Layered Space-Time Index Coding

Yu-Chih Huang, *Member, IEEE*, Yi Hong, *Senior Member, IEEE*, Emanuele Viterbo, *Fellow, IEEE*, and Lakshmi Natarajan

***Abstract*— Multicasting K independent messages via multiple-input multiple-output 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 (STBC), including perfect STBC, is proposed. We analyze the proposed LSTIC and show that it provides minimum determinant gains that are exponential with the amount of information contained in the side information for *any possible side information*. When constructed over a perfect STBC, the proposed LSTIC is itself a perfect STBC and hence many desired properties are preserved. To illustrate, we construct LSTIC over the following well-known STBCs: Golden code; 3×3, 4×4, and 6×6 perfect STBCs; and Alamouti code. Simulation results show that the obtained side information gain can be well predicted by our analysis.**

***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 previously received signals; in the coded caching technique [3], [4], the side information is prefetched into users' local cache memories during off-peak hours; and in wireless relay networks [5]–[7], 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 including [5], [6], [8]–[11] focuses on characterizing the capacity region of the AWGN broadcast channel with message side information. The capacity region of the two-user broadcast channel with receiver message side information has been completely characterized [5], [8]. 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. As a result, the capacity region for the three-user case has not been fully characterized for some index sets [9]–[11] and our knowledge about more than three users is limited to some special cases [12], [13].

The second category including [14]–[18] considers designing codes/constellations 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. In [14], Mahesh and Rajan consider the AWGN broadcast channel and assume that the transmitter knows all the index sets, i.e., the side information configuration is available at the transmitter. The scheme proposed in [14] consists of a linear index coding followed by an algorithm that maps coded bits onto a phase shift keying (PSK) modulation. It is shown in [14] that this scheme indeed can provide a reduction in probability of error proportional to the amount of side information.

Another line of research within this category ([15]–[18]), 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 [15]–[18] where all the receivers demand all the messages.

In [15] and [16], Natarajan *et al.* study code design for the AWGN broadcast channel where minimum distance is one of the most crucial parameters to be maximized. They first propose a coding scheme in [15] by partitioning

Manuscript received September 13, 2017; revised May 11, 2018; accepted May 19, 2018. Date of publication May 30, 2018; date of current version December 19, 2018. Y.-C. Huang was supported by the Ministry of Science and Technology, Taiwan, under Grant MOST 106-2628-E-305-001-MY3. Y. Hong and E. Viterbo were supported by the Australian Research Council through the Discovery Project under Grant DP160101077. L. Natarajan was supported by the INSPIRE Research Grant from the Department of Science and Technology, India, under Grant DST/INSPIRE/04/2015/002094. This paper was presented in part at the 2018 IEEE International Symposium on Information Theory.

Y.-C. Huang is with the Department of Communication Engineering, National Taipei University, New Taipei City 23741, Taiwan (e-mail: ychuang@mail.ntpu.edu.tw).

Y. Hong and E. Viterbo are with the Department of Electrical and Computer Systems Engineering, Monash University, Melbourne, VIC 3800, Australia (e-mail: yi.hong@monash.edu; emanuele.viterbo@monash.edu).

L. Natarajan is with the Department of Electrical Engineering, IIT Hyderabad, Sangareddy 502285, India (e-mail: lakshminatarajan@iith.ac.in).

Communicated by J.-F. Chamberland, Associate Editor for Communications.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIT.2018.2842144

multi-dimensional pulse amplitude modulation (PAM) into subsets via computer search for up to five messages with the message size up to 2^6. Exploiting the algebraic structure induced by the Chinese remainder theorem (CRT), a novel coding scheme, lattice index coding, is then proposed in [16] to accommodate *any number of messages* with message sizes relatively prime to each other. Both the schemes in [15] and [16] are shown to provide gains in minimum distance exponential with the rate of the side information, for any index set and any side information content.

In [17], Huang considers the same multicasting problem with message side information, where each link experiences a Rayleigh fading channel on top of the AWGN noise. It is well-known that in contrast to the AWGN channel, maximizing minimum distance alone is far from enough for the Rayleigh fading channel and the minimum product distance dominates the performance [19]–[21]. The lattice index coding scheme proposed in [17] generalizes the idea of [16] from some famous principal ideal domains to 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 and any side information content. The multicasting problem with message side information is then considered in [18] under the 2×2 MIMO setting where the transmitter and the receivers are equipped with two antennas. For such a MIMO setting, the minimum determinant of the code serves as one of the most important parameters to be maximized [21], [22] and algebraic space-time block codes (STBC) constructed from cyclic division algebras [23]–[26] are a class of codes that possess many desired properties. Since CRT does not hold for non-commutative rings such as cyclic division algebras, the trick used in [16] and [17] does not work here in general. In [18], the problem is circumvented by using the bijective mapping between the Golden algebra and a commutative ring found in [27] together with some special ideals whose group structure is preserved by the mapping. As a result, we successfully construct Golden-coded index coding from Golden code, a subclass of perfect codes for the case with two transmitter and receiver antennas, and show that the minimum determinant increases exponentially with the rate of the side information for any index set.

We note that in the absence of side information at receivers, the considered problem reduces to multicasting a common message over the MIMO channel to multiple receivers. For this setting, the code design problem is essentially identical for every receiver and one can focus on a single generic receiver; this makes the code design problem identical to that for the point-to-point MIMO channel that has been intensively investigated (see [22] and references therein). However, since conventional space-time codes do not take into account potential availability of side information at receivers, there is no guarantee that these codes can efficiently translate side information into performance gain. Of course having side information will never hurt, but asking steady and fair side information gain regardless of the content and the configuration of side information poses a new challenge. In fact, even for the single-antenna AWGN channel, Example 3 of [16] has shown that careless designs based on the Ungerboeck's set partitioning rule [28] may have bad performance for some side information configuration/content.

A. Contributions

We consider the problem of multicasting over $n \times n$ MIMO channel with message side information. Since the bijective mapping in [27] and the special ideals identified in [18] only work for the golden algebra, the cyclic division algebra underlying golden code, it is unclear how to construct good lattice index codes for a general $n \times n$ MIMO channel. In this work, we overcome this challenge by recognizing and leveraging the layered structure of algebraic lattice space-time codes to propose *layered space-time index coding* (LSTIC), a general framework of constructing lattice space-time index codes from algebraic STBC. 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 the SNR reduction (normalized by the rate of the side information) to achieve the same error probability, given 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 index set and any side information content*.

We apply the proposed framework with the Golden code, 3×3, 4×4, 6×6 perfect STBCs, and Alamouti code, and show that our analysis well predicts the actual side information gains obtained from simulations. For each of the above codes, we also provide a table of the corresponding prime ideal factorizations for $p < 100$, over which the LSTIC can be constructed according to the desired message sizes.

We note that the technique used in [18] attempts to partition the golden algebra into left ideals and requires the code to be constructed over some special left ideals whose group structure are preserved by the bijective mapping of [27]. In contrast, the proposed LSTIC partitions the cyclic division algebra layer by layer, where the partition in each layer can be done via CRT. When specialized to the Golden code, the proposed LSTIC is not a special case of the Golden-coded index coding in [18] and vice versa.

B. Notations

Throughout the paper, the following notations are used. Matrices are written in capital boldface, for example $\mathbf{X}$. Let $\mathrm{i} \triangleq \sqrt{-1}$ 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.

C. Organization

The rest of the paper is organized as follows. In Section II, we state the problem of physical-layer index coding over MIMO channel and formally define the side information gain, the performance measure that we will use throughout the paper. Background knowledge on algebra, algebraic number theory, and cyclic division algebra is given in Section III. The LSTIC is then proposed and analyzed in Section IV. In Sections V-IX, we construct LSTIC over Golden code, 3×3 perfect STBC, 4×4 perfect STBC, 6×6 perfect STBC, and Alamouti code. We then conclude the paper in Section X.

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 $\mathbb{E}[\|\mathbf{X}\|^2]=n_tT$. In a space-time code, each codeword $\mathbf{X}$ is used to transmit r information-bearing real symbols. 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 $\mathrm{SNR}_l \triangleq \frac{n_t}{\sigma_l^2}$.

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

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

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. This makes the problem of every ℓ identical for the base station. We therefore focus on a generic user and drop the subscript (superscript in some cases) ℓ. The dummy variable ℓ is then released for later use.

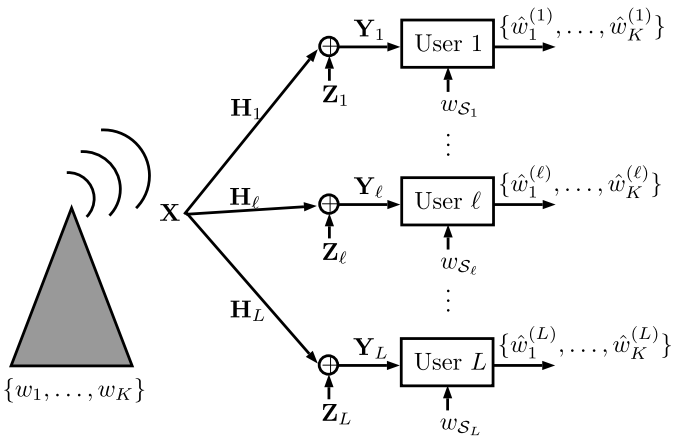

Fig. 1. Multicasting $\{w_1,\ldots,w_K\}$ over MIMO channel to L receivers where each receiver $\ell\in\{1,\ldots,L\}$ has a subset of messages $w_{\mathcal{S}_\ell}$ as side information.

Following [22], we define $\mathbf{A}\triangleq(\mathbf{X}-\mathbf{X}')(\mathbf{X}-\mathbf{X}')^\dagger$ for any pair of codeword matrices $\mathbf{X},\mathbf{X}'\in\mathcal{C}$. Let r be the rank of $\mathbf{A}$. For the generic user with $\mathcal{S}=\emptyset$, in the high SNR regime, the probability of mistaking $\mathbf{X}'$ for $\mathbf{X}$ can be bounded as

$$\Pr(\mathbf{X}\to\mathbf{X}')\leq\left(\frac{\mathrm{SNR}\,\Delta^{1/r}}{4\ n_t}\right)^{-rn_r},$$

where $\Delta=\prod_{m=1}^{r}\lambda_m$ with $\lambda_1,\ldots,\lambda_m$ being the non-zero eigenvalues of $\mathbf{A}$. Moreover, for full rank codes, i.e., $r=n_t$ and

$$\Delta=\prod_{m=1}^{n_t}\lambda_m=\det(\mathbf{A})\neq 0,$$

we define the *minimum determinant* of $\mathcal{C}$ as follows,

$$\delta(\mathcal{C})\triangleq\min_{\mathbf{X}\neq\mathbf{X}'\in\mathcal{C}}\det(\mathbf{A}).$$

If $\mathcal{C}$ is carved from a lattice Λ [29], we have

$$\delta(\mathcal{C})=\min_{\mathbf{X}\neq\mathbf{0}\in\Lambda}\det(\mathbf{X})^2. \tag{1}$$

To estimate the probability of error more accurately, let us define $N_{\mathbf{X}}$ the number of codewords $\mathbf{X}'\in\mathcal{C}$ resulting in $\det(\mathbf{A})=\delta(\mathcal{C})$ and define

$$N_{\mathcal{C}}\triangleq\frac{1}{|\mathcal{C}|}\sum_{\mathbf{X}\in\mathcal{C}}N_{\mathbf{X}}, \tag{2}$$

the average of $N_{\mathbf{X}}$ over $\mathbf{X} \in \mathcal{C}$. For a STBC carved from a lattice, we can now approximate the probability of error as

$$\begin{aligned} p_e &= \frac{1}{|\mathcal{C}|}\sum_{\mathbf{X}\in\mathcal{C}} \mathbb{P}\left(\bigcup_{\mathbf{X}'\neq\mathbf{X}} \mathbf{X}\to\mathbf{X}'\right) \\ &\overset{(a)}{\approx} \frac{1}{|\mathcal{C}|}\sum_{\mathbf{X}\in\mathcal{C}} N_{\mathbf{X}}\left(\frac{\mathrm{SNR}\delta(\mathcal{C})^{1/n_t}}{4\ n_t}\right)^{-n_t n_r} \\ &= N_{\mathcal{C}}\left(\frac{\mathrm{SNR}\delta(\mathcal{C})^{1/n_t}}{4n_t}\right)^{-n_t n_r}, \end{aligned} \tag{3}$$

where the approximation in (a) will become quite accurate in the high SNR regime.

Having had the approximation in (3), we can now follow [18] to derive the side information gain as follows. We first note that with the knowledge of side information $w_s = v_s, \forall s \in \mathcal{S}$, the generic user can throw away all the codewords that do not correspond to this side information. The codebook then becomes

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

a subcode of $\mathcal{C}$. Since $\mathcal{C}_{\mathcal{S}} \subseteq \mathcal{C}$, the minimum determinant of $\mathcal{C}_{\mathcal{S}}$, $\delta(\mathcal{C}_{\mathcal{S}})$, will be no less than $\delta(\mathcal{C})$. Let us now see how gains in minimum determinant can be translated into SNR gains. Following [18], we let SNR and $\mathrm{SNR}_{\mathcal{S}}$ be the SNR required for the codebooks $\mathcal{C}$ and $\mathcal{C}_{\mathcal{S}}$, respectively, to achieve a same error probability p_e. Then (3) says that

$$\begin{aligned} & N_{\mathcal{C}}\left(\frac{\mathrm{SNR}\delta(\mathcal{C})^{1/n_t}}{4\ n_t}\right)^{-n_t n_r} \\ &\approx\ N_{\mathcal{C}_{\mathcal{S}}}\left(\frac{\mathrm{SNR}_{\mathcal{S}}\delta(\mathcal{C}_{\mathcal{S}})^{1/n_t}}{4\ n_t}\right)^{-n_t n_r} \\ &(\Leftrightarrow)\quad 10\log_{10}(\mathrm{SNR}) - 10\log_{10}(\mathrm{SNR}_{\mathcal{S}}) \\ &\approx\ \frac{1}{n_t n_r}10\log_{10}\left(\frac{N_{\mathcal{C}}}{N_{\mathcal{C}_{\mathcal{S}}}}\right) + \frac{1}{n_t}10\log_{10}\left(\frac{\delta(\mathcal{C}_{\mathcal{S}})}{\delta(\mathcal{C})}\right), \end{aligned} \tag{4}$$

which represents the SNR gain in dB provided by the side information $w_{\mathcal{S}}$. As mentioned in [18] 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 SNR gain as $10\log_{10}\left(\delta(\mathcal{C}_{\mathcal{S}})/\delta(\mathcal{C})\right)^{1/n_t}$ 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

$$\Gamma(\mathcal{C},\mathcal{S}) \triangleq \frac{10\log_{10}\left(\frac{\delta(\mathcal{C}_{\mathcal{S}})}{\delta(\mathcal{C})}\right)}{n_t R_{\mathcal{S}}}, \tag{5}$$

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 (4) into the definition of side information gain results in a better approximation. Hence, although we use (5) as the design guideline throughout the paper, (4) is also used to confirm the simulation results.

III. Background

In this section, we first review basic knowledge including algebra and algebraic number theory. We then focus on cyclic division algebra and its connection to lattice STBC. To make the paper concise, we only review the minimum required background for understanding the discussion that follows. For details, please refer, for example, to [20], [22], and [30]–[32].

A. Algebra

Let $\mathcal{R}$ be a *commutative ring* equipped with two operations addition $+$ and multiplication $\cdot$. An *ideal* $\mathfrak{I}$ of $\mathcal{R}$ is an additive subgroup of $\mathcal{R}$ with respect to $+$ that absorbs the multiplication of $\mathcal{R}$, i.e., it satisfies $a\cdot r \in \mathfrak{I}$ for $a \in \mathfrak{I}$ and $r \in \mathcal{R}$. An ideal $\mathfrak{I}$ is a *principal ideal* if it can be generated by a singleton, i.e., $\mathfrak{I} = a\mathcal{R}$ for some $a \in \mathcal{R}$. A *proper ideal* $\mathfrak{I}$ is an ideal that is at the same time, a proper subset of $\mathcal{R}$, i.e., $\emptyset \neq \mathfrak{I} \subset \mathcal{R}$.

