Lattice Index Codes from Algebraic Number Fields

Yu-Chih Huang
Department of Communication Engineering
National Taipei University
{ychuang@mail.ntpu.edu.tw}

Abstract—Broadcasting $K$ independent messages to multiple users where each user has a subset of the $K$ messages as side information is studied. This problem can be regarded as a natural generalization of the well-known index coding problem to the physical-layer additive white Gaussian noise channel due to the analogy between these two problems. Recently, Natarajan, Hong, and Viterbo proposed a novel broadcasting strategy called lattice index coding which uses lattices constructed over principal ideal domains (PIDs) as a transmission scheme and showed that such a scheme provides uniform side information gains. In this paper, we generalize this strategy to rings of algebraic integers of number fields which may not be PIDs and show upper and lower bounds on the achievable side information gains. This generalization substantially enlarges the design space and includes some interesting examples in which all the messages are from the same field.

Index Terms—Lattice codes, index coding, and broadcast channel with side information.

I. INTRODUCTION AND PROBLEM STATEMENT

We consider a tower broadcasting $K$ independent messages \(\{w_1, w_2, \ldots, w_K\}\) to $L$ receivers where the received signal at the receiver $l$ is given by \(y_l = \sqrt{\text{SNR}_l}x_l + z_l\), with $x_l$ being the transmitted signal, $z_l \sim \mathcal{CN}(0,1)$ being Gaussian noise, and $\text{SNR}_l$ being signal-to-noise ratio. We further assume that the receiver $l$ has a subset of messages $w_{S_l} = \{w_k : k \in S_l\}$ as side information which is governed by its index $S_l \subset \{1, 2, \ldots, K\}$ as shown in Fig. 1. This problem is analogous to the index coding problem [1] [2] [3] [4] extended to the physical-layer AWGN channel.

In [5], Natarajan et al. formulated the problem and particularly studies the case where all the $L$ receivers demand all the $K$ messages but can have different subset of side information $S_l, l \in \{1, \ldots, L\}$. For a code $C$, one can define the side information gain of the receiver $l$ as

\[
\Gamma(C, S_l) \triangleq \frac{10 \log_{10}(d_{S_l}^2/d_0^2)}{R_{S_l}},
\]

where $d_0$ and $d_{S_l}$ are the minimum Euclidean distance of the code before and after $S_l$ is given, respectively, and $R_{S_l}$ is the sum rate of $w_{S_l}$, the messages with indices in $S_l$. This is the measure of the gain in squared Euclidean distance provided by each bit of side information in $S_l$. One can also define the overall side information gain for the system as

\[
\Gamma(C) \triangleq \min_{S_l} \Gamma(C, S_l).
\]

Natarajan et al. then proposed a novel coding scheme which uses nested lattice codes from lattices over some principal ideal domains (PIDs) and termed this scheme “lattice index codes”. Using the Chinese remainder theorem (CRT), they showed that the lattice index codes provide uniform side information gains, $\Gamma(C, S)$ is a constant for every choice of $S \subset \{1, 2, \ldots, K\}$, which mimics the behavior of a capacity-achieving index code at high message rates.

In this paper, we generalize the lattice index coding scheme in [5] to accommodate lattices constructed over general rings of algebraic integers. Our scheme is a direct extension of the one by Natarajan et al. [5] to number fields whose rings of integers may not form PID. Although for a general ring of algebraic integers, our generalization may not have the uniform side information gain property, we provide upper and lower bounds on $\Gamma(C, S)$ for every $S \subset \{1, 2, \ldots, K\}$. The bounds only differ by a constant governed by the underlying number field. This generalization substantially expands the design space and includes some interesting design examples. As pointed out in [5], one drawback of the lattice index codes therein is that the messages are not from the same fields. We provide some design examples which overcome this issue.

