lambda_k\right) = d_{\min}(\Lambda_K)$, and the side information rate is

$$\begin{aligned} R_S &= R_1 + \cdots + R_{K-1} = R - R_K = \frac{1}{n}\log_2|\mathscr{C}| - R_K \\ &= \frac{1}{n}\log_2|\Lambda/\Lambda_{\sf s}| - \frac{1}{n}\log_2|\Lambda_K/\Lambda_{\sf s}| \\ &= \frac{1}{n}\log_2\frac{\text{Vol}(\Lambda_{\sf s})}{\text{Vol}(\Lambda)} - \frac{1}{n}\log_2\frac{\text{Vol}(\Lambda_{\sf s})}{\text{Vol}(\Lambda_K)} = \frac{1}{n}\log_2\frac{\text{Vol}(\Lambda_K)}{\text{Vol}(\Lambda)}. \end{aligned}$$

Representing the volume of the fundamental region in terms of the minimum distance $d_{\min}$ and the center density δ (see (2)),

$$\begin{aligned} R_S &= \frac{1}{n}\log_2\left(\frac{d_{\min}(\Lambda_K)}{d_{\min}(\Lambda)}\right)^n + \frac{1}{n}\log_2\frac{\delta(\Lambda)}{\delta(\Lambda_K)} \\ &= \log_2\frac{d_S}{d_0} + \frac{1}{n}\log_2\frac{\delta(\Lambda)}{\delta(\Lambda_K)}. \end{aligned} \tag{5}$$

If Λ is the densest lattice in n dimensions, then $\delta(\Lambda) \geq \delta(\Lambda_K)$, and hence $R_S \geq \log_2\left({d_S}/{d_\bullet}\right)$. Thus the side information gain of $\mathscr{C}$ can be upper bounded as follows

$$\begin{aligned} \Gamma(\mathscr{C}) &= \min_S \frac{20\log_{10}\left({d_S}/{d_\bullet}\right)}{R_S} \leq \frac{20\log_{10}\left({d_S}/{d_0}\right)}{R_S} \\ &\leq \frac{20\log_{10}\left({d_S}/{d_\bullet}\right)}{\log_2\left({d_S}/{d_\bullet}\right)} = 20\log_{10}2 \approx 6 \text{ dB/b/dim.} \end{aligned}$$

This upper bound is valid when Λ is the densest lattice in n-dimensions, such as when Λ is $\mathbb{Z}$ or A_2. When Λ is not the densest lattice in $\mathbb{R}^n$, for example when $\Lambda = \mathbb{Z}^2$, it is possible to have $\delta(\Lambda_K) > \delta(\Lambda)$. In such cases, from (5), $R_S < \log_2\left({d_S}/{d_\bullet}\right)$, and Γ may exceed ~ 6 dB/b/dim. Note that Γ is a relative gain measured with respect to the performance of $\mathscr{C} = \Lambda/\Lambda_{\sf s}$ with no side information. Any amount of side information gain available over and above ~ 6 dB/b/dim is due to the lower packing efficiency of Λ when compared to Λ_K, and hence due to the inefficiency of $\mathscr{C}$ as a code in the point-to-point AWGN channel.

IV. Construction of lattice index codes based on the Chinese remainder theorem

Consider K distinct prime integers $p_1, \ldots, p_K \in \mathbb{Z}$, and their product $M = \prod_{k=1}^K p_k$. The Chinese remainder theorem [12, p. 159] states that the direct product $\mathbb{Z}/p_1\mathbb{Z} \times \cdots \times \mathbb{Z}/p_K\mathbb{Z}$ is isomorphic to $\mathbb{Z}/M\mathbb{Z}$ as a ring. The one-to-one correspondence between them is given by

$$(w_1, \ldots, w_K) \to w_1M_1 + w_2M_2 + \cdots + w_KM_K \bmod M\mathbb{Z},$$

where $w_k \in \mathbb{Z}/p_k\mathbb{Z}$ and $M_k = {M}/{p_k} = \prod_{\ell\neq k} p_\ell$. Since w_kM_k belongs to $M_k\mathbb{Z}/M\mathbb{Z}$, we observe that encoding the K source messages individually using the constellations $M_1\mathbb{Z}/M\mathbb{Z}, \ldots, M_K\mathbb{Z}/M\mathbb{Z}$, and generating the transmit symbol as their modulo-$M\mathbb{Z}$ sum yields an injective encoding map. Further, given the side information $w_S = a_S$, the minimum distance d_S between the valid codewords can be readily obtained as $\gcd(M_k, k \in S^{\sf c})$ (cf. Example 1). The codebook $\mathbb{Z}/M\mathbb{Z}$ can be thought of as a lattice index code built over the one-dimensional lattice $\Lambda = \mathbb{Z}$. We apply this encoding technique to arbitrary lattices Λ and show that the resulting lattice index codes provide large side information gains.

