Layered Space-Time Index Coding

§Yu-Chih Huang, †Yi Hong, †Emanuele Viterbo, and ‡Lakshmi Natarajan
§Department of Communication Engineering, National Taipei University
†Department of Electrical and Computer Systems Engineering, Monash University
‡Department of Electrical Engineering, Indian Institute of Technology Hyderabad

***Abstract*—Multicasting K independent messages via multiple-input multiple-output (MIMO) channels to multiple users where each user already has a subset of messages as side information is studied. A general framework of constructing *layered space-time index coding* (LSTIC) from a large class of space-time block codes (STBCs), including perfect STBCs, is proposed. We analyze the proposed LSTIC technique and show that it provides minimum determinant gains that are exponential in the amount of information contained in the side information for *any possible side information* at the receivers. When constructed over a perfect STBC, the proposed LSTIC is itself a perfect STBC and hence enjoys many desired properties.**

***Index Terms*—Index coding, broadcast channels, side information, space-time block codes, MIMO channel.**

I. Introduction

The index coding problem [1], [2] studies the problem of optimally broadcasting independent messages via noiseless links to multiple receivers where each receiver demands a subset of messages and already has another subset of messages as side information. The side information at a receiver is described by an index set and could be obtained from various means depending on the application. For example, in retransmissions in broadcast channel [1], the side information is decoded from the previous received signals; in the coded caching technique [3], the side information is prefetched into users' local cache memories during off-peak hours; and in wireless relay networks [4], [5], the side information is the users' own data and/or is decoded/overheard from the previous sessions.

At the physical layer, the index coding problem can in fact be modeled as the noisy broadcast channel with receiver side information. This problem has recently been investigated from two different perspectives and most of the prior works can be categorized accordingly into two groups. The first one focuses on characterizing the capacity region of the AWGN broadcast channel with message side information [6]. However, since the number of possible index sets increases exponentially with the number of users in the network, the problem quickly becomes intractable as the number of users increases.

The second category considers designing codes that possess some desired properties in the finite dimension regime. The main objective is to design codes such that the probability of error will decrease by an amount that is proportional to the amount of information contained in the side information. A series of work within this category ([7]–[9]), which seamlessly scales to any number of users, considers the scenario where the transmitter is oblivious of the index sets. This enables to handle large numbers of users, when the index sets to feedback to the transmitter require excessive resources and/or the complexity of designing the specific index code becomes excessive. The objective then becomes designing coding schemes that are fair to every possible index set. As a starting point, only the multicasting case is considered in [7]–[9] where all the receivers demand all the messages.

In [7], Natarajan *et al.* study code design for the AWGN broadcast channel where minimum distance is one of the most crucial parameters to be maximized. Exploiting the algebraic structure induced by the Chinese remainder theorem (CRT), a novel coding scheme, lattice index coding, is proposed in [7] to accommodate *any number of messages* with message sizes relatively prime to each other. The lattice index coding is shown to provide gains in minimum distance exponential with the rate of the side information, for any index set.

In [8], Huang considers the same multicasting problem with message side information, where each link experiences a Rayleigh fading channel on top of the AWGN noise. The lattice index coding scheme proposed in [8] generalizes the idea of [7] to design codes over any ring of algebraic integers. It is shown that codes thus constructed over rings of algebraic integers of totally real number fields provide gains in minimum product distance that is exponential with the rate of the side information for any index set. The multicasting problem with message side information is then considered in [9] under the 2×2 MIMO setting where the transmitter and the receivers are equipped with two antennas. Since CRT does not hold for non-commutative rings such as cyclic division algebras where most known space-time codes are constructed over, the technique used in [7] and [8] does not work here in general. In [9], we successfully constructed Golden-coded index coding from Golden code, a subclass of perfect codes for the 2×2 MIMO channel, by exploiting the bijective mapping between the Golden algebra and a commutative ring.

In this work, we consider the problem of multicasting over MIMO channel with message side information for arbitrary number of transmit antennas. We propose *layered space-time index coding* (LSTIC), a general framework of constructing lattice space-time index codes from algebraic space-time block

The work of Y.-C. Huang is supported by the Ministry of Science and Technology, Taiwan, under grant MOST 106-2628-E-305-001-MY3. The work of Yi Hong and Emanuele Viterbo is supported by the Australian Research Council (ARC) through the Discovery Project under grant DP160101077. The work of Lakshmi Natarajan is supported by the Department of Science and Technology through INSPIRE research grant DST/INSPIRE/04/2015/002094.

978-1-5386-4780-6/18/$31.00©2018 IEEE

codes (STBCs) based on cyclic division algebras [10]–[12]. We exploit the algebraic structure of these codes to encode the different messages into subcodes, which preserve all the good properties of the STBC, such as non-vanishing determinant and power efficiency.

Any receiver that has some of the messages as side information will be decoding a subcode that has an improved performance in terms of error probability. We provide a lower bound on the *side information gain* for any side information configuration. The side information gain essentially measures that for achieving a given probability of error in the low probability of error regime, how much SNR reduction (normalized by the rate of the side information) is achieved by revealing the side information. This lower bound implies an exponential increase of minimum determinant and is universal in the sense that it holds for *any possible side information index set*.