For an ideal $\mathfrak{I}$ and any two elements $a, b \in \mathcal{R}$, a is congruent to b *modulo* $\mathfrak{I}$ if and only if $a - b \in \mathfrak{I}$, which defines an equivalence relation. The *quotient ring* $\mathcal{R}/\mathfrak{I}$ of $\mathcal{R}$ by $\mathfrak{I}$ is the collection of equivalence classes with addition and multiplication defined as the original ones followed by modulo $\mathfrak{I}$ operation as follows,

$$\begin{aligned} (a+\mathfrak{I}) + (b+\mathfrak{I}) &= (a+b)+\mathfrak{I}, \text{ and} \\ (a+\mathfrak{I})\cdot(b+\mathfrak{I}) &= (a\cdot b)+\mathfrak{I}, \end{aligned}$$

respectively. A *prime ideal* $\mathfrak{p}$ of $\mathcal{R}$ is a proper ideal satisfying that whenever $ab \in \mathfrak{p}$ for $a, b \in \mathcal{R}$, then either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. We now define the *sum and product of ideals*. Let $\mathfrak{I}_1$ and $\mathfrak{I}_2$ be two ideals of $\mathcal{R}$, the sum of two ideals is itself an ideal and is defined as

$$\mathfrak{I}_1 + \mathfrak{I}_2 \triangleq \{a+b : a \in \mathfrak{I}_1, b \in \mathfrak{I}_2\}.$$

The product of $\mathfrak{I}_1$ and $\mathfrak{I}_2$ is again an ideal and is defined as

$$\mathfrak{I}_1\mathfrak{I}_2 \triangleq \left\{ \sum_{i=1}^{n} a_i b_i : a_i \in \mathfrak{I}_1, b_i \in \mathfrak{I}_2, n \in \mathbb{N} \right\}.$$

In general, $\mathfrak{I}_1\mathfrak{I}_2 \subseteq \mathfrak{I}_1 \cap \mathfrak{I}_2$. Two ideals are said to be *relatively prime* if $\mathcal{R} = \mathfrak{I}_1 + \mathfrak{I}_2$. When $\mathfrak{I}_1$ and $\mathfrak{I}_2$ are relatively prime, we further have $\mathfrak{I}_1\mathfrak{I}_2 = \mathfrak{I}_1 \cap \mathfrak{I}_2$. We say $\mathfrak{I}_1$ divides $\mathfrak{I}_2$, denoted as $\mathfrak{I}_1 | \mathfrak{I}_2$, if $\mathfrak{I}_2 = \mathfrak{I}_1\mathfrak{I}_3$ for some ideal $\mathfrak{I}_3$ and consequently $\mathfrak{I}_2 \subseteq \mathfrak{I}_1$.

Consider two commutative rings $\mathcal{R}_1$ and $\mathcal{R}_2$ with two operations $(+,\cdot)$ and $(\oplus,\odot)$, respectively. A *ring homomorphism* between $\mathcal{R}_1$ and $\mathcal{R}_2$ is a function $\sigma : \mathcal{R}_1 \to \mathcal{R}_2$ such that

$$\begin{aligned} \sigma(a+b) &= \sigma(a) \oplus \sigma(b),\ \forall a, b \in \mathcal{R}_1, \\ \sigma(a\cdot b) &= \sigma(a) \odot \sigma(b),\ \forall a, b \in \mathcal{R}_1. \end{aligned}$$

In other words, a ring homomorphism preserves the ring structure. A homomorphism is a monomorphism if it is injective and is an isomorphism if it is bijective. Moreover, an isomorphism $\sigma : \mathcal{R}_1 \to \mathcal{R}_1$ is called automorphism.

We now review two classical results in ring theory whose proofs can be found in a standard textbook.

Lemma 1 (Second isomorphism theorem [30, Th. 2.12]): Let $\mathcal{R}$ be a commutative ring, $\mathfrak{I}_1$ and $\mathfrak{I}_2$ be two ideals. We have the following isomorphism,

$$\mathfrak{I}_1/(\mathfrak{I}_1 \cap \mathfrak{I}_2) \cong (\mathfrak{I}_1 + \mathfrak{I}_2)/\mathfrak{I}_2.$$

In fact, the second isomorphism theorem holds for the more general case where $\mathfrak{I}_1$ is only a subring and not necessarily an ideal.

Lemma 2 (Chinese remainder theorem [30, Corollary 2.27]): Let $\mathfrak{I}_1, \ldots, \mathfrak{I}_n$ be ideals of a commutative ring $\mathcal{R}$. Moreover, $\mathfrak{I}_1, \ldots, \mathfrak{I}_n$ are relatively prime. We have

$$\mathcal{R}/\Pi_{i=1}^{n}\mathfrak{I}_i \cong \mathcal{R}/\mathfrak{I}_1 \times \ldots \times \mathcal{R}/\mathfrak{I}_n.$$

where $\times$ stands for Cartesian product and the operations of the right hand side are defined componentwise.

We provide a quick example for what have been reviewed above.

Example 3: Consider $\mathbb{Z}$ the set of all integers with ordinary addition $+$ and multiplication $\cdot$. Clearly, it forms a commutative ring. $2\mathbb{Z}$ is the principal ideal of $\mathbb{Z}$ consisting of all the even integers. Moreover, it is a prime ideal. The quotient $\mathbb{Z}/2\mathbb{Z} = \mathbb{Z}_2$ forms a ring with addition $+ \mod 2\mathbb{Z}$ and multiplication $\cdot \mod 2\mathbb{Z}$. Also, for $3\mathbb{Z}$ another principal prime ideal of $\mathbb{Z}$, we have the quotient ring $\mathbb{Z}/3\mathbb{Z} = \mathbb{Z}_3$. Since $2 \cdot (-1) + 3 \cdot 1 = 1$, $2\mathbb{Z} + 3\mathbb{Z} = \mathbb{Z}$ and thus $2\mathbb{Z}$ and $3\mathbb{Z}$ are relatively prime. One can easily verify that $2\mathbb{Z} \cap 3\mathbb{Z}$ is precisely $6\mathbb{Z}$. Now, the CRT guarantees the existence of a ring isomorphism between $\mathbb{Z}_6 = \mathbb{Z}/6\mathbb{Z}$ and $\mathbb{Z}_2 \times \mathbb{Z}_3$. One can verify that $\mathcal{M}(v_1, v_2) = 3v_1 - 2v_2 \mod 6\mathbb{Z}$ where $v_1 \in \mathbb{Z}_2$ and $v_2 \in \mathbb{Z}_3$ is a ring isomorphism.

B. Algebraic Numbers and Algebraic Integers

An *algebraic number* is a complex number that is a root of some polynomial with coefficients in $\mathbb{Z}$. Let $\mathbb{L}$ be a field and $\mathbb{K} \subset \mathbb{L}$ be a subfield; $\mathbb{L}$ is said to be a field extension of $\mathbb{K}$, which is usually denoted as $\mathbb{L}/\mathbb{K}$. $\mathbb{L}$ can be viewed as a vector space over $\mathbb{K}$. The *degree* of $\mathbb{L}$ over $\mathbb{K}$, denoted by $[\mathbb{L} : \mathbb{K}]$, is defined as the dimension of the vector space $\mathbb{L}$ over $\mathbb{K}$. A *number field* is a field extension of $\mathbb{Q}$ with finite degree, i.e., a finite extension $\mathbb{K}/\mathbb{Q}$. Every number field $\mathbb{K}$ can be generated from $\mathbb{Q}$ by adjoining an algebraic number θ, i.e., $\mathbb{K} = \mathbb{Q}(\theta)$. An *algebraic integer* is a complex number that is a root of some polynomial with the leading coefficient 1 and other coefficients in $\mathbb{Z}$. For a number field $\mathbb{K}$, we denote by $\mathfrak{O}_{\mathbb{K}}$ the *ring of integers* of $\mathbb{K}$ which comprises all the algebraic integers in $\mathbb{K}$.

Let $\mathbb{L}/\mathbb{K}$ be a *field extension* of $\mathbb{K}$ with degree $[\mathbb{L} : \mathbb{K}] = n$. Throughout the paper, we will further assume that $\mathbb{L}/\mathbb{K}$ is a *Galois extension*. There are exactly n distinct $\mathbb{K}$-automorphisms $\sigma_i : \mathbb{L} \to \mathbb{L}$ for $i \in \{1, \ldots, n\}$, i.e., automorphisms that fix $\mathbb{K}$. Such automorphisms are called (relative) *embeddings*. It can be shown that $\mathrm{Gal}(\mathbb{L}/\mathbb{K}) \triangleq \{\sigma_1, \ldots, \sigma_n\}$ form a group under function composition, which is called the *Galois group*. For $\alpha \in \mathbb{L}$, we define the norm of α as

$$N_{\mathbb{L}/\mathbb{K}}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha),$$

where $\sigma_2(\alpha), \ldots, \sigma_n(\alpha)$ are called the conjugates of $\sigma_1(\alpha) = \alpha$. Let $\{\alpha_1, \ldots, \alpha_n\}$ be an *integral basis* for $\mathfrak{O}_{\mathbb{L}}$, such that any element in $\mathfrak{O}_{\mathbb{L}}$ can be uniquely written as a linear combination of the basis element with coefficients $\mathbb{Z}$. The *discriminant* of a number field $\mathbb{L}$ is defined as

$$d_{\mathbb{L}} \triangleq \det \begin{pmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \ldots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \ldots & \sigma_2(\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \ldots & \sigma_n(\alpha_n) \end{pmatrix}^2.$$

Let $\mathfrak{I}$ be an ideal in $\mathfrak{O}_{\mathbb{L}}$, then $\mathfrak{I}$ can be generated by at most two elements, i.e., $\mathfrak{I} = \alpha\mathfrak{O}_{\mathbb{L}} + \beta\mathfrak{O}_{\mathbb{L}}$ for some $\alpha, \beta \in \mathfrak{O}_{\mathbb{L}}$. The norm of $\mathfrak{I}$ is defined as

$$N(\mathfrak{I}) \triangleq |\mathfrak{O}_{\mathbb{L}}/\mathfrak{I}|.$$

Moreover, if $\mathfrak{I} = \alpha\mathfrak{O}_{\mathbb{L}}$ is principal, $N(\mathfrak{I}) = |N_{\mathbb{L}/\mathbb{Q}}(\alpha)|$.

Let $\mathfrak{p}$ be a prime ideal in $\mathfrak{O}_{\mathbb{L}}$, the ring of integers of $\mathbb{L}$ with $[\mathbb{L} : \mathbb{Q}] = n$. We say that $\mathfrak{p}$ lies above a prime p if $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. For a prime p, the principal ideal $p\mathfrak{O}_{\mathbb{L}}$ can be factorized into $1 \le g \le n$ prime ideals as

$$p\mathfrak{O}_{\mathbb{L}} = \mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_g^{e_g},$$

where $e_i, i \in \{1, \ldots, g\}$, is the *ramification index* of $\mathfrak{p}_i$. Also, for each $\mathfrak{p}_i$, we have $N(\mathfrak{p}_i) = p^{f_i}$ and $\mathfrak{O}_{\mathbb{L}}/\mathfrak{p}_i \cong \mathbb{F}_{p^{f_i}}$ where $1 \le f_i \le n$ is the *inertial degree*. Overall, it can be shown that $\sum_{i=1}^{g} e_i f_i = n$. For a Galois extension, we have $e_1 = e_2 = \ldots = e_g = e$ and $f_1 = f_2 = \ldots = f_g = f$, which implies that $efg = n$. A prime p is ramified in $\mathfrak{O}_{\mathbb{L}}$ if not all $e_i = 1$ in the factorization of $p\mathfrak{O}_{\mathbb{L}}$. Ramified primes in $\mathfrak{O}_{\mathbb{L}}$ are precisely those p that divides the discriminant $d_{\mathbb{L}}$.

Example 4: Consider $\mathbb{Q}(\mathrm{i})$ the field extension obtained from $\mathbb{Q}$ by adjoining i. Every element in $\mathbb{Q}(\mathrm{i})$ has the form $a + b\mathrm{i}$ where $a, b \in \mathbb{Q}$; thus, it is a number field with degree 2. The two $\mathbb{Q}$-automorphisms are $\sigma_1(a + b\mathrm{i}) \to a + b\mathrm{i}$ and $\sigma_2(a + b\mathrm{i}) \to a - b\mathrm{i}$. The Galois group is cyclic and can be generated by σ_2. Since σ_1 is the identity mapping and σ_2 sends an element to its complex conjugate, the norm defined in this number field coincides with the Euclidean norm. The ring of integers is $\mathbb{Z}[\mathrm{i}]$, the Gaussian integers, having integral basis $\{1, \mathrm{i}\}$. The discriminant is computed as follows,

$$d_{\mathbb{Q}(\mathrm{i})} = \det \begin{pmatrix} 1 & \mathrm{i} \\ 1 & -\mathrm{i} \end{pmatrix}^2 = -4.$$

Since $2|d_{\mathbb{Q}(\mathrm{i})}$, $2\mathbb{Z}[\mathrm{i}] = \mathfrak{p}^2$ ramifies where $\mathfrak{p} = (1 + \mathrm{i})\mathbb{Z}[\mathrm{i}]$. This is the only ramified prime in $\mathbb{Q}(\mathrm{i})$. Also, $5\mathbb{Z}[\mathrm{i}] = \mathfrak{p}_1\mathfrak{p}_2$ splits into two prime ideals $\mathfrak{p}_1 = (1 + 2\mathrm{i})\mathbb{Z}[\mathrm{i}]$ and $\mathfrak{p}_2 = (1 - 2\mathrm{i})\mathbb{Z}[\mathrm{i}]$ with $e = 1$ and $f = 1$. Another example is that $3\mathbb{Z}[\mathrm{i}]$ is itself a prime ideal with $e = 1$ and $f = 2$. In each case, we have $efg = 2$.

C. Cyclic Division Algebra and Lattice Space-Time Codes

An *algebra* $\mathcal{A}$ over a field $\mathbb{L}$ is a set satisfying: *i)* it is a vector space over $\mathbb{L}$; *ii)* it is a ring with respect to addition and multiplication by elements of $\mathcal{A}$; and *iii)* $(\alpha a)b = a(\alpha b) = \alpha\ (ab)$ for any $\alpha \in \mathbb{L}$ and $a, b \in \mathcal{A}$. Let $\mathbb{L}/\mathbb{K}$ be a field extension of $\mathbb{K}$ of degree n whose Galois group is a cyclic group generated by σ. One can construct a *cyclic algebra* $\mathcal{A} = (\mathbb{L}/\mathbb{K}, \sigma, \gamma)$ as

$$\begin{aligned}\mathcal{A} &= (\mathbb{L}/\mathbb{K}, \sigma, \gamma) \\ &= \left\{x_0 + x_1\mathsf{e} + \ldots + x_{n-1}\mathsf{e}^{n-1} | x_0, \ldots, x_{n-1} \in \mathbb{L}\right\},\end{aligned}$$

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 (see [22] and reference therein), 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

$$\bar{\mathcal{A}}_{\mathfrak{I}} = \left\{x_0 + x_1\mathsf{e} + \ldots + x_{n-1}\mathsf{e}^{n-1} | x_0, \ldots, x_{n-1} \in \mathfrak{I}\right\}, \quad (6)$$

where $\mathfrak{I}$ is an ideal in $\mathfrak{O}_{\mathbb{L}}$. More specifically, an $n \times n$ STBC thus constructed can be obtained by putting $\bar{\mathcal{A}}_{\mathfrak{I}}$ into the matrix form given by

$$\mathcal{C}_{\mathfrak{I}} = \left\{ \begin{pmatrix} x_0 & x_1 & \ldots & x_{n-1} \\ \gamma\,\sigma(x_{n-1}) & \sigma(x_0) & & \sigma(x_{n-2}) \\ \vdots & & \ddots & \vdots \\ \gamma\,\sigma^{n-1}(x_1) & \gamma\,\sigma^{n-1}(x_2) & \ldots & \sigma^{n-1}(x_0) \end{pmatrix} \right| \left. x_0, \ldots, x_{n-1} \in \mathfrak{I} \right\}. \quad (7)$$

A layer $\ell \in \{0, \ldots, n-1\}$ of the codeword in $\mathcal{C}_{\mathfrak{I}}$ is the collection of the entries in positions $(m, (\ell + m) \mod (n))$ for $m \in \{1, \ldots, n\}$. We note that each layer $\ell \in \{0, \ldots, n-1\}$ corresponds to 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. From this point onward, we restrict the discussion to $\mathbb{K} = \mathbb{Q}(\mathrm{i})$ or $\mathbb{Q}(\omega)$, which corresponds to the case where each x_ℓ is a linear combination of n QAM or HEX constellation symbols. One observes that each codeword $\mathbf{X} \in \mathcal{C}_{\mathfrak{I}}$ conveys n symbols of $\mathbb{L}$, where each symbol x_ℓ is a linear combination of n QAM or HEX symbols. Therefore, the STBC thus constructed is *full-rate*. i.e., it uses an $n \times n$ matrix to transmit n^2 symbols. Another consequence of having each x_ℓ being a linear combination of n QAM or HEX symbols is that the code may not be energy-efficient as compared to sending QAM or HEX symbols directly. This drawback can often be overcome by choosing a suitable ideal $\mathfrak{I}$ such that $\mathcal{C}_{\mathfrak{I}}$ becomes a scaled and rotated version of $\mathbb{Z}[\mathrm{i}]^n$ or $\mathbb{Z}[\omega]^n$.

