Coprime Sensing via Chinese Remaindering over Quadratic Fields, Part I: Array Designs

Conghui Li, Lu Gan, *Senior Member, IEEE,* and Cong Ling, *Member, IEEE*

***Abstract*—A coprime antenna array consists of two or more sparse subarrays featuring enhanced degrees of freedom (DOF) and reduced mutual coupling. This paper introduces a new class of planar coprime arrays, based on the theory of ideal lattices. In quadratic number fields, a splitting prime p can be decomposed into the product of two distinct prime ideals, which give rise to the two sparse subarrays. Their virtual difference coarray enjoys a quadratic gain in DOF, thanks to the generalized Chinese Remainder Theorem (CRT). To enlarge the contiguous aperture of the coarray, we present hole-free symmetric CRT arrays with simple closed-form expressions. The ring of Gaussian integers and the ring of Eisenstein integers are considered as examples to demonstrate the procedure of designing coprime arrays. With Eisenstein integers, our design yields a difference coarray that is a subset of the hexagonal lattice, offering a significant gain in DOF over the rectangular lattice, given the same physical areas. Maximization of CRT arrays in the aspect of essentialness and the superior performance in the context of angle estimation will be presented in the companioning Part II.**

***Index Terms*—Array processing, Chinese Remainder Theorem, ideal lattices, sparse arrays.**

I. Introduction

An antenna array is a set of antennas placed in a certain configuration to transmit and/or receive signals. Earlier studies were based on uniform linear arrays (ULAs), uniform rectangular arrays (URAs) and uniform circular arrays (UCAs) by which only a limited number of sources were detected [2], [3].

Previous studies have investigated sparse arrays with $O(N)$ physical sensors for one-dimensional (1D) source estimation such as minimum redundancy arrays (MRAs) [4], nested arrays [5], super nested arrays [6], coprime arrays [7] and coprime arrays with displaced subarrays [8], which offer $O(N^2)$ DOF by exploiting the concept of the virtual coarray. Here the DOF of an array is defined as the number of uncorrelated sources that can be identified by the receiver array. Such arrays can identify more sources than the number of sensors because of the enhanced apertures of coarrays. Particularly, among these arrays, super nested arrays and coprime arrays along with their derivatives significantly alleviate the mutual coupling effect among antennas thanks to the sparse geometries.

In two-dimensional (2D) space, lattices have been well studied in the application of array processing where physical antenna subarrays can be placed on lattices. The virtual coarray is defined as a set of all difference vectors between subarrays. In an example of an antenna system with two subarrays, the cross-difference coarray is defined by

$$\mathcal{D} = \{\mathbf{d} : \mathbf{d} = \mathbf{G}_1\mathbf{x}_2 - \mathbf{G}_2\mathbf{x}_1\},$$

where $\mathbf{G_1x_2}$ and $\mathbf{G_2x_1}$ represent receiver sensor locations; $\mathbf{G}_1$ and $\mathbf{G}_2$ are generator matrices of the subarrays; and $\mathbf{x}_1$ and $\mathbf{x}_2$ are integer vectors [9], [10]. By selecting $\mathbf{G}_1$ and $\mathbf{G}_2$ to be commuting and left coprime integer matrices (i.e., there exist two integer matrices $\mathbf{M}$ and $\mathbf{N}$, such that $\mathbf{G_1M} + \mathbf{G_2N} = \mathbf{I}$, where $\mathbf{I}$ is the identity matrix), a difference coarray can be obtained, whereby the DOF surges to $O(|\det(\mathbf{G}_1\mathbf{G}_2)|)$ with $|\det(\mathbf{G}_1)| + |\det(\mathbf{G}_2)|$ sensors. A method based on Smith Form Decomposition was outlined in [9] to guarantee the coprimality of $\mathbf{G}_1$ and $\mathbf{G}_2$, whereas in [10], the two generator matrices satisfy the relation $\mathbf{G}_1 = \mathbf{G}_2\mathbf{P}$ where $\mathbf{P}$ is a 2-by-2 integer matrix. More recently, [11] derived a novel algorithm from the view of the sum-difference coarray where the coprimality of $\mathbf{G}_1$ and $\mathbf{G}_2$ was guaranteed by extending two orthogonal 1D coprime arrays. Examples of non-lattice based sparse arrays include [12], which redistributed the open-box array [13] to reduce the mutual coupling effect and possess the hole-free property. Nevertheless, the coarray has been restricted to a subset of $\mathbb{Z}$ or $\mathbb{Z}^2$ in previous studies [4]–[12].