Throughout the paper, the following notations are used. Matrices are written in capital boldface, for example $\mathbf{X}$. Let $\theta \triangleq \frac{1+\sqrt{5}}{2}$, $\bar{\theta} \triangleq \frac{1-\sqrt{5}}{2}$, $\mathrm{i} \triangleq \sqrt{-1}$, and $\omega \triangleq e^{\mathrm{i}2\pi/3}$ be the primitive cube root of unity. We denote by $\mathbb{Z}$, $\mathbb{Z}[\mathrm{i}] \triangleq \{a+b\mathrm{i} | a,b \in \mathbb{Z}\}$, and $\mathbb{Z}[\omega] \triangleq \{a+b\omega | a,b \in \mathbb{Z}\}$ the ring of integers, the ring of Gaussian integers, and the ring of Eisenstein integers, respectively. Also, we denote by $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ the field of rational numbers, the field of real numbers, and the field of complex numbers, respectively.

II. Problem Statement

Consider the network shown in Fig. 1 where there is a base station broadcasting messages to L users. The base station is equipped with n_t antennas and each user is equipped with n_r antennas. There are K independent messages $\{w_1, \ldots, w_K\}$ collocated at the base station and each w_k is uniformly distributed over $\{1, \ldots, M_k\}$. Each user demands all the K messages and already has a subset of the messages as side information. For user ℓ, we denote by $\mathcal{S}_\ell \subseteq \{1, \ldots, K\}$ the index set and the side information at the user is $w_{\mathcal{S}_\ell} \triangleq \{w_s | s \in \mathcal{S}_\ell\}$. The base station encodes the messages across space (n_t antennas) and time (T symbol durations) into an $n_t \times T$ codeword matrix $\mathbf{X}$ where each entry $x_{jt} \in \mathbb{C}$ and the codeword is subject to the power constraint $\mathbb{E}[\|\mathbf{X}\|^2] = n_t T$. In an algebraic space-time code, each codeword $\mathbf{X}$ is used to transmit r information-bearing real symbols. i.e., r is the dimension of the space-time code when viewed as a lattice code. We denote by $R_k = \log_2(M_k)/r$ the rate of the message w_k measured in bits per real symbol. The signal model between the base station and the user ℓ is given by

$$\mathbf{Y}_\ell = \mathbf{H}_\ell \mathbf{X} + \mathbf{Z}_\ell,$$

where $\mathbf{Y}_\ell$ is of size $n_r \times T$, $\mathbf{H}_\ell$ is a random $n_r \times n_t$ matrix with each element i.i.d. $\sim \mathcal{CN}(0,1)$, and $\mathbf{Z}_\ell$ is a random $n_r \times T$ matrix with each element i.i.d. $\sim \mathcal{CN}(0, \sigma_l^2)$. Each user is assumed to know the channel matrix $\mathbf{H}_\ell$ associated with its received signal, i.e., channel state information at the receiver is assumed. The signal-to-noise power ratio (SNR) is defined as $\mathrm{SNR}_\ell \triangleq \frac{n_t}{\sigma_\ell^2}$.

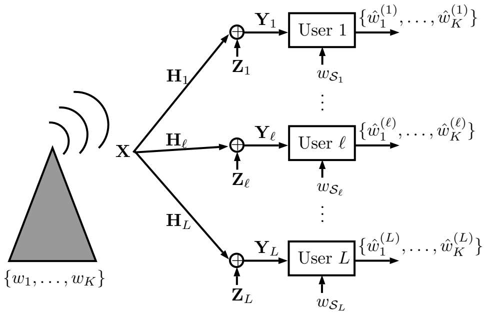

Fig. 1. Multicasting $\{w_1, \ldots, w_K\}$ over MIMO channel to L receivers where each receiver $\ell \in \{1, \ldots, L\}$ has a subset of messages $w_{\mathcal{S}_\ell}$ as side information.

Let ϕ be a bijective encoding function that maps the messages $(w_1, \ldots, w_K)$ to the transmitted signal $\mathbf{X}$. The codebook $\mathcal{C}$ is the collection of codewords given by

$$\mathcal{C} = \{\mathbf{X} = \phi(w_1, \ldots, w_K) | w_k \in \{1, \ldots, M_k\}, \forall k\}.$$

Based on the received signal $\mathbf{Y}_\ell$ and side information $w_{\mathcal{S}_\ell}$, the user ℓ forms $\{\hat{w}_1^{(\ell)}, \ldots, \hat{w}_K^{(\ell)}\}$ (or equivalently $\hat{\mathbf{X}}^{(\ell)}$) an estimate of $\{w_1, \ldots, w_K\}$ (or equivalently $\mathbf{X}$). The probability of error is defined as

$$p_e^{(\ell)} \triangleq \Pr\{(w_1, \ldots, w_K) \neq (\hat{w}_1^{(\ell)}, \ldots, \hat{w}_K^{(\ell)})\} = \Pr\{\mathbf{X} \neq \hat{\mathbf{X}}^{(\ell)}\},$$

where the second expression is often called the codeword error rate (CER). We emphasize here that the index set $\mathcal{S}_\ell$ can be any subset of $\{1, \ldots, K\}$ and is oblivious to the base station. We therefore focus on a generic user and drop the subscript (superscript in some cases) ℓ.