The determinant of the codeword $\mathbf{X} \in \mathcal{C}_{\mathfrak{I}}$ corresponding to $x \in \mathcal{A}$ is called the *reduced norm* of x. What is important about having the structure of cyclic division algebra is that when $\gamma \in \mathfrak{O}_{\mathbb{K}}$ is not the norm of an element in $\mathbb{L}$, it guarantees that the code is *fully diverse* and has *non-vanishing determinant* (NVD). This is evident from [26, Corollary1 and Corollary 2], which states that the reduced norm of $x \in \bar{\mathcal{A}}_{\mathfrak{O}_{\mathbb{L}}}$ belongs to $\mathfrak{O}_{\mathbb{K}}$ and thus $\delta(\mathcal{C}_{\mathfrak{O}_{\mathbb{L}}}) = 1$. Now, since $\mathfrak{I} \subseteq \mathfrak{O}_{\mathbb{L}}$, one has that $\delta(\mathcal{C}_{\mathfrak{I}}) \geq 1$. In fact, one can obtain better bounds on $\delta(\mathcal{C}_{\mathfrak{I}})$ as follows.

Lemma 5 ([26, Corollary 3 and Corollary 4]): Let $\mathcal{C}_{\mathfrak{I}}$ be a STBC built over the cyclic division algebra $\mathcal{A} = (\mathbb{L}/\mathbb{K}, \sigma, \gamma)$ as in (7), where $\gamma \in \mathfrak{O}_{\mathbb{K}}$ not the norm of an element in $\mathbb{L}$. Then,

$$N(\mathfrak{I}) \leq \delta(\mathcal{C}_{\mathfrak{I}}) \leq \min_{x \in \mathfrak{I}} N_{\mathbb{L}/\mathbb{Q}}(x).$$

We end this section by providing the definition of a *perfect* STBC as follows.

Definition 6: A $n \times n$ STBC is called a perfect STBC if *i)* it is full-rate; *ii)* it is fully diverse and has NVD property; *iii)* the energy used to send the coded symbol on each layer is equal to that for sending the uncoded symbol 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 and show that for any index set, it can provide 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 [18], we recognize the layered structure of STBC reviewed in Section III-C and perform partition 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 the layer ℓ. The main advantage of this approach is that now each layer's signal is in $\mathfrak{O}_{\mathbb{L}}$ and thereby one can apply CRT for partitioning. In what follows, we focus solely on cyclic division algebras with $\gamma \in \mathfrak{O}_{\mathbb{K}}$, such that none of $\gamma, \gamma^2, \ldots, \gamma^{n-1}$ are norms of element in $\mathbb{L}$. We focus on full-rate STBC and split the discussion into two parts depending on whether $\mathfrak{I}$ is principal or not. The first case includes constructions from 2×2, 3×3, and 4×4 perfect STBC while the second case encompasses constructions from the 6×6 perfect STBC. The similar approach can also be applied to Alamouti code for constructing Layered Alamouti-coded index coding, which will be discussed in Section IX.

Remark 7: We emphasize that the approach that we propose in the following in fact applies to any cyclic division algebra with the non-norm element γ with $\mathbb{K} = \mathbb{Q}(\mathrm{i})$ or $\mathbb{Q}(\omega)$. For instance, the STBC design with non-norm element $\gamma \in \mathbb{K}$ in [33] can also be used as the base STBC of our LSTIC. The main reason that we particularly focus on $\gamma \in \mathfrak{O}_{\mathbb{K}}$ is so that we can rely on Lemma 5 to prove a lower bound on the side information gain. Apart from this, the proposed method does not require $\gamma \in \mathfrak{O}_{\mathbb{K}}$.

Remark 8: As will become clear in the following sections, in the absence of side information, i.e., $\mathcal{S} = \emptyset$, the overall code of the proposed LSTIC is itself a lattice space-time code carved from a lattice Λ and hence can be decoded by

existing efficient decoding algorithms such as sphere decoding [34], [35]. Moreover, in the presence of side information, i.e., $\mathcal{S} \neq \emptyset$, the receiver will be decoding a subcode of the overall code. In particular, each subcode corresponds to a finite subset carved from a sublattice of Λ and again existing efficient sphere decoding algorithms can be implemented for decoding.

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, (6) 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 (7) can be rewritten as

$$\left\{ D(\alpha) \cdot \begin{pmatrix} x_0 & x_1 & \ldots & x_{n-1} \\ \gamma\,\sigma(x_{n-1}) & \sigma(x_0) & & \sigma(x_{n-2}) \\ \vdots & & \ddots & \vdots \\ \gamma\,\sigma^{n-1}(x_1) & \gamma\,\sigma^{n-1}(x_2) & \ldots & \sigma^{n-1}(x_0) \end{pmatrix} \middle| \, x_0, \ldots, x_{n-1} \in \mathfrak{O}_{\mathbb{L}} \right\}, \tag{8}$$

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 emphasize here that, as mentioned in Section III-C, the codebook that we actually use should be a scaled version of the above codebook to satisfy the power constraint. However, in our analysis, what we really care is the *ratio* between the minimum determinants of the codebooks with and without side information, where the scaling does not make any difference. Therefore, throughout the paper, when analyzing the proposed scheme, we ignore the scaling factor for the sake of brevity. On the other hand, in our simulations, we do take the scaling into account and normalize the codebook to make the parameters reflect the actual SNR.

We can now use the technique in [17] 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 $N(\mathfrak{q}_k) = q_k$, $k \in \{1, \ldots, K\}$. 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 an 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.

[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. But it is always commutative since a quotient ring of a commutative ring is always commutative. 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.

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

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

The overall codebook corresponds to

$$\bar{\mathcal{A}} = \left\{\alpha x_0 + \alpha x_1\mathsf{e} + \ldots + \alpha x_{n-1}\mathsf{e}^{n-1} | \; x_0, \ldots, x_{n-1} \in \mathfrak{O}_{\mathbb{L}}/\mathfrak{q}\right\},$$

a subset of $\bar{\mathcal{A}}_{\mathfrak{I}}$ and has the matrix form as that in (8) with $x_0, \ldots, x_{n-1} \in \mathfrak{O}_{\mathbb{L}}/\mathfrak{q}$.

For the proposed LSTIC within this class, we can show the following theorem.

Theorem 9: 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 in the proposed scheme, since we focus on full-rate STBC, each message is spread onto n layers of signals, which are elements of the number field $\mathbb{L}$ of degree $[\mathbb{L} : \mathbb{K}] = n$. Also, note that $\mathbb{K} = \mathbb{Q}(\mathrm{i})$ or $\mathbb{Q}(\omega)$. Therefore, each codeword sends $2n^2$ real symbols and the rate of the message w_k is given by

$$R_k = \frac{1}{2n^2}\log_2(q_k^n) = \frac{1}{2n}\log_2(q_k), \quad \text{bits per real symbol.} \tag{9}$$

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. Let us first take $\mathcal{S} = \{s\}$ for example. The ℓth layer's signal can then be rewritten as

$$\begin{aligned} x_\ell^{\{s\}} &= \mathcal{M}(w_{1,\ell}, \ldots, w_{s-1,\ell}, v_{s,\ell}, w_{s+1,\ell}, \ldots, w_{K,\ell}) \\ &\overset{(a)}{=} \mathcal{M}(0, \ldots, 0, v_s, 0, \ldots, 0) \\ &\quad + \mathcal{M}(w_{1,\ell}, \ldots, w_{s-1,\ell}, 0, w_{s+1,\ell}, \ldots, w_{K,\ell}) + \zeta_\ell^{\{s\}} \\ &= \xi_\ell^{\{s\}} + \tilde{x}_\ell^{\{s\}}, \end{aligned}$$

where $\tilde{x}_\ell^{\{s\}} \triangleq \mathcal{M}(w_{1,\ell}, \ldots, w_{s-1,\ell}, 0, w_{s+1,\ell}, \ldots, w_{K,\ell}) + \zeta_\ell^{\{s\}}$, $\zeta_\ell^{\{s\}} \in \mathfrak{q}$, and $\xi_\ell^{\{s\}} \triangleq \mathcal{M}(0, \ldots, 0, v_s, 0, \ldots, 0)$ is known at the receiver. The equality (a) above holds because $\mathcal{M}$ is an isomorphism. From CRT, we have

$$(x_\ell^{\{s\}} - \xi_\ell^{\{s\}}) \mod \mathfrak{q}_s = 0,$$

which implies that $x_\ell^{\{s\}}$ belongs to a shifted version of $\mathfrak{q}_s$. For the general $\mathcal{S}$, we can similarly show that

$$\begin{aligned} x_\ell^{\mathcal{S}} &= \mathcal{M}(d_{1,\ell}, \ldots, d_{K,\ell}) + \mathcal{M}(u_{1,\ell}, \ldots, u_{K,\ell}) + \zeta_\ell^{\mathcal{S}} \\ &= \xi_\ell^{\mathcal{S}} + \tilde{x}_\ell^{\mathcal{S}}, \end{aligned} \tag{10}$$

where $\zeta_\ell^{\mathcal{S}} \in \mathfrak{q}$, $\tilde{x}_\ell^{\mathcal{S}} = \mathcal{M}(u_{1,,\ell}, \ldots, u_{K,\ell}) + \zeta_\ell^{\mathcal{S}}$, and $\xi_\ell^{\mathcal{S}} \triangleq \mathcal{M}(d_{1,\ell}, \ldots, d_{K,\ell})$ with

$$d_{k,\ell} = \begin{cases} v_{k,\ell}, & k \in \mathcal{S}; \\ 0, & k \in \mathcal{S}^c, \end{cases} \tag{11}$$

and

$$u_{k,\ell} = \begin{cases} 0, & k \in \mathcal{S}; \\ w_{k,\ell}, & k \in \mathcal{S}^c. \end{cases} \tag{12}$$

Note that $\xi_\ell^{\mathcal{S}}$ 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

$$\Big\{\alpha(\xi_0^{\mathcal{S}} + \ldots + \xi_{n-1}^{\mathcal{S}}\mathsf{e}^{n-1}) + \alpha(\tilde{x}_0^{\mathcal{S}} + \ldots + \tilde{x}_{n-1}^{\mathcal{S}}\mathsf{e}^{n-1}) | \\ \tilde{x}_0^{\mathcal{S}}, \ldots, \tilde{x}_{n-1}^{\mathcal{S}} \in \Pi_{s\in\mathcal{S}}\mathfrak{q}_s\Big\},$$

Hence, thanks to that σ is 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

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

and

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

Note that the second part of $\tilde{\mathbf{X}}^{\mathcal{S}}$ is a codeword of the code

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

whose minimum determinant can be bounded by Lemma 5 as follows,

$$\delta(\mathcal{C}_{\Pi_{s\in\mathcal{S}}\mathfrak{q}_s}) \geq N(\Pi_{s\in\mathcal{S}}\mathfrak{q}_s). \tag{13}$$

The receiver can now subtract the known $\mathbf{V}^{\mathcal{S}}$ and compute the minimum determinant as

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

where (a) follows from the fact that $\mathbb{K} = \mathbb{Q}(\mathsf{i})$ or $\mathbb{Q}(\omega)$ is a quadratic extension. Plugging (13) into the above equation results in

$$\begin{aligned} \delta(\mathcal{C}_{\mathcal{S}}) &\geq N(\alpha)N(\Pi_{s\in\mathcal{S}}\mathfrak{q}_s) \\ &= N(\alpha)\Pi_{s\in\mathcal{S}}N(\mathfrak{q}_s) = N(\alpha)\Pi_{s\in\mathcal{S}}q_s, \end{aligned} \tag{14}$$

where the last equality follows from the fact that the ideal norm is multiplicative. Moreover, without revealing any side information, the overall codebook would have

$$\delta(\mathcal{C}) = N(\alpha)N(1) = N(\alpha). \tag{15}$$

Combining (9), (14), and (15) results in

$$\begin{aligned} \Gamma(\mathcal{C}, \mathcal{S}) &\geq \frac{10\log_{10}(\Pi_{s\in\mathcal{S}}q_s)}{n\frac{1}{2n}\sum_{s\in\mathcal{S}}\log_2(q_s)} \\ &= \frac{\sum_{s\in\mathcal{S}} 20\log_{10}(q_s)}{\sum_{s\in\mathcal{S}}\log_2(q_s)} = 6 \text{ dB/bits per real symbol.} \end{aligned}$$

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 an element in the ideal such that the inequality in (14) holds with equality. Hence, if $\mathfrak{q}_1, \ldots, \mathfrak{q}_K$ are all principal, $\Gamma(\mathcal{C}, \mathcal{S}) = 6$ dB for every $\mathcal{S}$. □

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 $\mathfrak{O}_{\mathbb{L}}$ as described in (6). 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 [30] 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 (7) with $x_0, \ldots, x_{n-1} \in \mathfrak{I}/\mathfrak{I}\mathfrak{q}$.

For the proposed LSTIC within this class, we can show the following theorem.

Theorem 10: 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

$$\Gamma(\mathcal{C}, \mathcal{S}) \geq 6 + \gamma_{\mathfrak{I}} \text{ dB/bits per real symbol,}$$

where

$$\gamma_{\mathfrak{I}} = 20\log_{10}\left(\frac{N(\mathfrak{I})}{\min_{x\in\mathfrak{I}} N_{\mathbb{L}/\mathbb{Q}}(x)}\right), \tag{16}$$

is negative and is only a function of $\mathfrak{I}$. i.e., it is independent of $\mathcal{S}$.

Proof: We again note that the rate of the message w_k is given by

$$R_k = \frac{1}{2n^2}\log_2(q_k^n) = \frac{1}{2n}\log_2(q_k), \quad \text{bits per real symbol.} \tag{17}$$

We consider a generic receiver having index set $\mathcal{S}$. Suppose the messages $w_s = v_s$ for $s \in \mathcal{S}$ are known, which means that $w_{s,\ell} = v_{s,\ell}$ for all $\ell \in \{0,\dots,n-1\}$ are known at the receiver. Similar to (10), we have

$$\begin{aligned} x_\ell^{\mathcal{S}} &= \mathcal{M}(d_{1,\ell},\dots,d_{K,\ell}) + \mathcal{M}(u_{1,\ell},\dots,u_{K,\ell}) + \zeta_\ell^{\mathcal{S}} \\ &= \xi_\ell^{\mathcal{S}} + \tilde{x}_\ell^{\mathcal{S}}, \end{aligned}$$

where $d_{k,\ell}$ and $u_{k,\ell}$ are defined in (11) and (12), respectively, and $\zeta_\ell^{\mathcal{S}} \in \mathfrak{I}\mathfrak{q}$. Therefore, we have

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

which means that $x_\ell^{\mathcal{S}}$ belongs to a shifted version of

$$\begin{aligned} \cap_{s\in\mathcal{S}}\mathfrak{I}\mathfrak{q}_s &\overset{(a)}{=} \cap_{s\in\mathcal{S}}(\mathfrak{I}\cap\mathfrak{q}_s) \\ &= \mathfrak{I}\cap(\cap_{s\in\mathcal{S}}\mathfrak{q}_s) \overset{(b)}{=} \mathfrak{I}\Pi_{s\in\mathcal{S}}\mathfrak{q}_s, \end{aligned}$$

where (a) follows from that $\mathfrak{I}$ and $\mathfrak{q}_s$ are relatively prime for each s and (b) is due to the fact that $\mathfrak{q}_1,\dots,\mathfrak{q}_K$ are relatively prime.