This paper along with its companion paper further completes the investigation of coprime array design by means of the Chinese remainder theorem (CRT) over quadratic fields. The classical CRT allows the reconstruction of a rational integer from its remainders by pairwise coprime divisors. A crucial consequence of this theorem is that it can be extended to a general form in ring theory, which allows the computation of algebraic integers by rephrasing the classical CRT in terms of ideals and rings [14]. As a result, the coprime arrays introduced in [7] and [9] can be interpreted as cases of CRT over $\mathbb{Z}$ and over $\mathbb{Z}^2$ respectively. Herein, we relate pairwise coprime algebraic integers to multi-dimensional lattices in Euclidean space through canonical embedding. Specifically, we apply CRT over *rings of algebraic integers* to construct coprime subarrays, which are subsets of *ideal*

This paper was presented in part at International Conference on Sampling Theory and Applications (SAMPTA), Tallinn, Estonia, July 3-7, 2017.

Conghui Li and Cong Ling are with the Department of Electrical and Electronic Engineering, Imperial College London, London, SW7 2AZ, U.K. (e-mail: conghui.li15@imperial.ac.uk; cling@ieee.org).

Lu Gan is with the Department of Electronic and Computer Engineering, Brunel University London, London, UB8 3PH, U.K. (e-mail: lu.gan@brunel.ac.uk).

lattices arising from the prime decomposition. However, the conditions pertaining to the coprimality of algebraic integers and ideal lattices are non-trivial.

This paper shows the connection between coprime algebraic integers and their corresponding lattices that are obtained by embeddings and represented by integer matrices. In general, the coprimality of integer matrices is defined in matrix rings [15], [16]. The class of integer matrices obtained from algebraic integers in this work may be seen as special matrix rings. Principal advantages of relating algebraic integers with matrices include commutativity, simplified expressions and the potential to exploit the nice properties of algebraic integers (e.g., the convenience to check coprimality). For instance, the coprimality issues of some classes of matrices such as adjugate pairs and skew circulant pairs [17], [18] can be addressed as special cases of algebraic conjugate integers. Examples of algebraic integers in *quadratic fields* including *ring of Gaussian integers* and *ring of Eisenstein integers* are studied in this paper.

An important advantage of *Eisenstein integers* is that the difference coarray becomes a subset of the hexagonal lattice A_2. It is well known that A_2 is the optimum lattice for sphere packing in two-dimensional space [19]. Numerical analysis reveals that the optimum packing density results in a 15.5% gain in DOF for a fixed physical area of the array. Due to this reason, the hexagonal geometry is currently used in the design of some phased-array antennas [20], [21]. This paper together with its accompanying paper puts forward the application of hexagonal lattices and hence provides the potential to decrease the physical array aperture without sacrificing DOF.

The main contribution of this paper along with its accompanying paper is that they further develop the design methods of 2D coprime arrays, which brings a new class of 2D array configurations, namely *CRT arrays*. Such arrays can provide enhanced DOF, sparse geometry, and hole-free coarrays. By lattice representations, the configurations of the proposed arrays along with their virtual coarrays enjoy simple closed-form expressions. This paper addresses the issues relating to geometry and the generation of CRT arrays including the mapping between number fields and lattices, coprimality issues pertaining quadratic integers and embedded matrices, and lattice representations of CRT arrays along with their coarrays, whereas the accompanying part II employs CRT arrays to propose practical algorithms for angle estimations in both active and passive sensing scenarios. Other potential applications of Chinese remaindering over quadratic fields include sparse 2D discrete fourier transform [22], the radar measurements on multiple targets [23], [24], filter banks [9], imaging [25], [26] and direction finding problems using compressive sensing [27].