II. LATTICE INDEX CODING OVER RINGS OF ALGEBRAIC INTEGERS

In this section, we propose constructing lattice index codes over rings of algebraic integers. This can be regarded as a direct extension of the scheme in [5] to number fields. We first discuss construction over rings of algebraic integers and then generalize it to self-similar lattices over such rings.
A. Construction over Rings of Algebraic Integers

Let \( K \) be an algebraic number field with degree \( n = [K : \mathbb{Q}] \) and signature \((r_1, r_2)\) and let \( \Omega_K \) be its ring of integers. Let \( p_1, \ldots, p_K \) be prime ideals of \( \Omega_K \) lying above \( p_1, \ldots, p_K \) with inertial degrees \( f_1, \ldots, f_K \), respectively. Moreover, \( p_1, \ldots, p_K \) are relatively prime. From CRT, we have a ring isomorphism

\[
\mathcal{M} : \mathbb{F}_{p_1} \times \ldots \times \mathbb{F}_{p_K} \rightarrow \Omega_K / \Pi_{k=1}^{K} p_k.
\]

(3)

Hence, one can have the decomposition

\[
\Omega_K = \mathcal{M}(\mathbb{F}_{p_1}^1, \ldots, \mathbb{F}_{p_K}^1) + \Pi_{k=1}^{K} p_k.
\]

(4)

Consider the canonical embedding \(^1\) given by

\[
\Psi(x) = (\sigma_1(x), \ldots, \sigma_n(x)),
\]

where \( \sigma_1, \ldots, \sigma_{r_1} \) are real \( \mathbb{Q} \)-monomorphisms and \( \sigma_{r_1+1}, \ldots, \sigma_n \) are the complex \( \mathbb{Q} \)-monomorphisms with \( \sigma_{r_1+1+2i} = \sigma_{r_1+i+i} \) for \( i \in \{1, 2\} \). For an ideal \( \mathfrak{I} \) we denote by \( \Lambda_{\mathfrak{I}} \) the lattice-representation obtained by mapping each element of \( \mathfrak{I} \) to \( \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \) via \( \Psi \). With this notation, from (4), one obtains that \( \Lambda_{\Omega_K} = \mathcal{M}(\mathbb{F}_{p_1}^1, \ldots, \mathbb{F}_{p_K}^1) + \Lambda_{\Pi_{k=1}^{K} p_k} \)

where we abuse the notation to use the same \( \mathcal{M} \) to denote the ring isomorphism before and after the mapping \( \Psi \). In the following, we will stick to the ideal-representation for the ease of presentation; however, one should be aware of that in practice the transmitted signal is from the lattice-representation.

We are now ready to describe the proposed lattice index coding scheme which essentially follows the idea in [5]. Let \( w_k \in \mathbb{F}_{p_k^1} \) for \( k \in \{1, \ldots, K\} \). For a particular set of \( (w_1, \ldots, w_K) \in \mathbb{F}_{p_1} \times \ldots \times \mathbb{F}_{p_K} \), the transmitted signal of the proposed scheme is given by

\[
x = \mathcal{M}(w_1, \ldots, w_K) \mod \Pi_{k=1}^{K} p_k.
\]

(6)

Note that the constellation defined above can be any complete set of coset representatives. We particularly choose one with the minimum energy as our constellation for energy saving. An example is provided in the following.

**Example 1** (Non-PID). Consider \( K = \mathbb{Q}(\sqrt{\delta}) \) whose ring of integers is \( \mathbb{Z}[\sqrt{\delta}] \). Note that this is not a PID so one cannot simply treat ideals as numbers as we did in PIDs. Consider the following two prime ideals \( p_1 = (3, 1 + \sqrt{-5}) \) and \( p_2 = (7, 3 + \sqrt{-5}) \) lying above \( p_1 = 3 \) and \( p_2 = 7 \), respectively. One can verify that \( p_1, p_2 = (21, 7 + 7\sqrt{-5}, 9 + 3\sqrt{-5}) \) (this can be further simplified as in a Dedekind domain, every ideal can be generated by at most two elements). Fig. 2 shows the proposed lattice index coding scheme (before \( \Psi(.) \)) constructed with these ideals. The labels in this figure represents the mapping from \( \mathbb{F}_3 \times \mathbb{F}_7 \) to the constellation. One can verify that this mapping is a ring isomorphism between \( \mathbb{F}_3 \times \mathbb{F}_7 \) and \( \Omega_K / p_1 \).