After revealing $w_{\mathcal{S}}$, the code $\mathcal{C}_{\mathcal{S}}$ would correspond to

$$\left\{(\xi_0^{\mathcal{S}} + \ldots + \xi_{n-1}^{\mathcal{S}}\mathsf{e}^{n-1}) + (\tilde{x}_0^{\mathcal{S}} + \ldots + \tilde{x}_{n-1}^{\mathcal{S}}\mathsf{e}^{n-1}) \middle| \tilde{x}_0^{\mathcal{S}},\dots,\tilde{x}_{n-1}^{\mathcal{S}} \in \mathfrak{I}\Pi_{s\in\mathcal{S}}\mathfrak{q}_s\right\},$$

We can now follow the steps in the proof of Theorem 9 to write $\mathbf{X} = \mathbf{V}^{\mathcal{S}} + \tilde{\mathbf{X}}^{\mathcal{S}}$ where $\tilde{\mathbf{X}}^{\mathcal{S}}$ belongs to

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

whose minimum determinant can be bounded via Lemma 5 by

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

One can now remove the contribution of $\mathbf{V}^{\mathcal{S}}$ from the received signal and bound the minimum determinant as

$$\begin{aligned} \delta(\mathcal{C}_{\mathcal{S}}) &\geq N(\mathfrak{I})N(\Pi_{s\in\mathcal{S}}\mathfrak{q}_s) \\ &= N(\mathfrak{I})\Pi_{s\in\mathcal{S}}N(\mathfrak{q}_s) = N(\mathfrak{I})\Pi_{s\in\mathcal{S}}q_s. \end{aligned} \tag{18}$$

When no side information is available, we can again use Lemma 5 to bound the minimum determinant as

$$N(\mathfrak{I}) \leq \delta(\mathcal{C}) \leq \min_{x\in\mathfrak{I}} N_{\mathbb{L}/\mathbb{Q}}(x). \tag{19}$$

Combining (17), (18), and (19) results in

$$\begin{aligned} \Gamma(\mathcal{C},\mathcal{S}) &\geq \frac{10\log_{10}\left(N(\Pi_{s\in\mathcal{S}}\mathfrak{q}_s)\frac{N(\mathfrak{I})}{\min_{x\in\mathfrak{I}}N_{\mathbb{L}/\mathbb{Q}}(x)}\right)}{n\frac{1}{2n}\sum_{s\in\mathcal{S}}\log_2(p_s)} \\ &= \frac{\sum_{s\in\mathcal{S}}20\log_{10}(q_s)}{\sum_{s\in\mathcal{S}}\log_2(q_s)} + \frac{20\log_{10}\left(\frac{N(\mathfrak{I})}{min_{x\in\mathfrak{I}}N_{\mathbb{L}/\mathbb{Q}}(x)}\right)}{\sum_{s\in\mathcal{S}}\log_2(p_s)} \\ &= 6 + \gamma_{\mathfrak{I},\mathcal{S}} \text{ dB/bits per real symbol.} \end{aligned}$$

Noting that $\gamma_{\mathfrak{I},\mathcal{S}} \leq 0$ from (19) and $\gamma_{\mathfrak{I},\mathcal{S}} \geq \gamma_{\mathfrak{I}}$ completes the proof. □

V. Layered Golden-Coded Index Coding

In this section, we propose layered Golden-coded index coding, a family of LSTIC constructed from Golden code. To provide a concrete illustration of how the proposed scheme works, we will walk through this example in detail. Before proceeding, we note that the layered Golden-coded index coding proposed here is different, in essence, from the Golden-coded index coding in [18]. Here, we partition the code layer by layer while in [18] we directly tackle the Golden algebra. We would like to emphasize that neither of these two schemes subsumes the other as a special case; however, the approach taken in [18] only works for some particular primes.

Let $\mathbb{L} = \mathbb{Q}(\mathsf{i},\sqrt{5})$ a quadratic extension of $\mathbb{K} = \mathbb{Q}(\mathsf{i})$ and consider the non-trivial $\mathbb{Q}(\mathsf{i})$-automorphism $\sigma : \sqrt{5} \to -\sqrt{5}$. Also, let $\gamma = \mathsf{i}$. The Golden code is built from the Golden algebra given by

$$\mathcal{G} = (\mathbb{Q}(\mathsf{i},\sqrt{5})/\mathbb{Q}(i),\sigma,\mathsf{i}) = \left\{x_0 + x_1\mathsf{e} | x_0, x_1 \in \mathbb{Q}(i,\sqrt{5})\right\},$$

where $\mathsf{e}^2 = \mathsf{i}$ and $z\mathsf{e} = \mathsf{e}\sigma(z)$. The ring of integers of $\mathbb{L}$ is $\mathfrak{O}_{\mathbb{L}} = \mathbb{Z}[\mathrm{i}][\theta]$ where $\theta = \frac{1+\sqrt{5}}{2}$. Let $\mathfrak{I} = \alpha\mathfrak{O}_{\mathbb{L}}$ be the principal ideal generated by $\alpha = 1 + \mathsf{i}\bar{\theta}$ where $\bar{\theta} \triangleq \sigma(\theta)$. The Golden code [25] corresponds to

$$\mathcal{G}_{\mathfrak{I}} = \{x_0 + x_1\mathsf{e} | x_0, x_1 \in \alpha\mathfrak{O}_{\mathbb{L}}\},$$

which can be put into the matrix form

$$\begin{aligned} \mathcal{C}_{\mathfrak{I}} &= \left\{ \frac{1}{\sqrt{5}} \begin{pmatrix} \alpha x_0 & \alpha x_1 \\ i\sigma(\alpha x_1) & \sigma(\alpha x_0) \end{pmatrix} \middle| x_0, x_1 \in \mathbb{Z}[i][\theta] \right\} \\ &= \left\{ \frac{1}{\sqrt{5}} \begin{pmatrix} \alpha(a+b\theta) & \alpha(c+d\theta) \\ i\sigma(\alpha)(c+d\bar{\theta}) & \sigma(\alpha)(a+b\bar{\theta}) \end{pmatrix} \middle| a,b,c,d \in \mathbb{Z}[\mathsf{i}] \right\}. \end{aligned}$$

The proposed layered Golden-coded index coding can be categorized into the class in Section IV-A. Let $\mathfrak{q}_1,\mathfrak{q}_2,\dots,\mathfrak{q}_K$ be prime ideals in $\mathfrak{O}_{\mathbb{L}}$ that are relatively prime. Let $\mathfrak{q}_1\dots\mathfrak{q}_K \triangleq \mathfrak{q}$. Also, let $|\mathfrak{O}_{\mathbb{K}}/\mathfrak{q}_k| = N(\mathfrak{q}_k) \triangleq q_k$ for $k \in \{1,\dots,K\}$ where q_ks are not necessarily primes. From CRT, we have

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

where $\mathbb{B}_{q_k} = \mathfrak{O}_{\mathbb{K}}/\mathfrak{q}_k$ is a commutative ring with size q_k. This guarantees the existence of $\mathcal{M} : \mathbb{B}_{q_1} \times \ldots \times \mathbb{B}_{q_K} \to \mathfrak{O}_{\mathbb{L}}/\mathfrak{q}$ an isomorphism that maps the messages to a complete set of coset leaders of $\mathfrak{O}_{\mathbb{L}}/\mathfrak{q}$ with minimum energy. In the proposed layered Golden-coded index coding scheme, we let $w_k \in \mathbb{B}_{q_k}^2$ and split it into $w_{k,0}, w_{k,1} \in \mathbb{B}_{q_k}$.

The sub-messages $w_{1,\ell},\ldots,w_{K,\ell}$, for $\ell \in \{0,1\}$, are encoded onto $\mathfrak{O}_{\mathbb{L}}/\mathfrak{q}$ via $\mathcal{M}$ to form

$$x_\ell = \mathcal{M}(w_{1,\ell},\ldots,w_{K,\ell}) \in \mathfrak{O}_{\mathbb{L}}/\mathfrak{q}, \quad \ell \in \{0,1\}. \tag{20}$$

The overall codebook becomes a Golden code

$$\mathcal{C} = \left\{ \frac{1}{\sqrt{5}} \begin{pmatrix} \alpha x_0 & \alpha x_1 \\ i\sigma(\alpha x_1) & \sigma(\alpha x_0) \end{pmatrix} \middle| \, x_0, x_1 \in \mathfrak{O}_{\mathbb{L}}/\mathfrak{q} \right\}. \tag{21}$$

From Theorem 9, we obtain the following corollary. Note that the proof of this corollary is almost identical to that of Theorem 9. However, as mentioned earlier, in order to provide a complete illustration, we still present the proof.

Corollary 11: For any $\mathcal{S} \subset \{1,\ldots,K\}$, the proposed layered Golden-coded index coding provides $\Gamma(\mathcal{C},\mathcal{S}) = 6$ dB/bits per real symbol.

Proof: The rate of the message w_k is given by

$$R_k = \frac{1}{8}\log_2(N(\mathfrak{q}_k)^2) \quad \text{bits per real symbol.} \tag{22}$$

Suppose some messages $w_{\mathcal{S}} \triangleq \{w_k = v_k | k \in \mathcal{S}\}$ are known; this means that both $w_{\mathcal{S},\ell} \triangleq \{w_{k,\ell} = v_{k,\ell} | k \in \mathcal{S}\}$ for $\ell = 0$ and $\ell = 1$ are known. Therefore, from Section IV-A, x_ℓ, $\ell \in \{0,1\}$, belongs to a shifted version of $\Pi_{k\in\mathcal{S}}\mathfrak{q}_k$. Thus, after revealing $w_{\mathcal{S}}$, the code $\mathcal{C}_{\mathcal{S}}$ becomes a shifted version of

$$\left\{ \frac{1}{\sqrt{5}} \begin{pmatrix} \alpha x_0 & \alpha x_1 \\ i\sigma(\alpha x_1) & \sigma(\alpha x_0) \end{pmatrix} \middle| \, x_0, x_1 \in \Pi_{k\in\mathcal{S}}\mathfrak{q}_k \right\}.$$

For every codeword $\tilde{\mathbf{X}}^{\mathcal{S}} \in \mathcal{C}_{\mathcal{S}}$ corresponding to $x_0, x_1 \in \Pi_{k\in\mathcal{S}}\mathfrak{q}_k$, the determinant is given by

$$\begin{aligned} \det(\tilde{\mathbf{X}}^{\mathcal{S}}) &= \frac{1}{5}\det\begin{pmatrix} \alpha x_0 & \alpha x_1 \\ i\sigma(\alpha x_1) & \sigma(\alpha x_0) \end{pmatrix} \\ &\overset{(a)}{=} \frac{1}{5}\det\begin{pmatrix} \alpha x_0 & \alpha x_1 \\ i\sigma(\alpha)\sigma(x_1) & \sigma(\alpha)\sigma(x_0)) \end{pmatrix} \\ &= \frac{1}{5}\det\begin{pmatrix} \alpha & 0 \\ 0 & \sigma(\alpha) \end{pmatrix}\det\begin{pmatrix} x_0 & x_1 \\ i\sigma(x_1) & \sigma(x_0) \end{pmatrix} \\ &= \frac{1}{5}N_{\mathrm{rd}}(\alpha)\det\begin{pmatrix} x_0 & x_1 \\ i\sigma(x_1) & \sigma(x_0) \end{pmatrix}, \end{aligned}$$

where (a) is due to that σ is a homomorphism. Now, plugging $|N_{\mathrm{rd}}(\alpha)|^2 = 5$ results in

$$\begin{aligned} \delta(\mathcal{C}_{\mathcal{S}}) &= \frac{1}{5}\left|\det\begin{pmatrix} x_0 & x_1 \\ i\sigma(x_1) & \sigma(x_0) \end{pmatrix}\right|^2 \\ &\overset{(a)}{=} \frac{1}{5}N(\Pi_{k\in\mathcal{S}}\mathfrak{q}_k) \overset{(b)}{=} \frac{1}{5}\Pi_{k\in\mathcal{S}}N(\mathfrak{q}_k), \end{aligned} \tag{23}$$

where (a) follows from [26, Corollary 3] and the fact that $\mathfrak{O}_{\mathbb{L}} = \mathbb{Z}[\mathrm{i}][\theta]$ is a principal ideal domain and (b) follows from the fact that algebraic norm is multiplicative. Now, combining what we have obtained in (22) and (23) and the fact that $\delta(\mathcal{C}) = 1/5$ result in

$$\Gamma(\mathcal{C},\mathcal{S}) = \frac{10\log_{10}(\Pi_{k\in\mathcal{S}}N(\mathfrak{q}_k))}{2\frac{1}{4}\sum_{k\in\mathcal{S}}\log_2\ N(\mathfrak{q}_k)} = 6 \text{ dB/bits per real symbol.}$$

□

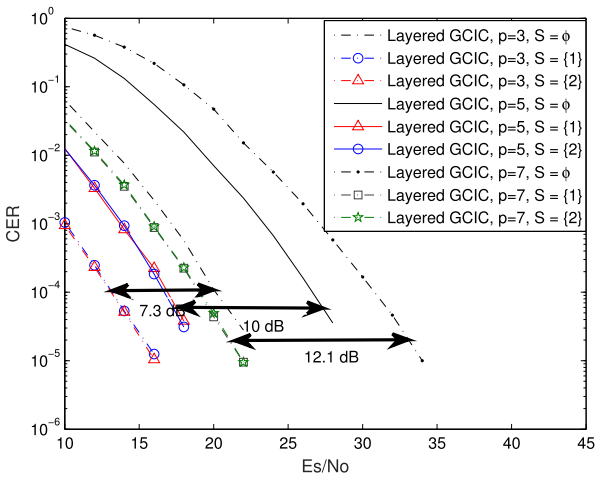

Fig. 2. CER performance for the proposed layered Golden-coded index coding. The curves with $\mathcal{S} = \emptyset$ correspond to the overall codes.

A. Examples and Simulation Results

In Table I, we factorize each prime $p < 100$ into prime ideals in $\mathfrak{O}_{\mathbb{L}}$ via Magma [36]. Any pair of ideals in this table is relatively prime and thus $\mathfrak{q}_k$ can be chosen as product of some prime ideals that have not been selected for some $\mathfrak{q}_{k'}$, $k' \neq k$. In Table I, we show ideals and their inertial degrees f. The ramification index of each prime ideal lying above $p \neq 2,5$ is 1 and is 2 for prime ideals lying above $2,5$. This can be seen by observing that

$$d_{\mathbb{L}} = 5^2 \cdot 4^2,$$

which has prime factors 2 and 5. Moreover, since $\mathfrak{O}_{\mathbb{L}}$ is a principal ideal domain, so every $p\mathfrak{O}_{\mathbb{L}}$ can be factorized into principal prime ideals.