We note that with the knowledge of side information $w_s = v_s, \forall s \in \mathcal{S}$, the generic user can expurgate all the codewords that do not correspond to this side information. The codebook then becomes

$$\mathcal{C}_\mathcal{S} \triangleq \left\{ \mathbf{X} = \phi(d_1, \ldots, d_K) \,\middle|\, \begin{array}{ll} d_k = v_k, & k \in \mathcal{S}; \\ d_k \in \{1, \ldots, M_k\}, & k \notin \mathcal{S}. \end{array} \right\},$$

a subcode of $\mathcal{C}$. To measure how much SNR one can save for achieving a target p_e by knowing $w_\mathcal{S}$, the authors in [9] derived the SNR gain as follows,

$$\frac{1}{n_t n_r} 10 \log_{10} \left(\frac{N_\mathcal{C}}{N_{\mathcal{C}_\mathcal{S}}} \right) + \frac{1}{n_t} 10 \log_{10} \left(\frac{\delta(\mathcal{C}_\mathcal{S})}{\delta(\mathcal{C})} \right), \quad (1)$$

where $\delta(\mathcal{C})$ is the minimum determinant of $\mathcal{C}$ and $N_\mathcal{C}$ is the averaged number of nearest neighbors in terms of minimum determinant. Moreover, as mentioned in [9] and many other work in the space-time code literature, it is in general not an easy task to keep tracking both $N_{\mathcal{C}_\mathcal{S}}$ and $\delta(\mathcal{C}_\mathcal{S})$ for lattice codes; we thereby focus solely on $\delta(\mathcal{C}_\mathcal{S})$ as our design guideline and define the side information gain as $10 \log_{10} (\delta(\mathcal{C}_\mathcal{S})/\delta(\mathcal{C}))^{1/n_t}$ dB. To get a fair comparison for every possible side information, we then normalize this side information gain by the rate of the side information and define the normalized side information gain as

$$\Gamma(\mathcal{C}, \mathcal{S}) \triangleq \frac{10 \log_{10} \left(\frac{\delta(\mathcal{C}_\mathcal{S})}{\delta(\mathcal{C})} \right)}{n_t R_\mathcal{S}}, \quad (2)$$

where the rate of the side information is defined as $R_{\mathcal{S}} \triangleq \sum_{s\in\mathcal{S}} R_s$ and is measured in bits per real symbol, which makes the normalized side information gain having the unit "dB/bits per real symbol". The side information gain essentially serves as an approximation of the SNR gain provided by side information $w_{\mathcal{S}}$, normalized by the rate of $w_{\mathcal{S}}$. We note that involving the first term of (1) into the definition of side information gain results in a better approximation. Hence, although we use (2) as the design guideline throughout the paper, (1) is also used to confirm the simulation results.

III. Background

In this section, we provide minimum background knowledge on cyclic division algebra and its connection to lattice STBC. For details, please refer, for example, to [12].

Let $\mathbb{L}/\mathbb{K}$ be a field extension of $\mathbb{K} = \mathbb{Q}(\mathrm{i})$ or $\mathbb{Q}(\omega)$ of degree n whose Galois group is a cyclic group generated by σ. One can construct $\mathcal{A} = (\mathbb{L}/\mathbb{K}, \sigma, \gamma)$ a *cyclic algebra*

$$\mathcal{A} = \left\{x_0 + x_1\mathsf{e} + \ldots + x_{n-1}\mathsf{e}^{n-1} | x_0, \ldots, x_{n-1} \in \mathbb{L}\right\},$$

where $\mathsf{e}^n = \gamma \in \mathbb{K}$ and $\lambda\mathsf{e} = \mathsf{e}\sigma(\lambda)$ for $\lambda \in \mathbb{L}$. $\mathcal{A}$ is said to be a division algebra if every non-zero element of $\mathcal{A}$ is invertible. A *cyclic division algebra* is a cyclic algebra that is at the same time a division algebra. In the space-time coding literature [12], a cyclic division algebra is usually constructed from a cyclic algebra $\mathcal{A} = (\mathbb{L}/\mathbb{K}, \sigma, \gamma)$ with carefully chosen γ such that none of $\gamma, \gamma^2, \ldots, \gamma^{n-1}$ are norms of some element of $\mathbb{L}$.

Consider $n_t = n_r = T = n$, an $n \times n$ STBC carved from $\mathcal{A}$ corresponds to a finite subset of

$$\bar{\mathcal{A}}_{\mathfrak{I}} = \left\{x_0 + x_1\mathsf{e} + \ldots + x_{n-1}\mathsf{e}^{n-1} | x_0, \ldots, x_{n-1} \in \mathfrak{I}\right\}, \quad (3)$$

where $\mathfrak{I}$ is an ideal in $\mathfrak{O}_{\mathbb{L}}$ the ring of integers of $\mathbb{L}$. More specifically, an $n\times n$ STBC thus constructed is obtained from the following matrix representation of $\bar{\mathcal{A}}_{\mathfrak{I}}$

$$\mathcal{C}_{\mathfrak{I}} = \quad (4)$$
$$\left\{ \left. \begin{pmatrix} x_0 & x_1 & \ldots & x_{n-1} \\ \gamma\sigma(x_{n-1}) & \sigma(x_0) & & \sigma(x_{n-2}) \\ \vdots & & \ddots & \vdots \\ \gamma\sigma^{n-1}(x_1) & \gamma\sigma^{n-1}(x_2) & \ldots & \sigma^{n-1}(x_0) \end{pmatrix} \right| x_\ell \in \mathfrak{I} \right\}.$$

A layer $\ell \in \{0, \ldots, n-1\}$ of a codeword in $\mathcal{C}_{\mathfrak{I}}$ consists of all the entries of the codeword matrix that are functions of the same $x_\ell \in \mathfrak{I}$. Here, we use the subscript $\mathfrak{I}$ in $\bar{\mathcal{A}}_{\mathfrak{I}}$ and $\mathcal{C}_{\mathfrak{I}}$ to emphasize that the elements x_ℓ for all ℓ are restricted to the ideal $\mathfrak{I}$. For transmission with finite input power constraint, one carves a subset from (a possibly shifted and scaled version of) $\mathcal{C}_{\mathfrak{I}}$ to form the codebook. In [11], it is shown that within this class of codes, there are codes that are particularly good, called *perfect codes* defined as follows.

