Algebraic Lattice Alignment for $K$-User Interference Channels

Amin Jafarian, Jubin Jose and Sriram Vishwanath

Abstract—This paper develops a new achievable region for the $K$-user symmetric interference channel using algebraic interference alignment. Our scheme uses lattice codebooks to transform the interference channel into an equivalent noiseless discrete-alphabet additive interference channel. Subsequently, algebraic alignment schemes are used to characterize the achievable rates for this channel.

I. INTRODUCTION

Additive Gaussian interference channels are basic components of wireless networks, and hence it is essential that we understand their limits to efficiently operate wireless systems. Even though the capacity region of the interference channel is still unknown in general, important progress has been made recently, especially in the case of two-user interference channels. It has been shown in [9] that the Han-Kobayashi achievability region is within one-bit of the capacity region irrespective of the channel gains. When the interference is sufficiently weak, the capacity region of two-user interference channel has been characterized [9], [11], [1]. Unfortunately, a majority of these results are specific to the two-user interference channel and do not extend naturally to $K$ (greater than two) user interference channels.

In the study of multi-user interference channels, a mechanism known as interference alignment has been developed [3]. Using this, the degrees of freedom (DoF) of the $K$ user time/frequency varying interference channels have been characterized and shown to equal $K/2$. More recently, constant (non-time varying channels) have also been analyzed from the DoF perspective. It has been shown in [8] that for irrational channel gains, a DoF of $K/2$ can be obtained. However, for rational channel gains, [8] shows that the DoF is strictly less than $K/2$. Although this DoF analysis provides us with valuable insight into the types of schemes needed for the interference channel, they are not always directly applicable for finite signal to noise ratio (SNR) systems.

In this paper, our goal is to develop achievable strategies for interference channels for any SNR using a lattice coding framework. The linearity of lattices facilitates alignment for the interference at each receiver. Lattices also enable us to transform the continuous input additive noise interference channel into an equivalent noise-free discrete input additive interference channel. This transformation allows us to use algebraic tools to align interference and thus determine a set of achievable rates for this channel. Note that, once reduced to a noise-free interference channel, then symbol alignment schemes (as used for DoF analysis [4]) can be used to determine achievable rates at any SNR.

Structured coding, especially lattice coding, has been studied fairly extensively in literature [2], [12], [10]. In particular, in [7], [6], it is shown to achieve the capacity of the point to point channel with or without additive state that is known non-causally to the transmitter. In the context of the interference channel, lattice codebooks are used in [2], [13], [14]. In [13],
lattice coding is capacity achieving for the class of channels where "very strong" interference condition is satisfied. Subsequently, a layered lattice coding scheme is introduced in [14] to determine a new set of achievable rates for this channel. Note that the approach in [14] and in this paper are similar in that they both use lattices to align interference in the system. The main difference is the way in which the interference and signal is differentiated. In [14], the signal and interference are separated into different "levels" (leading to level alignment). In this paper, the signal and interference are differentiated using algebraic techniques and thus is based on symbol alignment, as studied in [1] for high SNR.

The rest of this paper is organized as follows: We present the channel model in the next section, and some preliminaries about the lattices in section III. In Section IV, we address the main theorem of the paper and its proof and we conclude this work in Section V.

II. CHANNEL MODEL

The $K$ (greater than 2) user symmetric additive Gaussian noise interference channel is depicted in Figure 1. This channel consists of $K$ pairs of Transmitters and Receivers. Transmitter $i$ has a message $m_i \in M_i$ to communicate with its corresponding Receiver. Each transmitter uses a codebook $C_i$ and a mapping function $\phi_i(.)$ from its message set $M_i$ to its codebook $C_i$, i.e., $\phi_i : M_i \rightarrow C_i$. Transmitter $i$ sends the codeword $\phi_i(m_i)$ in order to communicate the message $m_i$. Each transmitter has an average power constraint $P_i$:

$$\frac{1}{|C_i|} \sum_{X_i \in C_i} \|X_i\|^2 \leq P_i,$$

where $\|\cdot\|$ is the Euclidean norm.

Note that, in this work, we assume a symmetric interference channel, i.e., all the power constraints $P_i$’s are equal to $P$, all the interferer gains are equal to an integer $a \in \mathbb{Z}$, all the direct gains are one, and all the additive noise powers are equal to $b \in \mathbb{Z}$. We make these assumptions to simplify our analysis and to avoid losing focus from the main concept introduced by this paper - that of algebraic alignment using lattices.