Simulation results for the proposed layered Golden-coded index coding are provided in Fig. 2. In this figure, three sets of simulations are performed. In the first one, we constructed the layered Golden-coded index coding with two principal ideals generated by $\beta_1 = (\bar{\theta} - i\theta)$ and $\beta_2 = (\bar{\theta} + \mathrm{i}\theta)$, respectively. From Table I, we see that each of these ideals corresponds to $p = 3$ and has inertial degree 2; thus, it has norm equal to $3^2 = 9$. Thus, each message $w_k \in \mathbb{B}_9^2$, which is then split into sub-messages $w_{k,1}, w_{k,2} \in \mathbb{B}_9$. The sub-messages $w_{1,\ell}$ and $w_{2,\ell}$ are then encoded into x_ℓ via (20), which is then put into the matrix form in (21). Moreover, from Table I, we know that $3\mathfrak{O}_{\mathbb{L}} = \beta_1\beta_2\mathfrak{O}_{\mathbb{L}}$. Therefore, the overall codebook corresponds to (21) with $x_0, x_1 \in \mathfrak{O}_{\mathbb{L}}/3\mathfrak{O}_{\mathbb{L}}$. 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 that when reveal either message, we expect to achieve SNR gain

$$\frac{1}{4}10\log_{10}\left(\frac{118}{10}\right) + \frac{1}{2}10\log_{10}(9) \approx 7.45 \text{ dB},$$

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

TABLE I

PRIME FACTORIZATION OF $p < 100$ IN $\mathbb{Z}[i][\theta]$ WHERE $\theta = \frac{1+\sqrt{5}}{2}$

p	$\mathfrak{p}$	f
2	$(1+\mathsf{i})$	2
3	$(\bar{\theta} - i\theta), (\bar{\theta} + \mathsf{i}\theta)$	2
5	$(1+\mathsf{i}\bar{\theta}), (1-\mathsf{i}\bar{\theta})$	1
7	$((1+\theta)+\mathsf{i}(1+\bar{\theta})), ((1+\theta)-\mathsf{i}(1+\bar{\theta}))$	2
11	$(3\mathsf{i}\theta - \mathsf{i}), (3\mathsf{i}\bar{\theta} - \mathsf{i})$	2
13	$(2+3\mathsf{i}), (2-3\mathsf{i})$	2
17	$(4+\mathsf{i}), (4-\mathsf{i})$	2
19	$(4\mathsf{i}\theta - i), (4\mathsf{i}\bar{\theta} - \mathsf{i})$	2
23	$((3\bar{\theta}-1)+\mathsf{i}(3\theta-1)), ((3\bar{\theta}-1)-\mathsf{i}(3\theta-1))$	2
29	$(2\mathsf{i}+\theta), (2\mathsf{i}+\bar{\theta}), (\bar{\theta}-2\mathsf{i}), (\theta-2\mathsf{i})$	1
31	$(2-5\bar{\theta}), (2-5\theta)$	2
37	$(6+\mathsf{i}), (6-\mathsf{i})$	2
41	$(\bar{\theta}+\mathsf{i}(2\theta-1)), (\bar{\theta}-\mathsf{i}(2\theta-1)), (\theta-\mathsf{i}(2\theta-1)), (\theta+\mathsf{i}(2\theta-1))$	1
43	$((4+\theta)+\mathsf{i}(4+\bar{\theta})), ((4+\bar{\theta})+\mathsf{i}(4+\theta))$	2
47	$((2+3\theta)-\mathsf{i}(2+3\bar{\theta})), ((2+3\bar{\theta})-\mathsf{i}(2+3\theta))$	2
53	$(7+2\mathsf{i}), (7-2\mathsf{i})$	2
59	$(7\theta-2), (7\bar{\theta}-2)$	2
61	$((2\bar{\theta}-1)+\mathsf{i}(\theta+1)), ((2\theta-1)+\mathsf{i}(\bar{\theta}+1)), ((2\theta-1)+\mathsf{i}(\theta+1)), ((2\bar{\theta}-1)+\mathsf{i}(\bar{\theta}+1))$	1
67	$((5\bar{\theta}-1)+\mathsf{i}(5\theta-1)), ((5\theta-1)+\mathsf{i}(5\bar{\theta}-1))$	2
71	$(8+\theta), (8+\bar{\theta})$	2
73	$(3+8\mathsf{i}), (3-8\mathsf{i})$	2
79	$(8\theta-3), (8\bar{\theta}-3)$	2
83	$((4+3\theta)+\mathsf{i}(4+3\bar{\theta})), ((4+3\bar{\theta})+\mathsf{i}(4+3\theta))$	2
89	$(2\bar{\theta}-\mathsf{i}(\theta+1)), (2\theta-\mathsf{i}(\bar{\theta}+1)), (2\bar{\theta}+\mathsf{i}(\theta+1)), (2\bar{\theta}+\mathsf{i}(\bar{\theta}+1))$	1
97	$(9+4\mathsf{i}), (9-4\mathsf{i})$	2

$\beta_2 = (1-\mathsf{i}\bar{\theta})^2$, respectively. From Table I, we see that $(1+\mathsf{i}\bar{\theta})$ and $(1-\mathsf{i}\bar{\theta})$ are both corresponding to $p=5$ with inertial degree 1; thus, $\beta_1\mathfrak{O}_{\mathbb{L}}$ 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 (21) with $x_0, x_1 \in \mathfrak{O}_{\mathbb{L}}/5\mathfrak{O}_{\mathbb{L}}$. 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

$$\frac{1}{4}10\log_{10}\left(\frac{656}{32}\right) + \frac{1}{2}10\log_{10}(25) \approx 10.27 \text{ dB},$$

where 656 and 32 inside the first logarithm are $N_{\mathcal{C}}$ and $N_{\mathcal{C}_{\mathcal{S}}}$, respectively and the 25 inside the second logarithm is the ratio of $\delta(\mathcal{C}_{\mathcal{S}})$ and $\delta(\mathcal{C})$. In the last set of simulations, the two prime ideals corresponding to $p=7$ 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

$$\frac{1}{4}10\log_{10}\left(\frac{2042}{41}\right) + \frac{1}{2}10\log_{10}(49) \approx 12.69 \text{ dB},$$

where 2042 and 41 inside the first logarithm are $N_{\mathcal{C}}$ and $N_{\mathcal{C}_{\mathcal{S}}}$, respectively and the 49 inside the second logarithm is the ratio of $\delta(\mathcal{C}_{\mathcal{S}})$ and $\delta(\mathcal{C})$.

Remark 12: We end this section by showing that the proposed layered Golden-coded index coding is not a special case of the Golden-coded index coding in [18] and vice versa. The Golden-coded index coding in [18] is constructed over $\mathbb{Z}[\mathsf{e}][\theta]$ with ideals of the form $(\alpha+\beta\mathsf{e})\mathbb{Z}[\mathsf{e}][\theta]$ where $\alpha, \beta \in \mathbb{Z}[\mathrm{i}]$. Consider $p=17$ for which [18, Example 6] indicates that $17\mathbb{Z}[\mathsf{e}][\theta]$ can be partitioned into 4 ideals, each with norm 17^2. So the Golden-coded index coding can take messages of size 17^2. To do the same for our layered scheme, it requires an ideal in $\mathbb{Z}[\mathrm{i}][\theta]$ to have norm 17, which is impossible from the result in Table I. Now, let us consider $p=29$ where Table I shows that $29\mathbb{Z}[\mathrm{i}][\theta]$ can be partitioned into four ideals, each with norm 29. Hence, the proposed layered Golden-coded index coding can take messages of size 29^2. This will require $29\mathbb{Z}[\mathsf{e}][\theta]$ to be partitioned into ideals of the form $\alpha+\beta\mathsf{e}$ with norm 29^2. However, using Magma, we obtain that $29\mathbb{Z}[\mathsf{e}][\theta] = \mathfrak{I}_1\mathfrak{I}_2\mathfrak{I}_3\mathfrak{I}_4$ with $\mathfrak{I}_1 = (\bar{\theta}+2\mathrm{i})\mathbb{Z}[\mathsf{e}][\theta]$, $\mathfrak{I}_2 = (\bar{\theta}-2\mathrm{i})\mathbb{Z}[\mathsf{e}][\theta]$, $\mathfrak{I}_3 = (\theta+2\mathrm{i})\mathbb{Z}[\mathsf{e}][\theta]$, and $\mathfrak{I}_4 = (\theta-2\mathrm{i})\mathbb{Z}[\mathsf{e}][\theta]$, where none of these satisfies the form required by the Golden-coded index coding.

VI. LSTIC BASED ON 3×3 PERFECT STBC

Let ζ_7 be the 7th root of unity and let $\theta \triangleq \zeta_7 + \zeta_7^{-1} = 2\cos\left(\frac{2\pi}{7}\right)$. Also, let $\mathbb{K} = \mathbb{Q}(\omega)$ and let $\mathbb{L} = \mathbb{Q}(\omega, \theta)$ the field extension of $\mathbb{K}$ with $[\mathbb{L}:\mathbb{K}] = 3$. Consider the cyclic division algebra

$$\mathcal{A} = (\mathbb{L}/\mathbb{K}, \sigma, \gamma) = \{x_0 + x_1\mathsf{e} + x_2\mathsf{e}^2 | x_0, \ldots, x_2 \in \mathbb{L}\},$$

where $\sigma : \zeta_7 + \zeta_7^{-1} \to \zeta_7^2 + \zeta_7^{-2}$ and $\mathsf{e}^3 = \gamma \triangleq j$. A 3×3 perfect STBC is constructed from

$$\bar{\mathcal{A}}_{\mathfrak{I}} = \{\alpha x_0 + \alpha x_1\mathsf{e} + \alpha x_2\mathsf{e}^2 | x_0, \ldots, x_2 \in \mathfrak{O}_{\mathbb{L}}\},$$

where $\alpha = 1+\omega+\theta$. The code will have the matrix form shown in (8).

One can now follow Section IV-A to construct LSTIC based on 3×3 perfect STBC. As a result, we have the following corollary whose proof is identical to that of Theorem 9 together with the fact that $\mathfrak{O}_{\mathbb{L}} = \mathbb{Z}[\omega][\theta]$ is a principal ideal domain.

TABLE II

PRIME FACTORIZATION OF $p < 100$ IN $\mathbb{Z}[\omega][\theta]$ WHERE $\theta = \zeta_7 + \zeta_7^{-1}$

p	$\mathfrak{p}$	f
2	(2)	6
3	$(1+\omega)$	3
5	(5)	6
7	$((\omega-1)\theta^2+(\omega-1)\theta-\omega+2), ((-\omega+1)\theta^2-(\omega-1)\theta+2\omega-1)$	1
11	(11)	6
13	$(\omega\theta^2+(\omega-1)\theta-\omega-1), ((\omega-1)\theta^2-\theta-\omega+1), (-\theta^2-\omega\theta+2)$ $(\omega\theta^2+\theta-2\omega+1), (-\omega\theta^2-\theta+\omega), (\omega\theta^2+\theta-2\omega)$	1
17	(17)	6
19	$(3-5\omega), (3\omega-5)$	3
23	(23)	6
29	$((2\omega-2)\theta^2-(\omega-1)\theta-4\omega+4), (3\omega\theta^2+2\omega\theta-4\omega), (3\omega\theta^2+\omega\theta-4\omega)$	2
31	$(\omega+5), (5\omega+1)$	3
37	$(7\omega-4), (3\omega+4)$	3
41	$((\omega-1)\theta^2-(2\omega-2)\theta-4\omega+4), (3\theta^2+\theta-3), ((2-2\omega)\theta^2-(3\omega-3)\theta+4\omega-4)$	2
43	$((\omega-1)\theta^2+\theta-2\omega+2), (\theta^2+(-\omega+2)\theta-1), ((\omega+1)\theta^2+\theta-2\omega-1)$ $(\theta^2+(\omega-1)\theta-2), (-\theta^2+(-\omega-1)\theta+1), ((-\omega+2)\theta^2+\theta+2\omega-3)$	1
47	(47)	6
53	(53)	6
59	(59)	6
61	$(5\omega+4), (4\omega+5)$	3
67	$(7-9\omega), (7\omega-9)$	3
71	$(\theta^2+\theta+3), (4\theta^2+3\theta-5), ((\omega-1)\theta^2-6\omega+6)$	2
73	$(8\omega-9), (9-\omega)$	3
79	$(7\omega+3), (3\omega+7))$	3
83	$(2\theta^2-2\theta-5), (4\theta^2+2\theta-5), (2\omega\theta^2+4j\theta-3\omega)$	2
89	(89)	6
97	$(-\theta^2-\theta-2\omega+3), (\theta^2-2\omega), (\theta-2\omega+2)$ $(-\theta^2-\theta+2\omega+1), (\theta^2+2\omega-2), (\theta+2\omega)$	1

Corollary 13: For any $\mathcal{S} \subset \{1,\ldots,K\}$, the proposed LSTIC based on 3×3 perfect STBC provides $\Gamma(\mathcal{C},\mathcal{S}) = 6$ dB/bits per real symbol.

A. Examples and Simulation Results

Here, we again factorize each prime $p < 100$ into prime ideals via Magma. We show ideals and their inertial degrees f. The ramification index of each prime ideal lying above p is given by

$$e = \begin{cases} 2, & p = 3; \\ 3, & p = 7; \\ 1, & \text{otherwise.} \end{cases}$$

This can be justified by observing that

$$d_{\mathbb{L}} = 3^3 7^4,$$

which has prime factors 3 and 7. Again, since $\mathfrak{O}_{\mathbb{L}}$ is a principal ideal domain, every $p\mathfrak{O}_{\mathbb{L}}$ can be factorized into principal prime ideals as shown in Table II.

Simulation results for the 3×3 case are presented in Fig. 3 where we construct LSTIC from the 3×3 perfect STBC with two principal ideals generated by $\beta_1 = ((\omega-1)\theta^2+(\omega-1)\theta-\omega+2)$ and $\beta_2 = ((-\omega+1)\theta^2-(\omega-1)\theta+2\omega-1)$. From Table II, we learn that both β_1 and β_2 correspond to $p=7$ and we have $\beta_1\beta_2\mathfrak{O}_{\mathbb{L}} = 7\mathfrak{O}_{\mathbb{L}}$. Hence, the overall codebook corresponds to (8) with $x_0, x_1, x_2 \in \mathfrak{O}_{\mathbb{L}}/3\mathfrak{O}_{\mathbb{L}}$. Fig. 3 indicates that by revealing either of the message to the receiver, one obtains a roughly 10.5 dB SNR reduction. On the other hand, our analysis shows that the SNR reduction one can expect is roughly

$$\frac{1}{9}10\log_{10}\left(\frac{5.9\times 10^{10}}{652428}\right) + \frac{1}{3}10\log_{10}(343) \approx 13.95 \text{ dB},$$

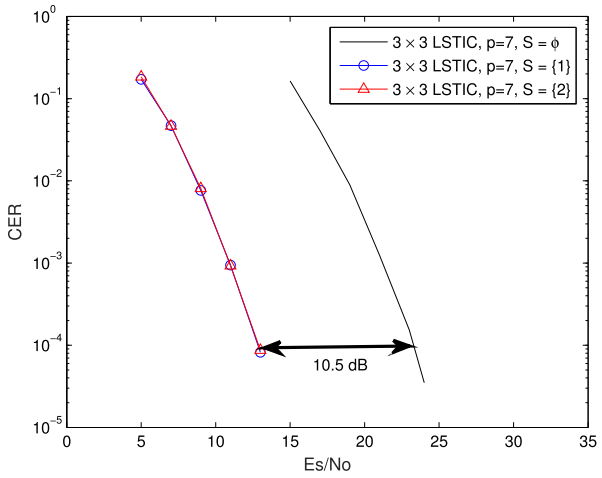

Fig. 3. CER performance for the proposed LSTIC constructed from 3×3 STBC. The curve with $\mathcal{S} = \emptyset$ corresponds to the overall code.

where the parameters inside the first and second logarithms are corresponding to gains in $N_{\mathcal{C}}$ and $\delta(\mathcal{C})$, respectively. The difference between the simulation results and our analysis is largely due to the fact that the SNR gain is measured at 10^{-4} CER, which is far from the asymptotic regime for a 3×3 STBC. This is evident by observing that the CER curves have not even exhibited the promised diversity order of 9.