Definition 1. A $n \times n$ STBC is called a perfect STBC if *i)* it is full-rate; *ii)* it is fully diverse and has non-vanishing determinant (NVD) property; *iii)* the energy used to send the coded symbols on each layer is equal to that for sending the uncoded symbols themselves; and *iv)* all the coded symbols have the same average energy.

IV. Proposed Layered Space-Time Index Coding

In this section, we propose the LSTIC scheme and show that for any side information index set, it can provide an SNR gain that is proportional to the information contained in the side information. In the proposed scheme, instead of directly tackling $\bar{\mathcal{A}}_{\mathfrak{O}_{\mathbb{L}}}$ as done in [9], we recognize the layered structure of STBCs based on cyclic division algebras and perform encoding layer by layer. More specifically, we split each message w_k, $k \in \{1, \ldots, K\}$, into n sub-messages, namely $w_{k,\ell}$ for $\ell \in \{0, \ldots, n-1\}$, and encode $w_{1,\ell}, \ldots, w_{K,\ell}$ into x_ℓ in the layer ℓ.

In what follows, we split the discussion into two parts depending on whether $\mathfrak{I}$ is principal or not.

A. LSTIC with principal $\mathfrak{I}$

Without loss of generality, we assume that $\mathfrak{I}$ is generated by some $\alpha \in \mathfrak{O}_{\mathbb{L}}$, i.e., $\mathfrak{I} = \alpha\mathfrak{O}_{\mathbb{L}}$. Then, (3) becomes

$$\begin{aligned} \bar{\mathcal{A}}_{\mathfrak{I}} &= \left\{x_0 + x_1\mathsf{e} + \ldots + x_{n-1}\mathsf{e}^{n-1} | x_0, x_1, \ldots, x_{n-1} \in \alpha\mathfrak{O}_{\mathbb{L}}\right\}, \\ &= \left\{\alpha x_0 + \alpha x_1\mathsf{e} + \ldots + \alpha x_{n-1}\mathsf{e}^{n-1} | x_0, x_1, \ldots, x_{n-1} \in \mathfrak{O}_{\mathbb{L}}\right\}, \end{aligned}$$

and each codeword matrix in (4) becomes

$$D(\alpha) \cdot \begin{pmatrix} x_0 & x_1 & \ldots & x_{n-1} \\ \gamma\sigma(x_{n-1}) & \sigma(x_0) & & \sigma(x_{n-2}) \\ \vdots & & \ddots & \vdots \\ \gamma\sigma^{n-1}(x_1) & \gamma\sigma^{n-1}(x_2) & \ldots & \sigma^{n-1}(x_0) \end{pmatrix}, \quad (5)$$

where $D(\alpha) \triangleq \begin{pmatrix} \alpha & 0 & \ldots & 0 \\ 0 & \sigma(\alpha) & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & \sigma^{n-1}(\alpha) \end{pmatrix}$.

We can now use the technique in [8] to partition $\mathfrak{O}_{\mathbb{L}}$. Let $\mathfrak{q}_1, \ldots, \mathfrak{q}_K$ be K ideals in $\mathfrak{O}_{\mathbb{L}}$ that are relatively prime and have the (ideal) norm $N(\mathfrak{q}_k) = q_k$, $k \in \{1, \ldots, K\}$. Note that $\mathfrak{q}_k$s are not necessarily prime ideals and q_ks are not necessarily prime. We have $\mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_K = \mathfrak{q}_1 \cdot \ldots \cdot \mathfrak{q}_K \triangleq \mathfrak{q}$. From CRT, we have

$$\mathfrak{O}_{\mathbb{L}}/\mathfrak{q} \cong \mathfrak{O}_{\mathbb{L}}/\mathfrak{q}_1 \times \ldots \times \mathfrak{O}_{\mathbb{L}}/\mathfrak{q}_K \cong \mathbb{B}_{q_1} \times \ldots \times \mathbb{B}_{q_K},$$

where $\mathbb{B}_{q_k} = \mathfrak{O}_{\mathbb{L}}/\mathfrak{q}_k$ is a commutative ring[1] with size q_k. Let $\mathcal{M}$ be a ring isomorphism that maps $\mathbb{B}_{q_1} \times \ldots \times \mathbb{B}_{q_K}$ to a complete set of coset leaders of $\mathfrak{O}_{\mathbb{L}}/\mathfrak{q}$ having minimum energy.

Now, for $k \in \{1, \ldots, K\}$, let $w_k \in \mathbb{B}_{q_k}^n$ which can be represented as $w_k = (w_{k,0}, \ldots, w_{k,n-1})$ where each $w_{k,\ell} \in \mathbb{B}_{q_k}$. The encoder collects $w_{1,\ell}, \ldots, w_{K,\ell}$ to form the signal of the layer $\ell \in \{0, \ldots, n-1\}$ as

$$x_\ell = \mathcal{M}(w_{1,\ell}, \ldots, w_{K,\ell}) \in \mathfrak{O}_{\mathbb{L}}/\mathfrak{q}, \quad \ell \in \{0, \ldots, n-1\}.$$

[1] Depending on the ideal $\mathfrak{q}_k$, this ring could be a finite field, a product of finite fields, a product of finite rings and finite fields, or others. Throughout the paper, we do not use the ring property of the messages and therefore, we do not emphasize which type of ring it is.