Let $\Lambda \subset \mathbb{R}^n$ be any n-dimensional lattice, and G its generator matrix. Let $p_1, \ldots, p_K$ be distinct primes, $M = \prod_{k=1}^K p_k$ and $M_k = {M}/{p_k}$. We construct our lattice index code by setting

$$\Lambda_{\sf s} = M\Lambda \text{ and } \Lambda_k = M_k\Lambda,\ k = 1, \ldots, K. \tag{6}$$

The cardinality of the k^{th} message is

$$|\Lambda_k/\Lambda_{\sf s}| = \frac{\text{Vol}\,(M\Lambda)}{\text{Vol}\,(M_k\Lambda)} = \frac{|\det(MG)|}{|\det(M_kG)|} = \frac{M^n}{M_k^n} = p_k^n,$$

and its rate is $R_k = {1}/{n}\log_2|\Lambda_k/\Lambda_{\sf s}| = \log_2 p_k$ b/dim.

Example 4. The code of Example 1 can be obtained by using $\Lambda = \mathbb{Z}$, and $(p_1, p_2, p_3) = (2, 3, 5)$. ■

In the following lemmas, we show that (6) generates a lattice index code with $\Gamma \approx 6$ dB/b/dim. Thus, when Λ is the densest lattice in its dimension, the proposed construction achieves the optimal side information gain over all lattice index codes constructed based on Λ.

Lemma 1. *For any S,* $\gcd(M_k, k \in S^{\sf c}) = \prod_{\ell\in S} p_\ell$.

Proof: Since p_k is not a factor of M_k, the primes p_k, $k \in S^{\sf c}$, are not factors of $\gcd(M_k, k \in S^{\sf c})$. The lemma follows by observing that $\prod_{\ell\in S} p_\ell$ divides M_k, $k \in S^{\sf c}$. ■

Lemma 2. *With the lattices $\Lambda_1, \dots, \Lambda_K$ and Λ_{s} defined as* (6)*,*

(i) the encoding map ρ in Definition 1 generates a lattice index code with transmit codebook $\mathscr{C} = \Lambda/\Lambda_{\mathsf{s}}$; and

(ii) for every choice of S, $\sum_{k \in S^{\mathsf{c}}} \Lambda_k = \prod_{\ell \in S} p_\ell \, \Lambda$.

Proof: In order to prove Part *(i)*, we need to show that ρ is injective, and $\Lambda_1 + \cdots + \Lambda_K = \Lambda$. From Lemma 1, $\gcd(M_k, k \in S^{\mathsf{c}}) = \prod_{\ell \in S} p_\ell$ for every choice of S. Hence, there exists a tuple $(b_k, k \in S^{\mathsf{c}})$ of integers such that $\sum_{k \in S^{\mathsf{c}}} b_k M_k = \prod_{\ell \in S} p_\ell$. It follows that, for every $\lambda \in \Lambda$, we have $\prod_{\ell \in S} p_\ell \lambda = \sum_{k \in S^{\mathsf{c}}} b_k M_k \lambda$, hence $\prod_{\ell \in S} p_\ell \, \Lambda \subset \sum_{k \in S^{\mathsf{c}}} M_k \Lambda$. Considering cosets modulo Λ_{s},

$$\prod_{\ell \in S} p_\ell \, \Lambda \, / \Lambda_{\mathsf{s}} \subset \sum_{k \in S^{\mathsf{c}}} \Lambda_k / \Lambda_{\mathsf{s}}. \tag{7}$$