![](image)

**Fig. 2.** A lattice index constellation constructed from \( \mathbb{Q}(\sqrt{-5}) \) where only those lattice points inside the black box are used and the labels are the mapping (a ring isomorphism). The triangles form the constellation after the first message is given to be 0 and the stars form the constellation after the second message is given to be 0.

\(^1\)Here, we use the same canonical embedding with that in [6] instead of the conventional one and that in [5] as this embedding characterizes the geometric structure of ideal lattices so that the Minkowski theorem in geometry of numbers can be easily applied.

---

1. Consider a shifted version of the proposed scheme.
2. Also, the triangles and stars represent the constellation after setting \( w_1 = 0 \) and \( w_2 = 0 \), respectively.

One important property of the proposed scheme regarding the side information gain is summarized in the following theorem.

**Theorem 2.** For the proposed lattice coding scheme over a number field \( K \) with discriminant \( \Delta_K \), the side information gain is approximately uniform. Specifically, the side information gain provided by \( S \subset \{1, \ldots, K\} \) is bounded by

\[
6 \text{ dB} \leq \gamma_S \leq 6 \text{ dB} + \gamma_S,
\]

where \( \gamma_S \triangleq \frac{10 \log_{10} |\Delta_S|}{\sum_{i \in S} \log_2 N(\mathfrak{p}_i)} \).

**Proof:** Let \( \mathfrak{J} = \Pi_{i \in S} \mathfrak{p}_i \). Also, for an ideal \( \mathfrak{I} \), we denote by \( N(\mathfrak{I}) \) its norm. First, one can easily compute the messages’ rate from the coset decomposition (4) as

\[
R_S = \frac{1}{n} \log_2 \frac{\text{Vol}(\Lambda_{\mathfrak{J}})}{\text{Vol}(\Lambda_{\mathfrak{I}})} = \frac{1}{n} \log_2 |\Omega_K / \mathfrak{I}|
\]

(8)

where (a) follows from the definition of the ideal norm operation and (b) is because the ideal norm operation is multiplicative. We then try to compute the minimum distance for the constellation after \( w_S \) is given. Note that suppose \( w_1 = v_1 \) is given, the signal becomes

\[
x_1 = \mathcal{M}(v_1, w_2, \ldots, w_K) \mod \Pi_{k=1}^{K} p_k
\]

(9)

where (a) is because \( \mathcal{M} \) is a ring isomorphism. One can then see that \( x_1 \) is a shifted version of \( x_1' = \mathcal{M}(0, w_2, \ldots, w_K) \mod \Pi_{k=1}^{K} p_k \). As a consequence of CRT, one has \( x_1' \in p_1 \). For a general set \( S \subset \{1, \ldots, K\} \), we define \( x_S' \) to be the signal
obtained by setting \( w_l = 0 \) for \( l \in S \) in \( x \). One can follow the same reasoning to see that CRT guarantees \( x' \in \Pi_{l \in S} p_l \).

Therefore, the minimum distance of this constellation can be bounded by

\[
\sqrt{n}N(\mathfrak{O})^{1/n} \leq d_S \leq \sqrt{n}N(\mathfrak{O})^{1/n} \sqrt{|\Delta_K|^{1/n}}, \tag{10}
\]

where the upper bound is from the Minkowski theorem in geometry of numbers and the lower bound can be shown by the arithmetic mean and geometric mean inequality (a proof of this bound can be found in [6, Sec. 6]).