The overall codebook is the matrix representation of

$$\bar{\mathcal{A}} = \left\{ \alpha x_0 + \ldots + \alpha x_{n-1} \mathsf{e}^{n-1} | x_0, \ldots, x_{n-1} \in \mathfrak{O}_{\mathbb{L}}/\mathfrak{q} \right\},$$

a subset of $\bar{\mathcal{A}}_{\mathfrak{I}}$, and has the matrix form as that in (5) with $x_0, \ldots, x_{n-1} \in \mathfrak{O}_{\mathbb{L}}/\mathfrak{q}$.

Note that for α and $\mathfrak{O}_{\mathbb{L}}$ such that perfect STBCs exist, the overall code $\bar{\mathcal{A}}$ is itself a perfect STBC since the perfect STBCs in [11] and $\bar{\mathcal{A}}$ share the same form but with $x_0, \ldots, x_{n-1}$ restricted to $\mathfrak{O}_{\mathbb{L}}$, a superset of $\mathfrak{O}_{\mathbb{L}}/\mathfrak{q}$ in $\bar{\mathcal{A}}$.

Theorem 2. For any $\mathcal{S} \subset \{1, \ldots, K\}$, the proposed LSTIC with principal $\mathfrak{I}$ provides a side information gain at least 6 dB/bits per real symbol, i.e., $\Gamma(\mathcal{C}, \mathcal{S}) \geq 6$ dB/bits per real symbol. Moreover, if all $\mathfrak{q}_k$, $k \in \{1, \ldots, K\}$, are principal, then $\Gamma(\mathcal{C}, \mathcal{S}) = 6$ dB/bits per real symbol.

Proof. We first note that the rate of the message w_k is

$$R_k = \frac{1}{2n^2} \log_2(q_k^n) = \frac{1}{2n} \log_2(q_k), \text{ bits/real symbol.} \quad (6)$$

Consider a generic receiver with index set $\mathcal{S}$, let the messages be $w_s = v_s$ for $s \in \mathcal{S}$. This means that $w_{s,\ell} = v_{s,\ell}$ for all $\ell \in \{0, \ldots, n-1\}$ are known at the receiver. Using the fact that $\mathcal{M}$ is an isomorphism, we can show that $x_\ell^{\mathcal{S}} = \xi_\ell^{\mathcal{S}} + \tilde{x}_\ell^{\mathcal{S}}$, where $\tilde{x}_\ell^{\mathcal{S}} = \mathcal{M}(u_{1,,\ell}, \ldots, u_{K,\ell}) + \zeta_\ell^{\mathcal{S}}$, $\zeta_\ell^{\mathcal{S}} \in \mathfrak{q}$, and $\xi_\ell^{\mathcal{S}} \triangleq \mathcal{M}(d_{1,\ell}, \ldots, d_{K,\ell})$ with

$$d_{k,\ell} = \begin{cases} v_{k,\ell}, & k \in \mathcal{S}; \\ 0, & k \in \mathcal{S}^c, \end{cases} \quad \text{and} \quad u_{k,\ell} = \begin{cases} 0, & k \in \mathcal{S}; \\ w_{k,\ell}, & k \in \mathcal{S}^c. \end{cases}$$

Note that $u_{k,\ell}$ corresponds to the unknown message and $\xi_\ell^{\mathcal{S}}$ is known at the receiver. We now have

$$\left(x_\ell^{\mathcal{S}} - \xi_\ell^{\mathcal{S}} \right) \mod \mathfrak{q}_s = 0, \quad \text{for all } s \in \mathcal{S},$$

which shows that $x_\ell^{\mathcal{S}}$ belongs to a shifted version of $\cap_{s \in \mathcal{S}} \mathfrak{q}_s = \Pi_{s \in \mathcal{S}} \mathfrak{q}_s$. Therefore, after revealing $w_{\mathcal{S}}$, the code $\mathcal{C}_{\mathcal{S}}$ corresponds to $\alpha(\xi_0^{\mathcal{S}} + \ldots + \xi_{n-1}^{\mathcal{S}} \mathsf{e}^{n-1}) + \alpha(\tilde{x}_0^{\mathcal{S}} + \ldots + \tilde{x}_{n-1}^{\mathcal{S}} \mathsf{e}^{n-1})$ where $\tilde{x}_0^{\mathcal{S}}, \ldots, \tilde{x}_{n-1}^{\mathcal{S}} \in \Pi_{s \in \mathcal{S}} \mathfrak{q}_s$. Hence, thanks to σ being a homomorphism, each codeword $\mathbf{X} \in \mathcal{C}_{\mathcal{S}}$ has the matrix form given by $\mathbf{X} = \mathbf{V}^{\mathcal{S}} + \tilde{\mathbf{X}}^{\mathcal{S}}$, where

$$\mathbf{V}^{\mathcal{S}} = D(\alpha) \cdot \begin{pmatrix} \xi_0^{\mathcal{S}} & \xi_1^{\mathcal{S}} & \cdots & \xi_{n-1}^{\mathcal{S}} \\ \gamma\sigma(\xi_{n-1}^{\mathcal{S}}) & \sigma(\xi_0^{\mathcal{S}}) & & \sigma(\xi_{n-2}^{\mathcal{S}}) \\ \vdots & & \ddots & \vdots \\ \gamma\sigma^{n-1}(\xi_1^{\mathcal{S}}) & \gamma\sigma^{n-1}(\xi_2^{\mathcal{S}}) & \ldots & \sigma^{n-1}(\xi_0^{\mathcal{S}}) \end{pmatrix},$$

and

$$\tilde{\mathbf{X}}^{\mathcal{S}} = D(\alpha) \cdot \begin{pmatrix} \tilde{x}_0^{\mathcal{S}} & \tilde{x}_1^{\mathcal{S}} & \cdots & \tilde{x}_{n-1}^{\mathcal{S}} \\ \gamma\sigma(\tilde{x}_{n-1}^{\mathcal{S}}) & \sigma(\tilde{x}_0^{\mathcal{S}}) & & \sigma(\tilde{x}_{n-2}^{\mathcal{S}}) \\ \vdots & & \ddots & \vdots \\ \gamma\sigma^{n-1}(\tilde{x}_1^{\mathcal{S}}) & \gamma\sigma^{n-1}(\tilde{x}_2^{\mathcal{S}}) & \ldots & \sigma^{n-1}(\tilde{x}_0^{\mathcal{S}}) \end{pmatrix}.$$