VII. LSTIC BASED ON 4×4 PERFECT STBC

Let ζ_{15} be the 15th root of unity and let $\theta \triangleq \zeta_{15} + \zeta_{15}^{-1} = 2\cos\left(\frac{2\pi}{15}\right)$. Also, let $\mathbb{K} = \mathbb{Q}(\mathrm{i})$ and let $\mathbb{L} = \mathbb{Q}(\mathrm{i},\theta)$ the field extension of $\mathbb{K}$ with $[\mathbb{L}:\mathbb{K}] = 4$. Consider the cyclic division

algebra

$$\mathcal{A}=(\mathbb{L}/\mathbb{K},\sigma,\gamma)=\{x_0+x_1\mathsf{e}+x_2\mathsf{e}^2+x_3\mathsf{e}^3|x_0,\ldots,x_3\in\mathbb{L}\},$$

where $\sigma:\zeta_{15}+\zeta_{15}^{-1}\rightarrow\zeta_{15}^{2}+\zeta_{15}^{-2}$ and $\mathsf{e}^4=\gamma\triangleq i$. A 4×4 perfect STBC is constructed from

$$\bar{\mathcal{A}}_{\mathfrak{I}}=\{\alpha x_0+\alpha x_1\mathsf{e}+\alpha x_2\mathsf{e}^2+\alpha x_3\mathsf{e}^3|x_0,\ldots,x_3\in\mathfrak{O}_{\mathbb{L}}\},$$

where $\alpha=(1-3\mathsf{i})+\mathsf{i}\theta^2$. The code will have the matrix form shown in (8).

One can now follow Section IV-A to construct LSTIC based on 4×4 perfect STBC. As a result, we have the following corollary.

Corollary 14: For any $\mathcal{S}\subset\{1,\ldots,K\}$, the proposed LSTIC based on 4×4 perfect STBC provides $\Gamma(\mathcal{C},\mathcal{S})\geq6$ 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.

A. Examples and Simulation Results

Here, we factorize each prime $p<100$ into prime ideals via Magma. In Table III, we show ideals and their inertial degrees f. The ramification index of each prime ideal lying above p is given by

$$e=\begin{cases}2, & p=2,3;\\ 4, & p=5;\\ 1, & \text{otherwise.}\end{cases}$$

This can be justified by observing that

$$d_{\mathbb{L}}=2^8 3^4 5^6,$$

which has prime factors 2, 3, and 5. Also, note that in this case, $p=3,5,29,89$ are factorized into non-principal prime ideals.

In Fig. 4, two sets of simulation results are presented. Let us consider ideals $\mathfrak{I}_1=(3,(5\mathsf{i}+2)\theta^3+7\mathsf{i}\theta^2+(4\mathsf{i}+4)\theta+7\mathsf{i}+7)$ and $\mathfrak{I}_2=(3,2\theta^3+2\mathsf{i}\theta^2+(7\mathsf{i}+5)\theta+8\mathsf{i}+6)$. From Table III and the ramification index of 3, we learn that $3\mathfrak{O}_{\mathbb{L}}=\mathfrak{I}_1^2\mathfrak{I}_2^2$ where $N(\mathfrak{I}_1^2)=N(\mathfrak{I}_2^2)=81$. Moreover, with some computation, we have that $\mathfrak{I}_1^2$ and $\mathfrak{I}_2^2$ are principal ideals with generators $\beta_1=(\mathsf{i}+1)\theta^3-3(\mathsf{i}+1)\theta+1$ and $\beta_2=(\mathsf{i}-1)\theta^3-3(\mathsf{i}-1)\theta-1$, respectively. In the first set, we construct LSTIC from 4×4 perfect STBC with two principal ideals corresponding to $p=3$ generated by β_1 and β_2, respectively. Each message consists of four sub-messages from $\mathbb{Z}_{81}$ and the overall codebook corresponds to the one in (8) with $x_0,x_1,x_2,x_3\in\mathfrak{O}_{\mathbb{L}}/3\mathfrak{O}_{\mathbb{L}}$. Fig. 4 indicates a roughly 5.5 dB SNR gain by revealing either message to the receiver. We note that the analysis predicts a roughly

$$\frac{1}{16}10\log_{10}\left(\frac{4.89\times10^9}{9099}\right)+\frac{1}{4}10\log_{10}(81)\approx8.35\text{ dB},$$

where again the parameters inside the first and second logarithms are corresponding to gains in $N_{\mathcal{C}}$ and $\delta(\mathcal{C})$, respectively.

In the second set of simulations, we consider ideals $\mathfrak{I}_1=(5,(14\mathsf{i}+21)\theta^3+(10\mathsf{i}+1)\theta^2+(12\mathsf{i}+21)\theta+4\mathsf{i}+22)$ and $\mathfrak{I}_2=(5,(20\mathsf{i}+7)\theta^3+(6\mathsf{i}+9)\theta^2+(21\mathsf{i}+8)\theta+8\mathsf{i}+5)$ that correspond to $p=5$. Again from III and the ramification index of 5, we learn that $5\mathfrak{O}_{\mathbb{L}}=\mathfrak{I}_1^4\mathfrak{I}_2^4$ where $N(\mathfrak{I}_1^2)=N(\mathfrak{I}_2^2)=625$.

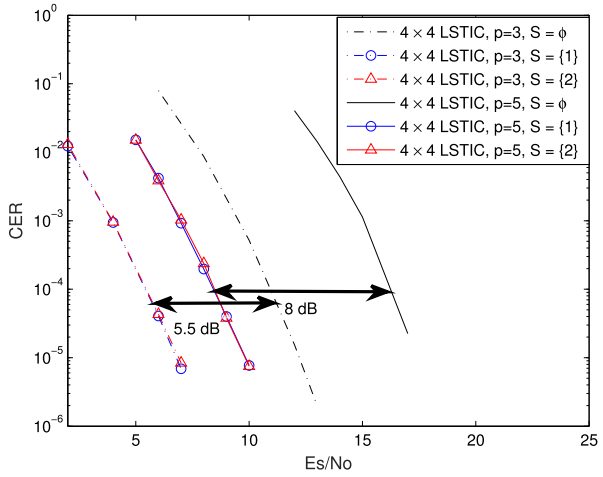

Fig. 4. CER performance for the proposed LSTIC constructed from 4×4 STBC. The curve with $\mathcal{S}=\emptyset$ corresponds to the overall code.

We have that $\mathfrak{I}_1^4$ and $\mathfrak{I}_2^4$ are principal ideals with generators $\beta_1=2\mathsf{i}-1$ and $\beta_2=2\mathsf{i}+1$, respectively. We again construct LSTIC from 4×4 perfect STBC with two principal ideals generated by β_1 and β_2, respectively. Simulation result in Fig. 4 shows a roughly 8 dB SNR gain obtained by revealing either message to the receiver. We again note that the analysis predicts a SNR gain of roughly

$$\frac{1}{16}10\log_{10}\left(\frac{4.65\times10^{14}}{2.18\times10^6}\right)+\frac{1}{4}10\log_{10}(625)\approx12.19\text{ dB}.$$

In both the cases, one observes that there is a difference between the simulation results and the analysis. This again can be explained by that the CER where we measure the side information gain is far from the asymptotic regime for a 4×4 STBC, which is again evident by observing that the CER curves have not exhibited the promised diversity order of 16.

VIII. LSTIC Based on 6×6 Perfect STBC

Let ζ_{28} be the 28th root of unity and let $\theta\triangleq\zeta_{28}+\zeta_{28}^{-1}=2\cos\left(\frac{\pi}{14}\right)$. Also, let $\mathbb{K}=\mathbb{Q}(\omega)$ and let $\mathbb{L}=\mathbb{Q}(\omega,\theta)$ the field extension of $\mathbb{K}$ with $[\mathbb{L}:\mathbb{K}]=6$. Consider the cyclic division algebra

$$\mathcal{A}=(\mathbb{L}/\mathbb{K},\sigma,\gamma)=\{x_0+x_1\mathsf{e}+\ldots+x_5\mathsf{e}^5|x_0,\ldots,x_5\in\mathbb{L}\},$$

where $\sigma:\zeta_{28}+\zeta_{28}^{-1}\rightarrow\zeta_{28}^{5}+\zeta_{28}^{-5}$ and $\mathsf{e}^6=\gamma\triangleq-\omega$. A 6×6 perfect STBC is constructed from

$$\bar{\mathcal{A}}_{\mathfrak{I}}=\{x_0+x_1\mathsf{e}+\ldots+x_5\mathsf{e}^5|x_0,\ldots,x_5\in\mathfrak{I}\},$$

where $\mathfrak{I}$ is such that $7\mathfrak{O}_{\mathbb{L}}=\mathfrak{I}^6\bar{\mathfrak{I}}^6$.

One can now follow Section IV-B to construct LSTIC based on 6×6 perfect STBC. As a result, we have the following corollary.

Corollary 15: For any $\mathcal{S}\subset\{1,\ldots,K\}$, the side information gain achieved by the proposed LSTIC based on 6×6 perfect STBC with non-principal ideal $\mathfrak{I}$ is lower bounded as

$$\Gamma(\mathcal{C},\mathcal{S})\geq6+\gamma_{\mathfrak{I}}\text{ dB/bits per real symbol},$$

where $\gamma_{\mathfrak{I}}$ is as shown in (16).

TABLE III

PRIME FACTORIZATION OF $p < 100$ IN $\mathbb{Z}[\mathsf{i}][\theta]$ WHERE $\theta = \zeta_{15} + \zeta_{15}^{-1}$. FOR $p = 29, 89$, WE ONLY LIST ONE OF THE EIGHT IDEALS DUE TO THE SPACE LIMITATION; THE OTHER SEVEN IDEALS CAN BE OBTAINED AS THE CONJUGATES

p	$\mathfrak{p}$	f
2	$(1+\mathsf{i})$	4
3	$(3, (5\mathsf{i}+2)\theta^3 + 7\mathsf{i}\theta^2 + (4\mathsf{i}+4)\theta + 7\mathsf{i} + 7), (3, 2\theta^3 + 2\mathsf{i}\theta^2 + (7\mathsf{i}+5)\theta + 8\mathsf{i} + 6)$	2
5	$(5, (14\mathsf{i}+21)\theta^3 + (10\mathsf{i}+1)\theta^2 + (12\mathsf{i}+21)\theta + 4\mathsf{i} + 22)$	1
	$(5, (20\mathsf{i}+7)\theta^3 + (6\mathsf{i}+9)\theta^2 + (21\mathsf{i}+8)\theta + 8\mathsf{i} + 5)$	
7	$((-\mathsf{i}+1)\theta^3 + (3\mathsf{i}-3)\theta - 2\mathsf{i} - 1), ((\mathsf{i}+1)\theta^3 - (3\mathsf{i}+3)\theta + 2\mathsf{i} - 1)$	4
11	$(2\mathsf{i}\theta^3 + \mathsf{i}\theta^2 - 6\mathsf{i}\theta - \mathsf{i} + 1), (\mathsf{i}\theta^3 - 2\mathsf{i}\theta + 1)$	2
	$((\mathsf{i}+1)\theta^3 + \mathsf{i}\theta^2 - (3\mathsf{i}+4)\theta - \mathsf{i}), (\theta^3 - \theta^2 - 3\theta - \mathsf{i} + 3)$	
13	$(2+3\mathsf{i}), (2-3\mathsf{i})$	4
17	$(4+\mathsf{i}), (4-\mathsf{i})$	4
19	$(\mathsf{i}\theta^3 - (4\mathsf{i}-1)\theta + \mathsf{i}), (\mathsf{i}\theta^3 - (1-\mathsf{i})\theta^2 - 3\mathsf{i}\theta - 2\mathsf{i} + 2)$	2
	$(\mathsf{i}\theta^3 + (\mathsf{i}+1)\theta^2 - 3\mathsf{i}\theta - 2\mathsf{i} - 2), (\mathsf{i}\theta^3 - (4\mathsf{i}+1)\theta + \mathsf{i})$	
23	$((3\mathsf{i}+3)\theta^3 - (9\mathsf{i}+9)\theta + 2\mathsf{i} + 1), ((3\mathsf{i}-3)\theta^3 - (9\mathsf{i}-9)\theta + 2\mathsf{i} - 1)$	4
29	$(29, (813\mathsf{i}+779)\theta^3 + (812\mathsf{i}+793)\theta^2 + (755\mathsf{i}+41)\theta + 814\mathsf{i} + 5)$	1
31	$(-2\mathsf{i}\theta^2 + 5\mathsf{i}), (2\mathsf{i}\theta^3 + 2\mathsf{i}\theta^2 - 6\mathsf{i}\theta - 3\mathsf{i}), (2\theta^3 - 8\theta + 1), (2\theta - 1)$	2
37	$(6+\mathsf{i}), (6-\mathsf{i})$	4
41	$((\mathsf{i}+2)\theta^3 - (3\mathsf{i}+6)\theta + \mathsf{i} + 1), ((2\mathsf{i}-1)\theta^3 + (3-6\mathsf{i})\theta + \mathsf{i})$	2
	$((2\mathsf{i}+1)\theta^3 - (6\mathsf{i}+3)\theta + \mathsf{i} + 1), ((2\mathsf{i}+1)\theta^3 - (6\mathsf{i}+3)\theta + \mathsf{i})$	
43	$((\mathsf{i}-1)\theta^3 - (3\mathsf{i}-3)\theta + 5\mathsf{i} + 4), ((\mathsf{i}+1)\theta^3 - (3\mathsf{i}+3)\theta + 5\mathsf{i} - 4)$	4
47	$((3\mathsf{i}+3)\theta^3 - (9\mathsf{i}+9)\theta + 5\mathsf{i} - 2), ((3\mathsf{i}-3)\theta^3 - (9\mathsf{i}-9)\theta + 5\mathsf{i} + 2)$	4
53	$(2+7\mathsf{i}), (2-7\mathsf{i})$	4
59	$(-2\theta^3 - \theta^2 + 7\theta - 1), (-\mathsf{i}\theta^3 - \mathsf{i}\theta^2 + 2\mathsf{i}\theta + 4\mathsf{i}), (-\mathsf{i}\theta^2 + \mathsf{i}\theta + 4\mathsf{i}), (-\theta^3 + \theta^2 + 4\theta - 1)$	2
61	$(\theta + \mathsf{i}), (\theta^3 - 4\theta + \mathsf{i} + 1), (-\theta^3 - \theta^2 + 3\theta + \mathsf{i} + 2), (\theta^2 + \mathsf{i} - 2)$	1
	$(\theta - \mathsf{i}), (\theta^3 - 4\theta - \mathsf{i} + 1), (-\theta^3 - \theta^2 + 3\theta - \mathsf{i} + 2), (\theta^2 - \mathsf{i} - 2)$	
67	$((5\mathsf{i}+5)\theta^3 - (15\mathsf{i}+15)\theta + 4\mathsf{i} + 1), ((5\mathsf{i}-5)\theta^3 - (15\mathsf{i}-15)\theta + 4\mathsf{i} - 1)$	4
71	$((3\mathsf{i}+1)\theta^3 + (\mathsf{i}+1)\theta^2 - (10\mathsf{i}+3)\theta - \mathsf{i}), ((\mathsf{i}-3)\theta^3 - 2\theta^2 + (9-4\mathsf{i})\theta + \mathsf{i} + 2)$	2
	$((\mathsf{i}+3)\theta^3 + 2\theta^2 - (4\mathsf{i}+9)\theta + \mathsf{i} - 2), ((3\mathsf{i}-1)\theta^3 + (\mathsf{i}-1)\theta^2 - (10\mathsf{i}-3)\theta - \mathsf{i})$	
73	$(3+8\mathsf{i}), (3-8\mathsf{i})$	4
79	$((2\mathsf{i}+1)\theta^3 - (7\mathsf{i}+2)\theta + \mathsf{i}), ((\mathsf{i}+2)\theta^3 - (\mathsf{i}-1)\theta^2 - (3\mathsf{i}+6)\theta + 3\mathsf{i} - 1)$	2
	$((\mathsf{i}-2)\theta^3 - (\mathsf{i}+1)\theta^2 - (3\mathsf{i}-6)\theta + 3\mathsf{i} + 1), ((1-2\mathsf{i})\theta^3 + (7\mathsf{i}-2)\theta - \mathsf{i})$	
83	$((3\mathsf{i}-3)\theta^3 - (9\mathsf{i}-9)\theta + 7\mathsf{i} + 4), ((3\mathsf{i}+3)\theta^3 - (9\mathsf{i}+9)\theta + 7\mathsf{i} - 4)$	4
89	$(89, (27\mathsf{i}+82)\theta^3 + (31\mathsf{i}+117)\theta^2 + (77\mathsf{i}+7669)\theta + 7896\mathsf{i} + 7771)$	1
97	$(9+4\mathsf{i}), (9-4\mathsf{i})$	4

In Table IV, we again factorize each prime $p < 100$ into prime ideals via Magma. We show ideals and their inertial degrees f. The ramification index of each prime ideal lying above p is given by

$$e = \begin{cases} 2, & p = 2, 3; \\ 6, & p = 7; \\ 1, & \text{otherwise.} \end{cases}$$

This can be justified by observing that

$$d_{\mathbb{L}} = 2^{12}3^6 7^{10},$$

which has prime factors 2, 3, and 7. In this case, for $p < 100$, we note that $p = 3, 7, 19, 31$ are factorized into non-principal prime ideals.