Let $\rho|_{S^{\mathsf{c}}}$ be the restriction of the encoding map (4) to the message symbols with indices in S^{c}, i.e., $\rho|_{S^{\mathsf{c}}}(x_k, k \in S^{\mathsf{c}}) = \sum_{k \in S^{\mathsf{c}}} x_k \bmod \Lambda_{\mathsf{s}}$. Note that $\sum_{k \in S^{\mathsf{c}}} \Lambda_k / \Lambda_{\mathsf{s}}$ is the image of the map $\rho|_{S^{\mathsf{c}}}$. From (7), $\prod_{\ell \in S} p_\ell \Lambda / \Lambda_{\mathsf{s}}$ is a subset of this image. The cardinality

$$\left| \prod_{\ell \in S} p_\ell \Lambda / \Lambda_{\mathsf{s}} \right| = \frac{|M|^n \mathrm{Vol}(\Lambda)}{|\prod_{\ell \in S} p_\ell|^n \mathrm{Vol}(\Lambda)} = \prod_{k \in S^{\mathsf{c}}} |p_k|^n$$

of this subset of the image of $\rho|_{S^{\mathsf{c}}}$ equals the cardinality $\prod_{k \in S^{\mathsf{c}}} |\Lambda_k / \Lambda_{\mathsf{s}}| = \prod_{k \in S^{\mathsf{c}}} |p_k|^n$ of the domain of $\rho|_{S^{\mathsf{c}}}$. Hence, we conclude that $\rho|_{S^{\mathsf{c}}}$ is an injective map, and the subset $\prod_{\ell \in S} p_\ell \Lambda / \Lambda_{\mathsf{s}}$ equals the entire image $\sum_{k \in S^{\mathsf{c}}} \Lambda_k / \Lambda_{\mathsf{s}}$. This implies that $\prod_{\ell \in S} p_\ell \Lambda = \sum_{k \in S^{\mathsf{c}}} \Lambda_k$, proving Part *(ii)* of this lemma. Choosing $S = \varnothing$, we observe that $\rho|_{S^{\mathsf{c}}} = \rho$ is injective, and $\sum_{k=1}^{K} \Lambda_k = \Lambda$. Hence, the transmit codebook $\mathscr{C} = \sum_{k=1}^{K} \Lambda_k / \Lambda_{\mathsf{s}} = \Lambda / \Lambda_{\mathsf{s}}$. This proves Part *(i)*. ■

Lemma 3. *For every choice of S, $R_S = \log_2 \left({}^{d_S}/_{d_\bullet} \right)$.*

Proof: From Lemma 2, we have $d_0 = d_{\min}(\Lambda)$, and $d_S = d_{\min}\left(\sum_{k \in S^{\mathsf{c}}} \Lambda_k\right) = d_{\min}\left(\prod_{\ell \in S} p_\ell \Lambda\right)$, and hence $d_S = \prod_{\ell \in S} p_\ell d_{\min}(\Lambda) = \prod_{\ell \in S} p_\ell d_0$. The side information rate corresponding to S is $R_S = \sum_{k \in S} \log_2 p_k = \log_2 \left(\prod_{\ell \in S} p_\ell\right)$. Hence, we conclude that $R_S = \log_2 (d_S / d_0)$. ■

Using $R_S = \log_2 \left({}^{d_S}/_{d_\bullet} \right)$ in (1), we have $\Gamma \approx 6$ dB/b/dim.

A similar construction of lattice codes using tuples of prime integers in $\mathbb{Z}[i]$ and $\mathbb{Z}[\omega]$ is reported in [18] for low complexity multilevel encoding and multistage decoding in compute-and-forward applications.

V. Conclusion and Discussion

We have proposed lattice index codes for the Gaussian broadcast channel where every receiver demands all the messages from the transmitter. We have introduced the notion of side information gain as a code design metric, and constructed lattice index codes based on the Chinese remainder theorem with $\Gamma \approx 6$ dB/b/dim. In [19] we have extended our construction to complex and quaternionic lattice index codes that provide further choices in terms of message rates at the source and side information rates at the receivers.

The lattice index codes constructed here can be used as modulation schemes together with strong outer codes. Consider K information streams, encoded independently using K outer codes over the alphabets $\mathcal{W}_1, \dots, \mathcal{W}_K$, respectively. The coded information streams are multiplexed using the lattice index code $\mathscr{C}$ and transmitted. If the minimum Hamming distance of the outer codes is d_H, then the minimum squared Euclidean distance at a receiver corresponding to S is at least $d_H \times d_S^2$. While the outer code improves error resilience, the inner lattice index code collects the gains from side information.