Note that the second matrix factor of $\tilde{\mathbf{X}}^{\mathcal{S}}$ in the previous equation is a codeword of the code

$$\mathcal{C}_{\Pi_{s \in \mathcal{S}} \mathfrak{q}_s} = \left\{ \begin{pmatrix} x_0 & x_1 & \cdots & x_{n-1} \\ \gamma\sigma(x_{n-1}) & \sigma(x_0) & & \sigma(x_{n-2}) \\ \vdots & & \ddots & \vdots \\ \gamma\sigma^{n-1}(x_1) & \gamma\sigma^{n-1}(x_2) & \ldots & \sigma^{n-1}(x_0) \end{pmatrix} \middle| x_\ell \in \prod_{s \in \mathcal{S}} \mathfrak{q}_s \right\}$$

whose minimum determinant can be bounded by [11, Corollary 3] as follows,

$$\delta(\mathcal{C}_{\Pi_{s \in \mathcal{S}} \mathfrak{q}_s}) \geq N(\Pi_{s \in \mathcal{S}} \mathfrak{q}_s). \quad (7)$$

Since the known offset $\mathbf{V}^{\mathcal{S}}$ can be subtracted at the receiver, the minimum determinant of $\mathcal{C}_{\mathcal{S}}$ is

$$\begin{aligned} \delta(\mathcal{C}_{\mathcal{S}}) &= |\det(D(\alpha))|^2 \delta(\mathcal{C}_{\Pi_{s \in \mathcal{S}} \mathfrak{q}_s}) = |N_{\mathbb{L}/\mathbb{K}}(\alpha)|^2 \delta(\mathcal{C}_{\Pi_{s \in \mathcal{S}} \mathfrak{q}_s}) \\ &\overset{(a)}{=} N(\alpha) \delta(\mathcal{C}_{\Pi_{s \in \mathcal{S}} \mathfrak{q}_s}) \overset{(b)}{\geq} N(\alpha) N(\Pi_{s \in \mathcal{S}} \mathfrak{q}_s) \\ &= N(\alpha) \Pi_{s \in \mathcal{S}} N(\mathfrak{q}_s) = N(\alpha) \Pi_{s \in \mathcal{S}} q_s, \end{aligned} \quad (8)$$

where (a) is due to the fact that $\mathbb{K} = \mathbb{Q}(\mathsf{i})$ or $\mathbb{Q}(\omega)$ is a quadratic extension and (b) follows from (7). Moreover, without revealing any side information, the overall codebook would have

$$\delta(\mathcal{C}) = N(\alpha) N(1) = N(\alpha). \quad (9)$$

Combining (6), (8), and (9) results in

$$\Gamma(\mathcal{C}, \mathcal{S}) \geq \frac{10 \log_{10}(\Pi_{s \in \mathcal{S}} q_s)}{n \frac{1}{2n} \sum_{s \in \mathcal{S}} \log_2(q_s)} = 6 \text{ dB/bits per real symbol.}$$

To prove the second statement, we note that if the ideal $\Pi_{s \in \mathcal{S}} \mathfrak{q}_s$ is principal, then we can indeed find elements in the ideal such that the inequality in (7) (and thus (b) in (8)) holds with equality. □

B. LSTIC with non-principal $\mathfrak{I}$

We now construct LSTIC from a STBC based on a cyclic division algebra $\mathcal{A} = (\mathbb{L}/\mathbb{K}, \sigma, \gamma)$ and a non-principal ideal $\mathfrak{I}$ in $\mathfrak{O}_{\mathbb{L}}$. Let $\mathfrak{q}_1, \ldots, \mathfrak{q}_K$ be K ideals in $\mathfrak{O}_{\mathbb{L}}$ that are relatively prime and have norm $N(\mathfrak{q}_k) = q_k$, $k \in \{1, \ldots, K\}$. We again let $\mathfrak{q}_1 \cdot \ldots \cdot \mathfrak{q}_K = \mathfrak{q}$. We further assume that each $\mathfrak{q}_k$ and $\mathfrak{I}$ are relatively prime, which also implies that $\mathfrak{q}$ and $\mathfrak{I}$ are relatively prime. From the second isomorphism theorem [13, Theorem 2.12] and CRT, we have

$$\begin{aligned} \mathfrak{I}/\mathfrak{I}\mathfrak{q} &\overset{(a)}{=} \mathfrak{I}/\mathfrak{I} \cap \mathfrak{q} \overset{(b)}{\cong} (\mathfrak{I} + \mathfrak{q})/\mathfrak{q} \overset{(c)}{=} \mathfrak{O}_{\mathbb{L}}/\mathfrak{q} \\ &\overset{(d)}{\cong} \mathfrak{O}_{\mathbb{L}}/\mathfrak{q}_1 \times \ldots \times \mathfrak{O}_{\mathbb{L}}/\mathfrak{q}_K \cong \mathbb{B}_{q_1} \times \ldots \times \mathbb{B}_{q_K}, \end{aligned}$$

where both (a) and (c) are due to the fact that $\mathfrak{q}$ and $\mathfrak{I}$ are relatively prime, (b) follows from the second isomorphism theorem, and (d) follows from CRT. We use $\mathbb{B}_{q_k}$ to denote the quotient ring that is isomorphic to $\mathfrak{O}_{\mathbb{L}}/\mathfrak{q}_k$ which has size q_k. Let $\mathcal{M}$ be an isomorphism that maps elements in $\mathbb{B}_{q_1} \times \ldots \times \mathbb{B}_{q_K}$ to a complete set of coset leaders of $\mathfrak{I}/\mathfrak{I}\mathfrak{q}$.