III. PRELIMINARIES ON LATTICES

A lattices is an additive subgroup of $\mathbb{R}^n$ isomorphic to $\mathbb{Z}^n$. One can write the lattice $\Lambda$ as the following:

$$\Lambda = \{ x \in \mathbb{R}^n : x = G z, z \in \mathbb{Z}^n \},$$

where $G \in \mathbb{R}^{n \times n}$ is a full rank $n$ by $n$ matrix. Voronoi region of the lattice $\Lambda$ is defined as all the points in $\mathbb{R}^n$ which are closer to a particular lattice point than any other lattice points. Because of the symmetry of lattices, we can define the Voronoi region around zero (which is always a lattice point) as the following:

$$V = \{ x \in \mathbb{R}^n : \|x\| \leq \|x-\lambda\| \quad \text{for all} \quad \lambda \in \Lambda \}.$$  

The second moment per dimension of a lattice is defined as:

$$\sigma^2(V) = \frac{\int_V \|x\|^2dx}{nVol(V)}.$$
Let $\mathcal{G}(\Lambda)$ denote the normalized second moment of the lattice $\Lambda$, defined as:

$$\mathcal{G}(\Lambda) = \frac{\sigma^2(\mathcal{V})}{\text{Vol}(\mathcal{V})^2}.$$  

It is known that $\mathcal{G}(\Lambda) \geq \frac{1}{2\pi e}$ for all the lattices. A lattice is called “good for quantization” if $\mathcal{G}(\Lambda) \approx \frac{1}{2\pi e}$ for large $n$.

$\Lambda$ is called “good for channel coding” if probability of error in decoding a Gaussian noise $Z$ with unit variance from the signal $Y = \lambda + Z$ where $\lambda \in \Lambda$ using lattice decoding goes to zero as $n \to \infty$.

We call lattices $\Lambda_c$ and $\Lambda_f$ nested lattice if $\Lambda_c \subset \Lambda_f$, where subscripts $c$ and $f$ stand “coarse” and “fine”. This represents the fact that in general $\Lambda_f$ has more number of points in a fixed region than $\Lambda_c$.

The nesting ratio of nested lattices $\Lambda_c \subset \Lambda_f$ is defined as:

$$\rho(\Lambda_c, \Lambda_f) \triangleq \left( \frac{\text{Vol}(\mathcal{V}_c)}{\text{Vol}(\mathcal{V}_f)} \right)^{\frac{1}{2}}.$$  

Note that if both the lattices $\Lambda_c$ and $\Lambda_f$ are “good for quantization”, the nesting ratio can be expressed as:

$$\rho(\Lambda_c, \Lambda_f) = \frac{\sigma^2(\mathcal{V}_c)}{\sigma^2(\mathcal{V}_f)}.$$  

IV. MAIN RESULTS

In this work, we show a lattice achievable scheme that can achieve certain rates in a symmetric $K$-user interference channel under strong interference, specifically, when $b = 1$ and $a \geq K - 1$.

**Theorem 1.** For a symmetric $K$-user Gaussian interference channel (as shown in Figure 1, with $b = 1$ and interference channel gain $a \in \mathbb{Z}$ such that $a \geq K - 1$), each user can achieve the following rate:

$$R = \frac{1}{4} (1 - \log_a(K - 1)) \log(P).$$

We use nested lattices as first proposed in [7] to construct the codebook $\mathcal{C}$ at each transmitter. Let $\Lambda_c \subset \Lambda_f$ constructed as the following:

$$\Lambda_f = G_1 \left( \frac{1}{p} G_2 \cdot \mathbb{Z}_p + \mathbb{Z}^n \right),$$  

(1)

$$\Lambda_c = G_1 \mathbb{Z}^n,$$  

(2)

where $n$ is a big positive integer, $G_1$ is an $n \times n$ real matrix, $G_2$ is an $n$-dimensional vector from $\mathbb{Z}_p^n$, the operation “$\cdot$” indicates the modulo $p$ multiplication, and $p$ is a prime integer satisfying the following:

$$a^{2l} < p < 2a^{2l}. \tag{3}$$

In the above equation, $a$ is the interference channel gain and $l$ is a positive integer. Let $\mathcal{C}_0 = \Lambda_f \cap \mathcal{V}_c$. The following lemma helps ensure the existence of an appropriate matrix $G_1$ and a vector $G_2$.