Combining (8), (10), and the fact that \( d_0 = \sqrt{n} \) \((1 \in \mathfrak{D}_K)\) results in

\[
\frac{20 \log_{10} N(\mathfrak{O})}{\log_2 N(\mathfrak{O})} \leq \Gamma(\mathcal{C}, S) \leq \frac{20 \log_{10} N(\mathfrak{O}) + 10 \log_{10} |\Delta_K|}{\log_2 N(\mathfrak{O})}, \tag{11}
\]

and thus

\[
6 \text{ dB} \leq \Gamma(\mathcal{C}, S) \leq 6 \text{ dB} + \frac{10 \log_{10} |\Delta_K|}{\sum_{l \in S} \log_2 p_l}. \tag{12}
\]

The above theorem provides a general means to bound the side information gain for the proposed scheme with a general \( \mathfrak{D}_K \). In fact, the bound may be sharpened differently for different classes of \( \mathfrak{D}_K \). In the following, we discuss this possibility.

**Theorem 3.** Let \( K = \mathbb{Q}(\sqrt{d}) \) an imaginary quadratic field with \( d < 0 \) square-free integer whose ring of integers \( \mathfrak{D}_K \) happens to be a PID, i.e., \( d \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\} \). For every \( S \subset \{1, \ldots, K\} \), we have \( \Gamma(\mathcal{C}, S) = 6 \text{ dB} \).

**Proof:** Since \( \mathfrak{D}_K \) is a PID, every ideal is generated by a singleton in \( \mathfrak{D}_K \); specifically, \( \mathcal{I} = \phi \mathfrak{D}_K \) for some \( \phi \in \mathfrak{D}_K \). Thus

\[
\Psi(\phi \mathfrak{D}_K) = \{\Psi(\phi x) : x \in \mathfrak{D}_K\}
\]

\[
\{\begin{bmatrix} \sigma_1(\phi) & 0 \\ 0 & \sigma_2(\phi) \end{bmatrix} \begin{bmatrix} \sigma_1(x) \\ \sigma_2(x) \end{bmatrix} : x \in \mathfrak{D}_K\}
\]

\[
= \mathbf{D}_\phi \Psi(x), \tag{13}
\]

where \( \mathbf{D}_\phi \) is the diagonal matrix with the \( i \)-th diagonal element being \( \sigma_i(\phi) \) and (a) is because \( \sigma_1 \) and \( \sigma_2 \) are homomorphisms.

Note that for an imaginary quadratic field which happens to be a PID, \( \mathbf{D}_\phi \) is an orthogonal matrix with \( \mathbf{D}_\phi^T \mathbf{D}_\phi = N(\phi) \cdot I \).

Now, let \( x_1, x_2 \in \mathfrak{D}_K \) are such that \( d_0^2 = \|\Psi(x_1) - \Psi(x_2)\|^2 \).

One has that \( \Psi(\phi x_1), \Psi(\phi x_2) \in \Psi(\phi \mathfrak{D}_K) \) with distance

\[
d^2 = \|\Psi(\phi x_1) - \Psi(\phi x_2)\|^2
\]

\[
= \|\mathbf{D}_\phi \Psi(x_1) - \mathbf{D}_\phi \Psi(x_2)\|^2
\]

\[
= N(\phi) d_0^2.
\]

Therefore,

\[
\Gamma(\mathcal{C}, S) \leq \frac{20 \log_{10} N(\phi)}{\log_2 N(\phi)}, \tag{15}
\]

which coincides with the lower bound in (11) and yields \( \Gamma(\mathcal{C}, S) = 6 \text{ dB} \).

Since \( \mathbb{Z}, \mathbb{Z}[i], \) and \( \mathbb{Z}[\omega] \) are rings of integers of number fields with degrees \( n = 1, n = 2, \) and \( n = 2, \) respectively, the lattice coding scheme in [5] is subsumed as a special case of the proposed scheme\(^2\) and Theorem 3 recovers the results in [5, Sec. IV-B]. The proposed scheme is in fact a direct generalization of their scheme to algebraic number fields and substantially expands the design space. On the other hand, there is another construction in [5] using Hurwitz quaternions \( \mathbb{H} \) (a ring of integers of Hamilton’s quaternions \( \mathbb{H} \)) which form a non-commutative PID. The construction proposed in this paper only considers commutative rings \( \mathfrak{O}_K \) and hence does not contain this construction.