For $k \in \{1, \ldots, K\}$, we again enforce $w_k = (w_{k,0}, \ldots, w_{k,n-1}) \in \mathbb{B}_{q_k}^n$ where each $\ell \in \{0, \ldots, n-1\}$. The sub-messages $w_{1,\ell}, \ldots, w_{K,\ell}$ are collected and encoded into x_ℓ the signal of the $\ell \in \{0, \ldots, n-1\}$ layer as

$$x_\ell = \mathcal{M}(w_{1,\ell}, \ldots, w_{K,\ell}) \in \mathfrak{I}/\mathfrak{I}\mathfrak{q}, \quad \ell \in \{0, \ldots, n-1\}.$$

The overall codebook now corresponds to $\{x_0 + x_1 \mathsf{e} + \ldots + x_{n-1} \mathsf{e}^{n-1} | x_0, \ldots, x_{n-1} \in \mathfrak{I}/\mathfrak{I}\mathfrak{q}\}$ a subset of $\bar{\mathcal{A}}_{\mathfrak{I}}$ and has the matrix form as that in (4) with $x_0, \ldots, x_{n-1} \in \mathfrak{I}/\mathfrak{I}\mathfrak{q}$. Note again that when $\mathfrak{I}$ and $\mathfrak{O}_{\mathbb{L}}$ are such that perfect STBCs exist, the overall code is itself a perfect STBC.

Theorem 3. For any $\mathcal{S} \subset \{1, \ldots, K\}$, the side information gain achieved by the proposed LSTIC with non-principal ideal $\mathfrak{I}$ is lower bounded as $\Gamma(\mathcal{C}, \mathcal{S}) \geq 6 + \gamma_{\mathfrak{I}}$ dB/bits per real symbol, where $\gamma_{\mathfrak{I}} = 20 \log_{10} \left(\frac{N(\mathfrak{I})}{\min_{x \in \mathfrak{I}} N_{\mathbb{L}/\mathbb{Q}}(x)} \right)$, is negative and is only a function of $\mathfrak{I}$ and is independent of $\mathcal{S}$.

This theorem can be proved in the similar vein to that of Theorem 2. Please refer to [14] for the proof.

C. Design examples for $n_t = 2$ and $K = 2$

Simulation results for the proposed LSTIC with Golden algebra for the 2×2 MIMO channel are provided in Fig. 2. In this figure, three sets of simulations are performed. In the first one, we constructed LSTIC with two principal ideals generated by $\beta_1 = (\bar{\theta} - \mathrm{i}\theta)$ and $\beta_2 = (\bar{\theta} + \mathrm{i}\theta)$, respectively, which both have norm equal to $3^2 = 9$. Thus, each message $w_k \in \mathbb{B}_9^2$. Since $3\mathfrak{O}_{\mathbb{L}} = \beta_1 \beta_2 \mathfrak{O}_{\mathbb{L}}$, the overall codebook corresponds to $x_0, x_1 \in \mathfrak{O}_{\mathbb{L}}/3\mathfrak{O}_{\mathbb{L}}$ and hence has the cubic shape. Simulation results in Fig. 2 show that revealing either message to the receiver provides roughly 7.3 dB of SNR gain. This conforms with the analysis using (1) that when reveal either message, we expect to achieve SNR gain $\frac{1}{4} 10 \log_{10} \left(\frac{118}{10} \right) + \frac{1}{2} 10 \log_{10} (9) \approx 7.45$ dB, where 118 and 10 inside the first logarithm are $N_{\mathcal{C}}$ and $N_{\mathcal{C}_{\mathcal{S}}}$, respectively and the 9 inside the second logarithm is the ratio of $\delta(\mathcal{C}_{\mathcal{S}})$ and $\delta(\mathcal{C})$.

In the second set of simulations, the two principal ideals are replaced by those generated by $\beta_1 = (1 + \mathrm{i}\bar{\theta})^2$ and $\beta_2 = (1 - \mathrm{i}\bar{\theta})^2$, respectively. $\beta_1 \mathfrak{O}_{\mathbb{L}}$ and $\beta_2 \mathfrak{O}_{\mathbb{L}}$ both have norm equal to $5^2 = 25$. Moreover, $5\mathfrak{O}_{\mathbb{L}} = \beta_1 \beta_2 \mathfrak{O}_{\mathbb{L}}$; thereby, the overall codebook corresponds to $x_0, x_1 \in \mathfrak{O}_{\mathbb{L}}/5\mathfrak{O}_{\mathbb{L}}$ and hence has the cubic shape. Simulation results in Fig. 2 show that revealing either message to the receiver provides roughly 10 dB of SNR gain. This again coincides with the analysis which says that by revealing one side information, we can expect an SNR gain of $\frac{1}{4} 10 \log_{10} \left(\frac{656}{32} \right) + \frac{1}{2} 10 \log_{10} (25) \approx 10.27$ dB, where 656 and 32 inside the first logarithm are $N_{\mathcal{C}}$ and $N_{\mathcal{C}_{\mathcal{S}}}$, respectively. In the last set of simulations, the two prime ideals generated by $\beta_1 = \left((1 + \theta) + \mathrm{i}(1 + \bar{\theta}) \right)$ and $\beta_2 = \left((1 + \theta) - \mathrm{i}(1 + \bar{\theta}) \right)$ with $\beta_1 \beta_2 = 7\mathfrak{O}_{\mathbb{L}}$ are considered. Simulation results show that a roughly 12.1 dB SNR gain can be obtained by revealing either of the message. This again can be well predicted by the analysis which indicates that we can expect an SNR gain of $\frac{1}{4} 10 \log_{10} \left(\frac{2042}{41} \right) + \frac{1}{2} 10 \log_{10} (49) \approx 12.69$ dB.