**Lemma 1.** Assuming that $p^{\frac{2}{n}} \leq P$, there exist a matrix $G_1$ and a vector $G_2$ such that the followings are satisfied:

1) $\sigma^2(\mathcal{V}_c) = P$,
2) $\Lambda_f$ is “good for channel coding”, and
3) Lattices $\Lambda_c$ and $\Lambda_f$ are “good for quantization”.

**Proof of Lemma 1.** Follows directly from [7] and [5]. \hfill \Box

First, we choose

$$p \approx P^\frac{2}{l}. \tag{4}$$

From the Inequality (3) and Equation (4), we obtain:

$$a^{2l} < P^\frac{2}{l} < 2a^{2l} \Rightarrow$$

$$2l \log(a) < \frac{n}{2} \log(P) < 1 + 2l \log(a) \Rightarrow$$

$$\frac{2l}{n} \log(a) < \frac{1}{2} \log(P) < \frac{1}{n} + \frac{2l}{n} \log(a). \tag{6}$$

By choosing $n$ and $l$ large enough such that Equation (5) is still satisfied, and by employing
Equation (6), we get the following for sufficiently large $n$:

$$
\frac{2l}{n} \log(a) \approx \frac{1}{2} \log(P).
$$

(7)

Without loss of generality, let $g_1 \neq 0$ be the first index of the matrix $G_2$. We define sets

$$
A = \left\{ s : s = \sum_{i=0}^{t-1} t_i a^{2i}, 0 \leq t_i \leq \left\lfloor \frac{a-1}{K-1} \right\rfloor \right\},
$$

(8)

$$
B = \left\{ w : w = [g_1^{-1} \cdot s] \mod p, \ s \in A \right\}.
$$

(9)

Following lemma states some important properties regarding the cardinality of these two sets.

**Lemma 2.** Let $s_i \in A$ for $i \in \{1, 2, ..., K\}$ be any $K$ elements of $A$ and $q = s_1 + a \sum_{i=2}^{K} s_i$ ($K$ is the number of users). Then we have the following:

1) There exists a one-to-one map from $q$ to $s_1$.

2) $q < a^{2l} < p$, and

3) $|B| = |A| \geq \left( \frac{a}{K-1} \right)^l$.

**Proof of Lemma 2.** We prove each part of the lemma separately.

1) From the definition of $A$, one can rewrite each element $s_i \in A$ in base $a$ as the following:

$$
s_i = [0 \ t_{l-1,i} 0 \ t_{l-2,i} 0 ... \ t_{1,i} 0 \ t_{0,i}]_a,$$

where each $0 \leq t_{j,i} \leq \left\lfloor \frac{a-1}{K-1} \right\rfloor$. Let $g_j = \sum_{i=2}^{K} t_{j,i}$ for $j \in \{0, 1, ..., l-1\}$. One can check that $g_j \leq a - 1$ and therefore $q$ can be written in base $a$ as the following:

$$
q = [g_{l-1} \ t_{l-1,1} \ g_{l-2} \ t_{l-2,1} ... \ g_1 \ t_{1,1} \ g_0 \ t_{0,1}]_a.
$$

(11)

So, $s_1$ can be decoded from $q$ by focusing on the odd-positioned entries of $q$ when written in base $a$.

2) From Equation (11), one can easily see that $q < a^{2l} < p$.

3) The cardinality of the set $A$ can be easily computed as:

$$
|A| = \left( \left\lfloor \frac{a-1}{K-1} \right\rfloor + 1 \right)^l \geq \left( \frac{a}{K-1} \right)^l.
$$

The same cardinality result for the set $B$ follows if we can demonstrate a one to one mapping from $|A|$ to $|B|$. One can check that from $[g \cdot a] \mod p = [g \cdot b] \mod p$, it can be shown that $a = b$ if both $a$ and $b$ are less than $p$, which is the case here. Note that $s_i < a^{2l} < p$ for all $i$’s. So, the mapping $a \rightarrow [g \cdot a] \mod p$ induces a one-to-one mapping from $|A|$ to $|B|$, and as a result $|B| = |A|$.