**Remark 4.** Here, we always choose \( p_1, \ldots, p_K \) to be prime ideals that are relatively prime, which is by no means necessary. In fact, the CRT only requires those ideals to be relatively prime. i.e., \( p_i + p_k = \mathfrak{D}_K \) for any pair of \((i, k) \in \{1, \ldots, K\}^2 \) in order to make \( \cap_{i=1}^K p_i = \Pi_{i=1}^K p_i \). The reason that we restrict ourselves to prime ideals is because in a typical communication system, messages are usually encoded by codes over finite fields. Therefore, it is of primary interest to study the case where we actually get a field. Nonetheless, all the results above can be carried over to the general case where \( p_k \)'s are relatively prime but may not be prime ideals.

**B. Construction using Lattices over Number Fields**

So far, what we have had is merely an \( n \)-dimensional modulation scheme instead of a coding scheme. Here, akin to [5], we extend the scheme proposed above over \( \mathfrak{D}_K \) to higher dimension and construct a lattice index code from \( \mathfrak{D}_K \)-lattices. Let \( \mathfrak{D}_K \) be the ring of integers of a number field with degree \( n \) and signature \((r_1, r_2) \). Let \( p_1, \ldots, p_K \) be prime ideals lying above \( p_1, \ldots, p_K \), respectively, and \( \mathcal{M} \) be the ring isomorphism discussed above.

Now consider a \( m \)-dimensional \( \mathfrak{D}_K \)-lattices \( \Lambda \triangleq \mathcal{G} \cdot \mathcal{D}_K^m \) where \( \mathcal{G} \) is the generator matrix. Also, define its sub-lattices \( \Lambda_k \triangleq \mathcal{G} \cdot \left( \Pi_{i=1,i\neq k}^K p_i \right)^m \). The lattices considered are the above ones embedded into the Euclidean space as \( \Lambda = \Psi(\Lambda) \) and \( \Lambda_k = \Psi(\Lambda_k) \) for \( k \in \{1, \ldots, K\} \). We have the following decomposition

\[
\Lambda = \Psi(\mathcal{G} \cdot \mathcal{D}_K^m)
\]

\[
\equiv (a) \quad \mathcal{G} \cdot \Psi(\mathcal{D}_K^m)
\]

\[
\equiv (b) \quad \mathcal{G} \cdot \Psi \left( \sum_{k=1}^K c_k \Pi_{i=1,i\neq k}^K p_i \right)^m
\]

\[
\equiv (c) \quad \mathcal{G} \cdot \left( \sum_{k=1}^K \left(c_k \Pi_{i=1,i\neq k}^K p_i \right)^m + \left( \Pi_{i=1}^K p_i \right)^m \right)
\]

\[
\equiv \sum_{k=1}^K \Lambda_k + \Lambda_s, \tag{17}
\]

where in (a) \( \mathcal{G} \) is an \( mn \times mn \) matrix which consists of \( m^2 \)

\( n \times n \) sub-matrices \( \mathcal{G}_{ij} = \text{diag}(\Psi(G_{ij})) \) where \( G_{ij} \) is the \( i \)th

\(^2\)Note that the embeddings used in [5] and here are different but isomorphic to each other.
row $j$th column element of $G$ for $1 \leq i, j \leq m$, (b) follows from the decomposition of $\Omega_K$ in (4), and in (c) $c_k$ is the constant such that CRT holds.

It is clear that $\Lambda_s \subset \Lambda_k \subset \Lambda$ for every $k \in \{1, \ldots, K\}$ and hence one can talk about coset decomposition. The proposed lattice index coding scheme uses this fact and is then given by

$$C = \Lambda/\Lambda_s = \sum_{k=1}^{K} \Lambda_k/\Lambda_s, \quad (18)$$

where by $\Lambda_k/\Lambda_s$ we mean a complete set of coset representatives such that $C$ would have the minimum energy.