IX. LAYERED ALAMOUTI-CODED INDEX CODING

In this section, we construct space-time index codes for 2×1 MISO channel from Alamouti code [23]. Alamouti code can be regarded as codes constructed over Hamilton quaternions [37], the $\mathbb{R}$-algebra of dimension 4 given by

$$\mathbb{H} = \{a + b\mathsf{i} + c\mathsf{j} + d\mathsf{k} | a, b, c, d \in \mathbb{R}\},$$

where $\mathsf{i}^2 = -1$, $\mathsf{j}^2 = -1$, $\mathsf{k}^2 = -1$, and $\mathsf{k} = \mathsf{ij} = -\mathsf{ji}$. We note that $\mathbb{H}$ is a cyclic division algebra

$$\mathbb{H} = (\mathbb{Q}(\mathsf{i})/\mathbb{Q}, \sigma, -1) = \{x_0 + \mathsf{j}x_1 | x_0, x_1 \in \mathbb{Q}(i)\},$$

where $\sigma : \mathsf{i} \to -\mathsf{i}$ and $\lambda\mathsf{j} = \mathsf{j}\sigma(\lambda)$. This induces a layered structure of the Alamouti code. Now, consider $\tilde{\mathbb{H}} = \{x_0 + \mathsf{j}x_1 | x_0, x_1 \in \mathbb{Z}[\mathsf{i}]\}$, an Alamouti code corresponds to a finite subset of

$$\mathcal{C}_{\mathbb{Z}[\mathsf{i}]} \triangleq \left\{ \begin{pmatrix} x_0 & -x_1^* \\ x_1 & x_0^* \end{pmatrix} \middle| x_0, x_1 \in \mathbb{Z}[\mathsf{i}] \right\}.$$

Thus, Alamouti code does not belong to the family of codes considered in Section IV (which have base fields $\mathbb{K} = \mathbb{Q}(\mathsf{i})$ or $\mathbb{Q}(\mathsf{j})$). Fortunately, one can follow the same approach and obtain Alamouti-coded index coding as follows.

Note that $\mathbb{Z}[\mathsf{i}]$ is a principal ideal domain; so every ideal can be generated by a singleton. Let $\phi_1, \ldots, \phi_K$ be K elements in $\mathbb{Z}[\mathsf{i}]$ that are relatively prime. Also, define $q = \Pi_{k=1}^K \phi_k$ and define $N(\phi_k) = q_k$ for $k \in \{1, \ldots, K\}$ where q_ks are not necessarily primes. From CRT, we have

$$\mathbb{Z}[\mathsf{i}]/q\mathbb{Z}[\mathsf{i}] \cong \mathbb{Z}[\mathsf{i}]/\phi_1\mathbb{Z}[\mathsf{i}] \times \ldots \times \mathbb{Z}[\mathsf{i}]/\phi_K\mathbb{Z}[\mathsf{i}] \cong \mathbb{B}_{q_1} \times \ldots \times \mathbb{B}_{q_K},$$

where $\mathbb{B}_{q_k} = \mathbb{Z}[\mathsf{i}]/\phi_k\mathbb{Z}[\mathsf{i}]$ is a commutative ring with size q_k. Let $\mathcal{M}$ be an isomorphism that maps the messages onto a complete set of coset leaders of $\mathbb{Z}[\mathsf{i}]/q\mathbb{Z}[\mathsf{i}]$ with minimum energy. For $k \in \{1, \ldots, K\}$, we enforce $w_k \in \mathbb{B}_{q_k}^2$ which can be represented as $w_k = (w_{k,0}, w_{k,1})$ where each $w_{k,\ell} \in \mathbb{B}_{q_k}$. The encoder maps $w_{1,\ell}, \ldots, w_{K,\ell}$ into the signal of the layer $\ell \in \{0, 1\}$ as

$$x_\ell = \mathcal{M}(w_{1,\ell}, \ldots, w_{K,\ell}) \in \mathbb{Z}[\mathsf{i}]/q\mathbb{Z}[\mathsf{i}], \quad \ell \in \{0, 1\}.$$

TABLE IV

PRIME FACTORIZATION OF $p < 100$ IN $\mathbb{Z}[\omega][\theta]$ WHERE $\theta = \zeta_{28} + \zeta_{28}^{-1}$

p	$\mathfrak{p}$	f
2	$(\theta^4 - 5\theta^2 + \theta + 5)$	6
3	$(3, (7\omega+6)\theta^5 + (3\omega+6)\theta^4 + (3\omega+2)\theta^3 + (3\omega+8)\theta^2 + (8\omega+4)\theta + 3\omega + 5)$	3
	$(3, (7\omega+8)\theta^5 + (\omega+1)\theta^4 + (\omega+4)\theta^3 + (7\omega+7)\theta^2 + (3\omega+7)\theta + 5\omega + 6)$	
5	$((\omega-1)\theta^5 + (\omega-2)\theta^4 + (4-5\omega)\theta^3 + (9-5\omega)\theta^2 + (5\omega-2)\theta + 6\omega - 8)$	6
	$((1-\omega)\theta^5 + (1-2\omega)\theta^4 + (4\omega-5)\theta^3 + (9\omega-5)\theta^2 + (5-2\omega)\theta - 8\omega + 6)$	6
7	$(7, (32\omega+15)\theta^5 + (22\omega+21)\theta^4 + (23\omega+14)\theta^3 + (44\omega+10)\theta^2 + (18\omega+21)\theta + 3\omega + 20)$	1
	$(7, (36\omega+12)\theta^5 + (22\omega+27)\theta^4 + (26\omega+36)\theta^3 + (23\omega+42)\theta^2 + (14\omega+43)\theta + 9\omega + 29)$	
11	$((\omega+1)\theta^5 - (2\omega+1)\theta^4 - (4\omega+5)\theta^3 + (9\omega+5)\theta^2 + (2\omega+5)\theta - 8\omega - 6)$	6
	$((\omega+1)\theta^5 + (2\omega+1)\theta^4 - (4\omega+5)\theta^3 - (9\omega+5)\theta^2 + (2\omega+5)\theta + 8 + 6)$	
13	$(\omega\theta^4 - (5\omega-1)\theta^2 + 5\omega - 3), ((1-\omega)\theta^4 + (4\omega-5)\theta^2 - 2\omega + 4), ((\omega-1)\theta^4 + (5-4\omega)\theta^2 + 3\omega - 5)$	2
	$((\omega-1)\theta^4 + (4-5\omega)\theta^2 + 5\omega - 2), (\omega\theta^4 - (4\omega+1)\theta^2 + 2\omega + 2), ((1-\omega)\theta^4 + (5\omega-4)\theta^2 - 5\omega + 3)$	
17	$((\omega-1)\theta^4 - (2\omega+1)\theta^3 + (5-2\omega)\theta^2 + (3\omega+3)\theta + 2\omega - 5)$	
	$((\omega-1)\theta^5 + 3\theta^4 + (3-6\omega)\theta^3 + (\omega-13)\theta^2 + (8\omega+1)\theta - 4\omega + 10)$	6
19	$(19, (61\omega+187)\theta^5 + (107\omega+256)\theta^4 + (123\omega+152)\theta^3 + (87\omega+168)\theta^2 + (100\omega+76)\theta + 172\omega + 278)$	3
	$(19, (89\omega+144)\theta^5 + 176\omega\theta^4 + (198\omega+167)\theta^3 + (42\omega+90)\theta^2 + (42\omega+214)\theta + 134\omega + 293)$	
	$(19, (103\omega+89)\theta^5 + (27\omega+254)\theta^4 + (229\omega+360)\theta^3 + (296\omega+260)\theta^2 + (100\omega+197)\theta + 61\omega + 239)$	
	$(19, (158\omega+258)\theta^5 + (98\omega+84)\theta^4 + (119\omega+3)\theta^3 + (159\omega+249)\theta^2 + (234\omega+184)\theta + 28\omega + 19)$	
23	$((3-2\omega)\theta^4 - (\omega+1)\theta^3 + (9\omega-16)\theta^2 + (\omega+6)\theta - 9\omega + 16)$	
	$((3-\omega)\theta^4 + (2\omega-1)\theta^3 + (7\omega-16)\theta^2 + (6-7\omega)\theta - 7\omega + 16)$	6
29	$(\theta^5 - \theta^4 - 5\theta^3 + 4\theta^2 + 5\theta - 3), (\theta^4 - \theta^3 - 5\theta^2 + 3\theta + 4), (\omega\theta^2 - \omega\theta - 3\omega)$	2
	$(\omega\theta^2 + \omega\theta - 3\omega), (\theta^4 + \theta^3 - 5\theta^2 - 3\theta + 4), (\theta^5 + \theta^4 - 5\theta^3 - 4\theta^2 + 5\theta + 3)$	
31	$(31, (724\omega+833)\theta^5 + (545\omega+827)\theta^4 + (656\omega+170)\theta^3 + (771\omega+171)\theta^2 + (715\omega+907)\theta + 680\omega + 916)$	3
	$(31, (45\omega+21)\theta^5 + (266\omega+398)\theta^4 + (942\omega+59)\theta^3 + (506\omega+472)\theta^2 + (43\omega+69)\theta + 210\omega + 417)$	
	$(31, (927\omega+236)\theta^5 + (56\omega+700)\theta^4 + (151\omega+808)\theta^3 + (525\omega+9)\theta^2 + (749\omega+157)\theta + 951\omega + 828)$	
	$(31, (194\omega+143)\theta^5 + (848\omega+7)\theta^4 + (305\omega+255)\theta^3 + (521\omega+168)\theta^2 + (378\omega+357)\theta + 861\omega + 890)$	
37	$((1-\omega)(\theta^5 - \theta^4 - 5\theta^3) + (5-6\omega)(\theta^2 + \theta) + 5\omega - 3), ((1-\omega)\theta^4 + (\omega-2)\theta^3 + (4\omega-3)\theta^2 + (5-2\omega)\theta - 4\omega + 3)$	3
	$((\omega-1)(\theta^5 - \theta^4 - 5\theta^3) + (5\omega-6)(\theta^2 + \theta) - 3\omega + 5), (\omega\theta^4 - (\omega+1)\theta^3 - (4\omega-1)\theta^2 + (2\omega+3)\theta + 4\omega - 1)$	
41	$(\theta^4 - \theta^3 - (4-\omega)\theta^2 - (\omega-3)\theta - \omega + 2), (\theta^5 + \omega\theta^4 - (\omega+5)\theta^3 - (5\omega+1)\theta^2 + (3\omega+5)\theta + 6\omega + 2)$	2
	$(\omega\theta^4 + (\omega-1)\theta^3 - 4\omega\theta^2 + (3-3\omega)\theta + 4\omega - 2), (\omega\theta^4 - \theta^3 - (4\omega+1)\theta^2 + (4-\omega)\theta + 2\omega + 3)$	
	$(\theta^3 - (\omega+1)\theta^2 - 2\theta + 3\omega + 1), (\omega\theta^5 + \omega\theta^4 - 5\omega\theta^3 + (1-5\omega)\theta^2 + (5\omega+1)\theta + 5\omega - 2)$	
43	$((2-\omega)\theta^4 + (5\omega-9)\theta^2 - 5\omega + 7), ((1-\omega)\theta^4 + (6\omega-5)\theta^2 - 7\omega + 5), (\theta^4 + (\omega-4)\theta^2 - 2\omega + 2)$	2
	$((2\omega-1)\theta^4 + (5-9\omega)\theta^2 + 7\omega - 5), ((1-\omega)\theta^4 + (5\omega-6)\theta^2 - 5\omega + 7), ((\omega-1)\theta^4 + (4-3\omega)\theta^2 - 2)$	
47	$((1-\omega)(2\theta^5 - 2\theta^4 - 7\theta^3 + 5\theta^2 + \theta + 8), ((\omega-1)(2\theta^5 + 2\theta^4 - 7\theta^3 - 5\theta^2 + \theta - 8))$	6
53	$(3\theta^4 + 5\theta^3 - 17\theta^2 - 13\theta + 17), ((\omega-1)(3\theta^5 - 2\theta^4 - 20\theta^3 + 5\theta^2 + 30\theta + 8))$	6
59	$(3\omega\theta^5 - 18\omega\theta^3 + 21\omega\theta + 2\omega), (3\omega\theta^5 - 18\omega\theta^3 + 21\omega\theta - 2\omega)$	6
61	$(5 - 9\omega), (4 - 9\omega)$	6
67	$(7\omega + 2), (2\omega + 7)$	6
71	$((2-\omega)\theta^4 + (\omega-1)\theta^3 + (5\omega-9)\theta^2 + (4-3\omega)\theta - 5\omega + 7), (-\theta^5 + \theta^4 + (6-\omega)\theta^3 - 6\theta^2 + (3\omega-9)\theta - \omega + 8)$	2
	$(\theta^5 - \theta^4 - 5\theta^3 + (6-\omega)\theta^2 + (6-\omega)\theta + 2\omega - 7), (\theta^5 + \theta^4 - 5\theta^3 + (\omega-6)\theta^2 + (6-\omega)\theta - 2\omega + 7)$	
	$((\omega-1)(\theta^5 + \theta^4 - 6\theta^2) + (5-6\omega)\theta^3 + (9\omega-6)\theta + 8\omega - 7), (\omega\theta^4 - \theta^3 - 4\omega\theta^2 + 3\theta + 2\omega - 2)$	
73	$(\omega + 8), (8\omega + 1)$	6
79	$(7 - 10\omega), (3 - 10\omega)$	6
83	$(\theta^5 - 5\theta^3 - \theta^2 + 6\theta + 4), ((2-2\omega)\theta^4 + (\omega-1)\theta^3 + (9\omega-9)\theta^2 + (2-2\omega)\theta - 8\omega + 8)$	2
	$((\omega-1)(\theta^5 + \theta^4 - 4\theta^3 - 4\theta^2 + 2\theta + 4), (\theta^5 - 5\theta^3 + \theta^2 + 6\theta - 4)$	
	$(2\theta^4 + \theta^3 - 9\theta^2 - 2\theta + 8), (\theta^5 - \theta^4 - 4\theta^3 + 4\theta^2 + 2\theta - 4)$	
89	$(5\omega\theta^4 - (2\omega+1)\theta^3 + (1-18\omega)\theta^2 + (2-\omega)\theta + 18\omega - 1))$	6
	$((3-2\omega)\theta^5 + (3-2\omega)\theta^4 + (17\omega-23)\theta^3 + (15\omega-20)\theta^2 + (39-31\omega)\theta - 32\omega + 38)$	6
97	$(\theta^2 + 2\omega - 4), (\omega\theta^4 - 4\omega\theta^2 + 2\omega + 2), ((1-\omega)\theta^4 + (5\omega-5)\theta^2 - 3\omega + 5)$	2
	$(\theta^2 - 2\omega - 2), (\theta^4 - 4\theta^2 + 2\omega + 2), (\omega\theta^4 - 5\omega\theta^2 + 3\omega + 2)$	

The overall codebook becomes a subset of $\mathcal{C}_{\mathbb{Z}[\mathrm{i}]}$ given by

$$\mathcal{C} \triangleq \left\{ \begin{pmatrix} x_0 & -x_1^* \\ x_1 & x_0^* \end{pmatrix} \middle| \, x_0, x_1 \in \mathbb{Z}[\mathrm{i}]/q\mathbb{Z}[\mathrm{i}] \right\}. \tag{24}$$

For the proposed layered Alamouti-coded index coding, we provide the following result without proof. The proof is essentially identical to the proof of Theorem 9.