We end this section by noting that as we show in [14, Remark 11], when specialized to Golden algebra, the proposed LSTIC is not a special case of the Golden-coded index coding in [9] and vice versa. Moreover, the framework proposed in this paper works for any algebraic lattice STBC. More design examples including the 3×3, 4×4, and 6×6 perfect codes are available in [14].

V. Conclusions

In this paper, we have studied the problem of multicasting K independent messages via MIMO links to multiple receivers where each of them already has a subset of messages as side information. A novel scheme, LSTIC, constructed using the framework of cyclic division algebras has been proposed for exploiting receiver side information without prior knowledge of the side information configuration at the transmitter. It has been shown that the proposed LSTIC possesses the desirable property that for any possible side information the minimum determinant increases exponentially as the rate of the side information increases. Moreover, when constructed over a perfect STBC, the perfect STBC properties are preserved by our construction and the LSTIC is itself a perfect STBC.

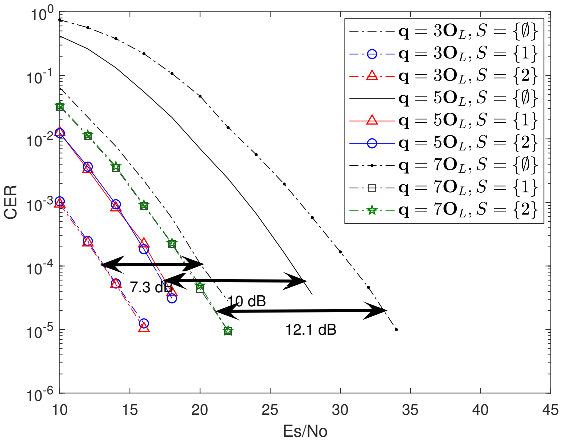

Fig. 2. CER performance for the proposed LSTIC.

References

[1] Y. Birk and T. Kol, "Informed-source coding-on-demand (ISCOD) over broadcast channel," in *Proc. IEEE INFOCOM*, Mar. 1998, pp. 1257–1264.

[2] ——, "Coding on demand by an informed source (ISCOD) for efficient broadcast of different supplemental data to caching clients," *IEEE Trans. Inf. Theory*, vol. 52, no. 6, pp. 2825–2830, Jun. 2006.

[3] M. A. Maddah-Ali and U. Niesen, "Fundamental limits of caching," *IEEE Trans. Inf. Theory*, vol. 60, no. 5, pp. 2856–2867, May 2014.

[4] T. Oechtering, C. Schnurr, I. Bjelakovic, and H. Boche, "Broadcast capacity region of two-phase bidirectional relaying," *IEEE Trans. Inf. Theory*, vol. 54, no. 1, pp. 454–458, Jan. 2008.

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

[6] B. Asadi, L. Ong, and S. J. Johnson, "Optimal coding schemes for the three-receiver AWGN broadcast channel with receiver message side information." *IEEE Trans. Inf. Theory*, vol. 61, no. 10, pp. 5490–5503, Oct. 2015.

[7] L. Natarajan, Y. Hong, and E. Viterbo, "Lattice index coding," *IEEE Trans. Inf. Theory*, vol. 61, no. 12, pp. 6505–6525, Dec. 2015.

[8] Y.-C. Huang, "Lattice index codes from algebraic number fields," *IEEE Trans. Inf. Theory*, vol. 63, no. 4, pp. 2098–2112, Apr. 2017.

[9] Y.-C. Huang, Y. Hong, and E. Viterbo, "Golden-coded index coding," in *Proc. IEEE ISIT*, Jun. 2017, pp. 2548–2552.

[10] B. A. Sethuraman, B. S. Rajan, and V. Shashidhar, "Full-diversity, high-rate space-time block codes from division algebra," *IEEE Trans. Inf. Theory*, vol. 49, no. 10, pp. 2596–2616, Oct. 2003.

[11] F. Oggier, G. Rekaya, J.-C. Belfiore, and E. Viterbo, "Perfect space-time block codes," *IEEE Trans. Inf. Theory*, vol. 52, no. 9, pp. 3885–3902, Sep. 2006.

[12] F. Oggier, J.-C. Belfiore, and E. Viterbo, "Cyclic division algebras: A tool for space-time coding," *Foundations and Trends in Communications and Information Theory*, vol. 4, no. 1, pp. 1–95, 2007.

[13] T. W. Hungerford, *Algebra (Graduate Texts in Mathematics)*. Springer, 1974.

[14] Y.-C. Huang, Y. Hong, E. Viterbo, and L. Natarajan, "Layered space-time index coding," *IEEE Trans. Inf. Theory*, Sep. 2017, submitted, arXiv:1709.04379 [cs.IT].