We now prove some properties of lattice index codes thus constructed. We first note that for every $S \subset \{1, \ldots, K\}$, it can be easily seen from (16) that

$$R_S = \frac{1}{mn} \log_2((\prod_{l\in S} p_l)^{m_f}) = \frac{1}{n} \sum_{l \in S} \log_2(N(p_l)). \quad (19)$$

Moreover, note that from (18), the transmitted signal is

$$x = \sum_{k=1}^{K} \lambda_k, \quad (20)$$

where $\lambda_k \in \Lambda_k/\Lambda_s$. Given a $S \subset \{1, \ldots, K\}$, the signal belongs to

$$x_S = \sum_{l \in S} \lambda_l + \sum_{k \notin S} \Lambda_k/\Lambda_s, \quad (21)$$

which is a shifted version of

$$\sum_{k \notin S} \Lambda_k/\Lambda_s$$

$$= G \cdot \Psi \left( \sum_{k \notin S} (c_k \Pi_{1 \leq i \neq k} p_i)^m \right) / G \cdot \Psi \left( (\Pi_{1 \leq i} p_i)^m \right)$$

$$= G \cdot \Psi \left( (\Pi_{l \notin S} p_l)^m \right) / G \cdot \Psi \left( (\Pi_{k=1} p_k)^m \right), \quad (22)$$

where the last equality follows from the fact that $p_l, p_k$ are relatively prime for $l \neq k$. It is unfortunately however that we have not been able to prove general results similar to the one in Theorem 2. In the following, we again provide tight bound for imaginary quadratic integers which happen to be PIDs. This slightly generalized the result in [5, Lemma 3].

**Theorem 5.** Let $K = \mathbb{Q}(\sqrt{d})$ an imaginary quadratic field with $d < 0$ square-free integer whose ring of integers $\Omega_K$ happens to be a PID. i.e., $d \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}$. Let $C$ be a lattice index code constructed using lattice over $\Omega_K$. For every $S \subset \{1, \ldots, K\}$, we have $\Gamma(C, S) = 6 dB$.

**Proof:** For PIDs, (22) can be rewritten as

$$G \cdot \Psi \left( (\Pi_{l \notin S} p_l)^m \right) / G \cdot \Psi \left( (\Pi_{k=1} p_k)^m \right), \quad (23)$$

and hence $x_S$ belongs to a shifted version of $G \cdot \Psi (\Pi_{l \in S} \phi_l \Omega_K^m)$. Let

$$D_\phi = I_m \otimes \text{diag}(\Psi(\phi)), \quad (24)$$

where $\otimes$ is the Kronecker product and (a) is true for every imaginary quadratic field. Now, note that for every $a \in \Omega_K$ and $\phi \in \Omega_K$, one has

$$G \cdot \Psi(\phi)a = G \cdot D_\phi \cdot \Psi(a) = D_\phi \cdot G \cdot \Psi(a), \quad (25)$$

where the last equality in is due to the special structures of $D$ and $D_\phi$. One can then show the result by following the steps in Theorem 3 and the fact that $D_\phi$ is an orthogonal matrix.

**Remark 6.** In [5, eq(7)], Natarajan et al. used another approach to bound the side information gain which involves the center density of lattices $\Lambda$ and $\Lambda_k$. A similar bound can be obtained straightforwardly for our scheme. This bound implies that for the proposed lattice index coding scheme over number fields, the gap is not necessarily limited by $\Delta_K$ as in Theorem 2; one may get a smaller gap by first constructing a dense lattice $\Lambda$ from $\Omega_K$ and then use $\Lambda$ for constructing lattice index codes as above. We suspect that for a sufficiently large dimension, one can use Construction A to construct very dense lattices over $\Omega_K$ which will shrink the gap. We do not pursue this approach here and leave it as a potential future work.