Theorem 16: For any $\mathcal{S} \subset \{1, \ldots, K\}$, the proposed Alamouti-coded index coding provides $\Gamma(\mathcal{C}, \mathcal{S}) = 6$ dB/bits per real symbol.

A. Examples and Simulation Results

Here, we list choices of ϕ_k lying above a prime $p < 100$. In Table V, we show principal ideals and their inertial degrees f. From $d_{\mathbb{Q}(\mathrm{i})} = 4$, we know that the ramification index of each prime ideal lying above $p \neq 2$ is 1 and is 2 for prime ideals lying above 2.

Simulation results for using the proposed layered Alamouti-coded index coding over the 2×1 MISO channel are provided in Fig. 5. In this figure, we construct the proposed layered Alamouti-index coding with two ideals generated by $\beta_1 = 1 + 2\mathrm{i}$ and $\beta_2 = 1 - 2\mathrm{i}$, respectively. From Table V, we know that $5\mathbb{Z}[\mathrm{i}] = \beta_1\beta_2\mathbb{Z}[\mathrm{i}]$ and each ideal has norm equal to $p = 5$. Each message consists of two sub-messages in $\mathbb{Z}_5$ and we encode the sub-messages of the same layer into the signal of that layer. The overall codebook becomes (24) with $x_0, x_1 \in \mathbb{Z}[\mathrm{i}]/5\mathbb{Z}[\mathrm{i}]$. The results in Fig. 5 indicates a roughly 8.1 dB SNR gain when either message is revealed to

TABLE V
PRIME FACTORIZATION OF $p < 100$ IN $\mathbb{Z}[\mathrm{i}]$

p	(ϕ)	f
2	$(1+\mathrm{i})$	1
3	(3)	2
5	$(1+2\mathrm{i}), (1-2\mathrm{i})$	1
7	(7)	2
11	(11)	2
13	$(2+3\mathrm{i}), (2-3\mathrm{i})$	1
17	$(1+4\mathrm{i}), (1-4\mathrm{i})$	1
19	(19)	2
23	(23)	2
29	$(2+5\mathrm{i}), (2-5\mathrm{i})$	1
31	(31)	2
37	$(1+6\mathrm{i}), (1-6\mathrm{i})$	1
41	$(5+4\mathrm{i}), (5-4\mathrm{i})$	1
43	(43)	2
47	(47)	2
53	$(2+7\mathrm{i}), (2-7\mathrm{i})$	1
59	(59)	2
61	$(5+6\mathrm{i}), (5-6\mathrm{i})$	1
67	(67)	2
71	(71)	2
73	$(3+8\mathrm{i}), (3-8\mathrm{i})$	1
79	(79)	2
83	(83)	2
89	$(5+8\mathrm{i}), (5-8\mathrm{i})$	1
97	$(4+9\mathrm{i}), (4-9\mathrm{i})$	1

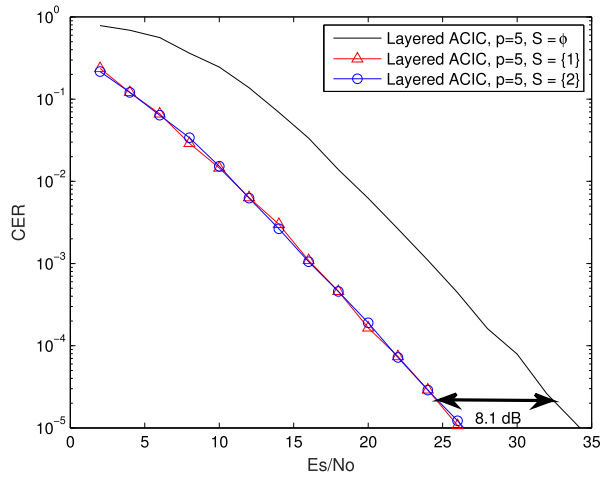

Fig. 5. CER performance for the proposed layered Alamouti-coded index coding (ACIC). The curve with $\mathcal{S} = \emptyset$ corresponds to the overall code.

the receiver. This can be accurately predicted by our analysis that revealing either message leads to an SNR gain given by

$$\frac{1}{2}10\log_{10}\left(\frac{4}{2}\right) + \frac{1}{2}10\log_{10}(25) \approx 8.49 \text{ dB},$$

where 4 and 2 in the first logarithms are $N_{\mathcal{C}}$ and $N_{\mathcal{C}_{\mathcal{S}}}$, respectively, and 25 inside the second logarithm corresponds to the gain in determinant.

X. 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 over STBC has been proposed for exploiting side information without prior knowledge of the side information configuration. It has been shown that the proposed LSTIC possesses the nice property that for any possible side information the minimum determinant increases exponentially as the rate of the side information increases. Moreover, when constructed over perfect STBC, the perfect STBC properties are preserved by our construction and therefore the LSTIC is itself a perfect STBC. Examples including constructions of LSTIC over Golden code, 3×3 perfect STBC, 4×4 perfect STBC, 6×6 perfect STBC, and Alamouti code have been provided and simulations have been conducted to corroborate our analysis. Since Alamouti code also belongs to the family of orthogonal designs [38], it is encouraged to see whether the proposed method can partition other STBC designs which are not constructed from cyclic division algebras. A potential future work is to extend the proposed method to other STBCs that are of practical importance, such as orthogonal designs, quasi-orthogonal designs [39], and fast-decodable STBCs [40].

REFERENCES

[1] Y. Birk and T. Kol, "Informed-source coding-on-demand (ISCOD) over broadcast channels," in *Proc. IEEE INFOCOM*, Mar./Apr. 1998, pp. 1257–1264.
[2] Y. Birk and T. Kol, "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] M. A. Maddah-Ali and U. Niesen, "Coding for caching: Fundamental limits and practical challenges," *IEEE Commun. Mag.*, vol. 54, no. 8, pp. 23–29, Aug. 2016.
[5] T. J. 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.
[6] G. Kramer and S. Shamai (Shitz), "Capacity for classes of broadcast channels with receiver side information," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Sep. 2007, pp. 313–318.
[7] W.-C. Kuo and C.-C. Wang, "Two-flow capacity region of the COPE principle for wireless butterfly networks with broadcast erasure channels," *IEEE Trans. Inf. Theory*, vol. 59, no. 11, pp. 7553–7575, Nov. 2013.
[8] Y. Wu, "Broadcasting when receivers know some messages *a priori*," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2007, pp. 1141–1145.
[9] J. W. Yoo, T. Liu, and F. Xue, "Gaussian broadcast channels with receiver message side information," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2009, pp. 2472–2476.
[10] 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. Inf. Theory (ISIT)*, Jun. 2014, pp. 81–85.
[11] 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.
[12] E. Tuncel, "Slepian–Wolf coding over broadcast channels," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1469–1482, Apr. 2006.
[13] L. Natarajan, Y. Hong, and E. Viterbo, "Capacity optimality of lattice codes in common message Gaussian broadcast channels with coded side information," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2017, pp. 1833–1837.
[14] A. A. Mahesh and B. S. Rajan, "Index coded PSK modulation," in *Proc. IEEE Wireless Commun. Netw. Conf.*, Apr. 2016, pp. 1–7.
[15] L. Natarajan, Y. Hong, and E. Viterbo, "Index codes for the Gaussian broadcast channel using quadrature amplitude modulation," *IEEE Commun. Lett.*, vol. 19, no. 8, pp. 1291–1294, Aug. 2015.
[16] L. Natarajan, Y. Hong, and E. Viterbo, "Lattice index coding," *IEEE Trans. Inf. Theory*, vol. 61, no. 12, pp. 6505–6525, Dec. 2015.
[17] Y.-C. Huang, "Lattice index codes from algebraic number fields," *IEEE Trans. Inf. Theory*, vol. 63, no. 4, pp. 2098–2112, Apr. 2017.

[18] Y.-C. Huang, Y. Hong, and E. Viterbo, "Golden-coded index coding," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2017, pp. 2548–2552.
[19] J. Boutros, E. Viterbo, C. Rastello, and J.-C. Belfiore, "Good lattice constellations for both Rayleigh fading and Gaussian channels," *IEEE Trans. Inf. Theory*, vol. 42, no. 2, pp. 502–518, Mar. 1996.
[20] F. Oggier and E. Viterbo, "Algebraic number theory and code design for Rayleigh fading channels," *Commun. Inf. Theory*, vol. 1, no. 3, pp. 333–416, 2004.
[21] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge, U.K.: Cambridge Univ. Press, 2005.
[22] F. Oggier, J.-C. Belfiore, and E. Viterbo, "Cyclic division algebras: A tool for space-time coding," *Found. Trends Commun. Inf. Theory*, vol. 4, no. 1, pp. 1–95, 2007.
[23] S. M. Alamouti, "A simple transmit diversity technique for wireless communications," *IEEE J. Sel. Areas Commun.*, vol. 16, no. 8, pp. 1451–1458, Oct. 1998.
[24] B. A. Sethuraman, B. S. Rajan, and V. Shashidhar, "Full-diversity, high-rate space-time block codes from division algebras," *IEEE Trans. Inf. Theory*, vol. 49, no. 10, pp. 2596–2616, Oct. 2003.
[25] J.-C. Belfiore, G. Rekaya, and E. Viterbo, "The golden code: A 2×2 full-rate space-time code with nonvanishing determinants," *IEEE Trans. Inf. Theory*, vol. 51, no. 4, pp. 1432–1436, Apr. 2005.
[26] 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.
[27] D. Champion, J.-C. Belfiore, G. Rekaya, and E. Viterbo, "Partitioning the Golden code: A framework to the design of space-time coded modulation," in *Proc. Can. Workshop Inf. Theory*, 2005, pp. 1–2.
[28] G. Ungerboeck, "Channel coding with multilevel/phase signals," *IEEE Trans. Inf. Theory*, vol. TIT-28, no. 1, pp. 55–67, Jan. 1982.
[29] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*. New York, NY, USA: Springer Verlag, 1999.
[30] T. W. Hungerford, *Algebra* (Graduate Texts in Mathematics). New York, NY, USA: Springer-Verlag, 1974.
[31] I. Stewart and D. Tall, *Algebraic Number Theory and Fermat's Last Theorem*. Boca Raton, FL, USA: CRC Press, 2001.
[32] S. Lang, *Algebraic Number Theory* (Graduate Texts Mathematics). New York, NY, USA: Springer-Verlag, 1994.
[33] P. Elia, B. A. Sethuraman, and P. V. Kumar, "Perfect space–time codes for any number of antennas," *IEEE Trans. Inf. Theory*, vol. 53, no. 11, pp. 3853–3868, Nov. 2007.
[34] E. Viterbo and J. Boutros, "A universal lattice code decoder for fading channels," *IEEE Trans. Inf. Theory*, vol. 45, no. 5, pp. 1639–1642, Jul. 1999.
[35] G. Rekaya and J.-C. Belfiore, "On the complexity of ml lattice decoders for decoding linear full rate space-time codes," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul./Jul. 2003, p. 206.
[36] W. Bosma, J. Cannon, and C. Playoust, "The Magma algebra system. I. The user language," *J. Symbolic Comput.*, vol. 24, pp. 235–265, 1997.
[37] J. H. Conway and D. A. Smith, *On Quaternions and Octonions*. Boca Raton, FL, USA: CRC Press, 2003.
[38] V. Tarokh, H. Jafarkhani, and A. R. Calderbank, "Space-time block codes from orthogonal designs," *IEEE Trans. Inf. Theory*, vol. 45, no. 5, pp. 1456–1467, Jul. 1999.
[39] H. Jafarkhani, "A quasi-orthogonal space-time block code," *IEEE Trans. Commun.*, vol. 49, no. 1, pp. 1–4, Jan. 2001.
[40] E. Biglieri, Y. Hong, and E. Viterbo, "On fast-decodable space–time block codes," *IEEE Trans. Inf. Theory*, vol. 55, no. 2, pp. 524–530, Feb. 2009.

Yu-Chih Huang (M'14) received his Ph.D degree in electrical and computer engineering from Texas A&M University (TAMU) in 2013. He was a postdoctoral research associate at TAMU from 2013 to 2015. Since February 2015, he has been with the Department of Communication Engineering, National Taipei University, Taiwan, where he is currently an Associate Professor. In 2012, he spent the summer as a research intern in Bell Labs, Alcatel-Lucent. His research interests are in information theory, network information theory, lattice coding theory, and wireless communications.

Yi Hong (S'00–M'05–SM'10) is currently a Senior Lecturer at the Department of Electrical and Computer Systems Eng., Monash University, Melbourne, Australia. She obtained her Ph.D. degree in Electrical Engineering and Telecommunications from the University of New South Wales (UNSW), Sydney, and received the NICTA-ACoRN Earlier Career Researcher Award at the Australian Communication Theory Workshop, Adelaide, Australia, 2007. She currently serves on the Australian Research Council College of Experts (2018-2020).

Dr. Hong was an Associate Editor for IEEE WIRELESS COMMUNICATION LETTERS and *Transactions on Emerging Telecommunications Technologies (ETT)*. She was the General Co-Chair of IEEE Information Theory Workshop 2014, Hobart; the Technical Program Committee Chair of Australian Communications Theory Workshop 2011, Melbourne; and the Publicity Chair at the IEEE Information Theory Workshop 2009, Sicily. She was a Technical Program Committee member for many IEEE leading conferences. Her research interests include communication theory, coding and information theory with applications to telecommunication engineering.

Emanuele Viterbo (M'95–SM'04–F'11)is currently a professor in the ECSE Department and an Associate Dean in Graduate Research at Monash University, Melbourne, Australia. He received his Ph.D. in 1995 in Electrical Engineering, from the Politecnico di Torino, Torino, Italy. From 1990 to 1992 he was with the European Patent Office, The Hague, The Netherlands, as a patent examiner in the field of dynamic recording and error-control coding. Between 1995 and 1997 he held a post-doctoral position in the Dipartimento di Elettronica of the Politecnico di Torino. In 1997-98 he was a post-doctoral research fellow in the Information Sciences Research Center of AT&T Research, Florham Park, NJ, USA. From 1998-2005, he worked as Assistant Professor and then Associate Professor, in Dipartimento di Elettronica at Politecnico di Torino. From 2006-2009, he worked in DEIS at University of Calabria, Italy, as a Full Professor.

Prof. Emanuele Viterbo is an ISI Highly Cited Researcher since 2009. He served as Associate Editor of IEEE TRANSACTIONS ON INFORMATION THEORY, *European Transactions on Telecommunications* and *Journal of Communications and Networks*, and Guest Editor for IEEE *Journal of Selected Topics in Signal Processing*: Special Issue Managing Complexity in Multiuser MIMO Systems. Prof. Emanuele Viterbo was awarded a NATO Advanced Fellowship in 1997 from the Italian National Research Council. His main research interests are in lattice codes for the Gaussian and fading channels, algebraic coding theory, algebraic space-time coding, digital terrestrial television broadcasting, digital magnetic recording, and irregular sampling.

Lakshmi Natarajan is an Assistant Professor in the Department of Electrical Engineering, Indian Institute of Technology Hyderabad. He received the B.E. degree from the College of Engineering, Guindy, in electronics and communication in 2008, and the Ph.D. degree from the Indian Institute of Science, Bangalore, in 2013. Between 2014 and 2016 he held a post-doctoral position at the Department of Electrical and Computer Systems Engineering, Monash University, Australia. His primary research interests are coding and information theory for communication systems.

Dr. Natarajan is an Editor of the IEEE WIRELESS COMMUNICATIONS LETTERS. He was the recipient of the Seshagiri-Kaikini Medal 2013-14 for best Ph.D. thesis, Department of Electrical Communication Engineering, Indian Institute of Science, Bangalore. He was recognized as an Exemplary Reviewer by the editorial board of the IEEE WIRELESS COMMUNICATIONS LETTERS in 2013, 2015 and 2016. He served as the Publications Co-Chair of the 2018 National Conference on Communications (NCC), Hyderabad, and as the Local Arrangements Co-Chair of the 2016 Australian Communications Theory Workshop, Melbourne and the 2016 Australian Information Theory School, Melbourne. He was also a member of the technical program committee of the 2018 International Conference on Signal Processing and Communications (SPCOM).