□

Note that $\Lambda \subset \mathbb{Z}_p$. We define $L_h$, a subset of $\Lambda_f$, as the following:

$$
L_h = G_1 \left( \frac{1}{p} G_2 \cdot B + \mathbb{Z}_p^n \right).
$$

(10)

**Proof of Theorem 1.** We define the codebook $\mathcal{C} = \Lambda_h \cap \mathcal{V}_c$. Note that $\mathcal{C} \subset \mathcal{C}_0$. Next, we discuss the encoding/decoding scheme.

**Encoding Scheme:**
Each transmitter picks a random function from its message set to the codebook $\mathcal{C}$. To transmit message $m_i$, transmitter $i$ sends the corresponding codeword $X_i \in \mathcal{C}$.

**Decoding Scheme:**
Receiver $i$ observes signal

$$
Y_i = X_i + a \sum_{j=1,j \neq i}^{K} X_j + N_i,
$$

where $N_i$ is a Gaussian noise with unit power. Since $X_i \in \mathcal{C}$, we can also assume for each $X_i$ there exists $w_i \in B$ and $z_i \in \mathbb{Z}_p^n$ that satisfy the following:

$$
\exists w_i, z_i : X_i = G_1 \left( \frac{1}{p} G_2 \cdot w_i + z_i \right).
$$

(11)

Let $s_i = g_1 \cdot w_i$. Note that $s_i \in A$ as $w_i \in B$ and the mapping from $B$ to $A$ is one to one as
discussed earlier. To decode the message \( m_i \), receiver will take the following steps.

1) **Remove the noise:** Since \( a \in \mathbb{Z} \),

\[
\hat{Y}_i = X_i + a \sum_{j=1, j \neq i}^{K} X_j \text{ is an element of the lattice } \Lambda_f. \text{ If the lattices are such that the conditions of the Lemma 1 are satisfied, eliminate the noise } N \text{ and obtain } \hat{Y}_i \text{ from } Y_i.
\]

2) **Compute** \( q_i = s_i + a \sum_{j=1, j \neq i}^{K} s_j \).

For the computation in step 2, we use the following lemma.

**Lemma 3.** \( q_i \) can be obtained as the following:

\[
q_i = [(pG_2^{-1}\hat{Y}_i)_1 \mod p, \quad (12)
\]

where \((V)_1\) indicates the first entry of the vector \( V \).

**Proof of Lemma 3.** Using Equation (11), we simplify the right hand side of the lemma statement as the following:

\[
[(pG_2^{-1}\hat{Y}_i)_1 \mod p
\]

\[
= [(G_2(w_i + a \sum_{j=1, j \neq i}^{K} w_j
\]

\[
+ p \sum_{j=1}^{K} z_j)_1 \mod p
\]

\[
= [g_1(w_i + a \sum_{j=1, j \neq i}^{K} w_j)_1 \mod p
\]

\[
= [s_i + a \sum_{j=1, j \neq i}^{K} s_j \mod p \quad (12)
\]

\[
= s_i + a \sum_{j=1, j \neq i}^{K} s_j = q_i,
\]

where Equation (12) follows from the second statement of Lemma 2. \( \square \)

3) **Decode** \( X_i \): Once we have \( q_i \), one can use the first part of Lemma 2 to decode \( s \). \( X_i \) can be computed from \( s_i \) as:

\[
X_i = \left[ \frac{1}{p} G_1 G_2 \cdot (g_1^{-1} s_i) \right] \mod \Lambda_c.
\]

To complete the proof, we need to show that the codebook \( \mathcal{C} \) has enough number of codewords. Let \( |\mathcal{C}| = 2^{nR} \). From Equation (7) and the third statement of Lemma 2, \( R \) can be computed as the following:

\[
R = \frac{1}{n} \log(|\mathcal{C}|) \geq \frac{l}{n} \log \left( \frac{a}{K-1} \right)
\]

\[
= \frac{1}{4} \log(p) \frac{\log \left( \frac{a}{K-1} \right)}{\log(a)}
\]

\[
= \frac{1}{4} \left( 1 - \log_a(K-1) \right) \log(p). \quad (13)
\]

\( \square \)

V. CONCLUSION

In this work, a lattice coding based alignment scheme is proposed for the \( K \)-user Gaussian interference channel. Using this scheme one can use algebraic (symbol level) alignment to generate an achievable set of rates at any SNR.

**ACKNOWLEDGMENT**

We are grateful to Uri Erez for his helpful comments.

**REFERENCES**