### III. Design Examples

In this section, we study some interesting designs of the proposed lattice index coding scheme. One direction for future research mentioned in [5] is to relax a fact of their scheme that $w_{i,s}$ are from different fields. For allowing a fixed number of messages $K$ from the same field $\mathbb{F}_p$ in our scheme, what we are looking for is a number field $K$ in which $p$ splits into at least $K$ prime ideals. In what follows, we particularly look at $K$ having degree $n = K$; hence, we look for $K$ in which $p$ splits completely. Moreover, in order to make the side information gain close to uniform, from Theorem 2, one observes that the discriminant $\Delta_K$ has to be small. For designing a sequence of coding scheme which can take arbitrarily number (possibly infinite) of messages from the same field $\mathbb{F}_p$, we need a sequence of number fields $\{K_l\}$ with small discriminant $\Delta_K$, and $p$ splits into at least $K$ prime ideals in every $K_l$. For the reader who is familiar with algebraic geometric coding theory, the design guideline is very similar to the ones in [7].

**A. Cyclotomic Fields [8]**

Let $\zeta_m$ be a primitive $m$th root of unity and $n = \phi(m)$ where $\phi$ is the Euler phi function. Then $K_m = \mathbb{Q}(\zeta_m)$ is a totally complex number field with degree $n$. i.e., it has
signature $(0, n/2)$. The ring of integers of is $\mathcal{O}_{K_m} = \mathbb{Z}[\zeta_m]$ and the discriminant is given by

$$\Delta_{K_m} = (-1)^{\phi(m)/2} \frac{m^{\phi(m)}}{\prod_{p|m} p^{\nu(m)/(p-1)}}. \quad (26)$$

The study of cyclotomic extensions has a rich history and plays an important role in the long pursuit of the Fermat’s last theorem.

In what follows, we will use the property regarding the behavior of primes. Let $p$ be a natural prime: i) $p\mathcal{O}_{K_m}$ ramifies if and only if $p|m$ and ii) if $\gcd(p, m) = 1$ and $f$ is the least natural number such that $p^f \equiv 1 \bmod m$, then $p\mathcal{O}_{K_m} = p_1 \cdot \cdots \cdot p_h$ where $h \cdot f = n$ and $f$ is the inertial degree for $p_1, \ldots, p_h$. In particular, $p\mathcal{O}_K$ splits completely into $p\mathcal{O}_K = p_1 \cdot \cdots \cdot p_n$ with $N(p_i) = p$ for $i \in \{1, \ldots, n\}$ if and only if $p \equiv 0 \bmod m$.

We now consider lattice index codes over cyclotomic integers. Consider broadcasting $K$ independent messages as described above. We first construct cyclotomic extension $K_m$ with degree $\phi(m) = K$. By Dirichlet’s prime theorem, there are infinitely many primes $p \equiv 0 \bmod m$ for every $m \in \mathbb{N}$. Thus, for such primes, $p\mathcal{O}_K$ splits completely into $p\mathcal{O}_K = p_1 \cdot \cdots \cdot p_n$ with $N(p_i) = p$ for $i \in \{1, \ldots, n\}$ and can be fixed for arbitrary $K$. Hence, we provide a design example where the field size $p$ can be fixed for arbitrary $K$. Before proceeding, we must note that this design is inspired by [7]. Let us start by introducing the foundation of the class field theory.

**Theorem 8** (Hilbert 1898 and Furtwängler 1930). For any number field $K$, there exists a unique finite extension $K'$ (called the Hilbert class field) such that i) $K'/K$ is Galois and the Galois group is isomorphic to the ideal class group of $K$; ii) $K'/K$ is the maximal unramified Abelian extension; iii) for any prime $p$, the inertial degree is the order of $p$ in the ideal class group of $K$; and iv) every ideal of $K$ is principal in $K'$.