The new lattice index codes are designed using a tuple of prime numbers. Hence, the cardinalities of the resulting message alphabets are not all equal, and not all of them are powers of 2. It will be interesting to design codes that have greater freedom of choice in message sizes.

References

[1] Z. Bar-Yossef, Y. Birk, T. S. Jayram, and T. Kol, "Index coding with side information," *IEEE Trans. Inf. Theory*, vol. 57, no. 3, pp. 1479–1494, Mar. 2011.

[2] N. Alon, E. Lubetzky, U. Stav, A. Weinstein, and A. Hassidim, "Broadcasting with side information," in *Proc. 49th IEEE Symp. Foundations of Computer Science (FOCS)*, Oct. 2008, pp. 823–832.

[3] S. El Rouayheb, A. Sprintson, and C. Georghiades, "On the index coding problem and its relation to network coding and matroid theory," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3187–3195, Jul. 2010.

[4] Y. Wu, "Broadcasting when receivers know some messages a priori," in *Proc. IEEE Int. Symp. Information Theory (ISIT)*, Jun. 2007, pp. 1141–1145.

[5] G. Kramer and S. Shamai, "Capacity for classes of broadcast channels with receiver side information," in *Proc. IEEE Information Theory Workshop (ITW)*, Sep. 2007, pp. 313–318.

[6] J. Sima and W. Chen, "Joint network and Gelfand-Pinsker coding for 3-receiver Gaussian broadcast channels with receiver message side information," in *Proc. IEEE Int. Symp. Information Theory (ISIT)*, Jun. 2014, pp. 81–85.

[7] B. Asadi, L. Ong, and S. Johnson, "The capacity of three-receiver AWGN broadcast channels with receiver message side information," in *Proc. IEEE Int. Symp. Information Theory (ISIT)*, Jun. 2014, pp. 2899–2903.

[8] E. Tuncel, "Slepian-Wolf coding over broadcast channels," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1469–1482, Apr. 2006.

[9] L. Xiao, T. Fuja, J. Kliewer, and D. Costello, "Nested codes with multiple interpretations," in *Proc. 40th Annu. Conf. Information Sciences and Systems (CISS)*, Mar. 2006, pp. 851–856.

[10] Y. Ma, Z. Lin, H. Chen, and B. Vucetic, "Multiple interpretations for multi-source multi-destination wireless relay network coded systems," in *Proc. IEEE 23rd Int. Symp. Personal Indoor and Mobile Radio Communications (PIMRC)*, Sep. 2012, pp. 2253–2258.

[11] F. Barbosa and M. Costa, "A tree construction method of nested cyclic codes," in *Proc. IEEE Information Theory Workshop (ITW)*, Oct. 2011, pp. 302–305.

[12] K. H. Rosen, *Elementary number theory and its applications*. Addison-Wesley, 2005.

[13] G. Ungerboeck, "Channel coding with multilevel/phase signals," *IEEE Trans. Inf. Theory*, vol. 28, no. 1, pp. 55–67, Jan. 1982.

[14] J. H. Conway and N. Sloane, *Sphere packings, lattices and groups*. New York: Springer-Verlag, 1999.

[15] G. Forney, "Coset codes. I. Introduction and geometrical classification," *IEEE Trans. Inf. Theory*, vol. 34, no. 5, pp. 1123–1151, Sep. 1988.

[16] R. Zamir, S. Shamai, and U. Erez, "Nested linear/lattice codes for structured multiterminal binning," *IEEE Trans. Inf. Theory*, vol. 48, no. 6, pp. 1250–1276, Jun. 2002.

[17] H. Cohn and A. Kumar, "Optimality and uniqueness of the Leech lattice among lattices," *Ann. of Math.*, vol. 170, no. 3, pp. 1003–1050, Nov. 2009.

[18] Y.-C. Huang and K. Narayanan, "Multistage compute-and-forward with multilevel lattice codes based on product constructions," in *Proc. IEEE Int. Symp. Information Theory (ISIT)*, Jun. 2014, pp. 2112–2116.

[19] L. Natarajan, Y. Hong, and E. Viterbo, "Lattice index coding," *submitted to IEEE Trans. Inf. Theory*, 2014. [Online]. Available: http://arxiv.org/abs/1410.6569