For a prime $p$, the Hilbert $p$-class field of $K$ is the maximal $p$-extension (i.e., its degree is a power of $p$) $K'_p$ of $K$ contained in $K'$. One can construct a sequence of $p$-extensions $\{K_i\}$ with $K'_p = (K_{i-1})_p$ and we refer to this sequence of fields as the $p$-class field tower of $K_0$. The tower terminates at $i$ if it is the smallest index such that $K_{i+1} = K_i$. One can also specify a set of primes $T$ in which every prime splits completely in every field in the sequence. We call such sequence of field extensions the $T$-decomposing $p$-class field tower.

From a result in [7, Proposition 19] [9], one can actually construct an infinite $T$-decomposing 2-class field tower if some mild conditions hold. In what follows, we provide an example which is borrowed from [7, Lemma 20].

**Example 9.** Let $d = 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19$ and consider the imaginary quadratic extension $K_0 = \mathbb{Q}(\sqrt{-d})$. One can show that $29\mathcal{O}_{K_0} = p_1, p_2$ with $N(p_1) = N(p_2) = 29$. Let $T = \{p_1, p_2\}$. One can show that $K_0$ has an infinite $T$-decomposing 2-class field tower $K_0 \subset K_1 \subset \cdots$ which never terminates and 29 splits completely all the way up the tower. For any $K$, one can then pick a field $K_i$ in this sequence which has a degree $n \geq K$ and $K$ prime ideals with norm 29 to construct a lattice index code. Note that in [7], there are some examples with even smaller primes such as 17 and 19.

**IV. CONCLUDING REMARKS**

In this paper, the problem of broadcasting $K$ independent messages to multiple users where each of them has a subset of messages as side information has been studied. A lattice index coding scheme has been proposed which is a generalization of the scheme in [5] to general rings of algebraic integers. Upper and lower bounds on the side information gains have been provided which differ only by a constant governed by the underlying number fields. This generalization has substantially expanded the design space and some interesting design examples in which messages are all from the same finite field have been discussed. One potential future work is to consider a larger class of nested lattice codes in addition to self-similar ones considered in both [5] and this paper. A natural extension along this line is to use the multilevel lattices proposed by Huang and Narayanan [10] which has been shown able to produce good lattices. We believe that this would lead one to achievable rates all the way up to the capacity region.

**REFERENCES**

1. Y. Birk and T. Kol, “Informed-source coding-on-demand (ISCOD) over broadcast channel,” in Proc. IEEE INFOCOM, pp. 1257–1264, Mar. 1998.
2. Z. Bar-Yossef, Y. Birk, T. S. Jayram, and T. Kol, “Index coding with side information,” in Proc. IEEE FOCS, pp. 197–206, Oct. 2006.
3. Z. Bar-Yossef, Y. Birk, T. S. Jayram, and T. Kol, “Index coding with side information,” IEEE Trans. Inf. Theory, vol. 57, pp. 1479–1494, Mar. 2011.
4. S. El Rouayheb, A. Sprintson, and C. Georghiades, “On the index coding problem and its relation to network coding and matroid theory,” IEEE Trans. Inf. Theory, vol. 56, pp. 3187–3195, July 2010.
5. L. Natarajan, Y. Hong, and E. Viterbo, “Lattice index coding,” arXiv:1410.6569 [cs.IT], Oct. 2014.
6. C. Peikert and A. Rosen, “Lattices that admit logarithmic worst-case to average-case connection factors,” in Proc. ACM STOC, June 2007.
7. V. Guruswami, “Constructions of codes from number fields,” IEEE Trans. Inf. Theory, vol. 49, pp. 594–603, Mar. 2003.
8. L. C. Washington, Introduction to Cyclotomic Fields (Graduate Texts in Mathematics). Springer, 1997.
9. H. W. Lenstra, “Codes from algebraic number fields,” Mathematics and Computer Science II, Fundamental Contributions in the Netherlands since 1945, pp. 95–104, 1986.
10. Y.-C. Huang and K. R. Narayanan, “Multistage compute-and-forward with multilevel lattice codes based on product constructions,” in Proc. IEEE ISIT, June 2014. arXiv:1401.2228 [cs.IT].