The rest of the paper is organized as follows. Before constructing coprime lattices from prime ideals in Section III, the concepts of quadratic fields and their rings of integers are briefly reviewed in Section II along with algebraic lattices. Based on CRT, Section IV proposes a new class of coprime arrays allocated on coprime lattices and derives closed-form expressions of CRT array geometries, which are inherent in any *rings of algebraic integers*. Section V extends CRT to hole-free symmetric CRT whereby the parameter identifiability is enhanced, after which examples are provided for $\mathbb{Z}^2$ and A_2 as special cases of quadratic integers. Section VI concludes the paper.

Notations: Bold font lowercase letters (e.g., $\mathbf{x}_1$), bold font uppercase letters (e.g., $\mathbf{G}$), fraktur font letters (e.g., $\mathfrak{p}_1$) and calligraphy font alphabets (e.g., $\mathcal{D}$) denote vectors, matrices, principal ideals and sets respectively. $\mathbb{Z}$ and $\mathbb{Q}$ denote rational integers $\{\cdots -1, 0, 1 \cdots\}$ and rational numbers $\{\frac{a}{b} \mid a, b \in \mathbb{Z},\ b \neq 0\}$ respectively. $\mathbb{R}^F$ denotes the F-dimensional Euclidean space. $\mathrm{Re}(m)$ and $\mathrm{Im}(m)$ represent the real and imaginary parts of a complex number m respectively. $\mathrm{N}(m) = m\hat{m}$ denotes the norm of m where $\hat{m}$ is the algebraic conjugate of m (Section II-A). For example in the ring of Gaussian integers, with $m = 3 + 2i$, it can be readily verified that $\mathrm{N}(m) = m\hat{m} = 13$.

II. Review of Quadratic Fields and Algebraic Lattices

Let us first briefly review some definitions and preliminary results related to *quadratic field* along with its *ring of integers*; and based on *algebraic integers*, the construction of *algebraic lattices*, on which sensor arrays can be allocated. [7], [14]

A. Quadratic Field and Its Ring of Integers

A quadratic field K is a field extension of degree 2 over rational numbers $\mathbb{Q}$, i.e., it is a $\mathbb{Q}$-vector space of dimension two. Note that $\mathbb{Q} \subseteq K$. For instance, $\sqrt{-1}$ is not an element in $\mathbb{Q}$ but it is an element in the field extension of $\mathbb{Q}$. In order to be a field, this new field extended from $\mathbb{Q}$ must contain $\mathbb{Q}$ and all the powers and multiples of $\sqrt{-1}$. In other words, $\mathbb{Q}$ is extended into a new vector space over $\mathbb{Q}$, which is generated by the powers of $\sqrt{-1}$. Let $i \triangleq \sqrt{-1}$ and $\mathbb{Q}(i)$ denote this field extension. Every element $m \in \mathbb{Q}(i)$ can be expressed as $m = m_1 + m_2 i$, $m_1, m_2 \in \mathbb{Q}$, i.e., $\{1, i\}$ is the basis of $\mathbb{Q}(i)$. In this case, an *algebraic integer* takes the form of $m_1 + m_2 i$ where $m_1, m_2, \in \mathbb{Z}$. The ring of integers of $\mathbb{Q}(i)$ is the set of all algebraic integers in $\mathbb{Q}(i)$, which can be represented by $\mathbb{Z}[i] = \{m_1 + m_2 i, m_1, m_2, \in \mathbb{Z}\}$.

In general, a quadratic field is denoted by $K = \mathbb{Q}(\sqrt{D})$, where D is a square-free rational integer. Note that if D is a perfect square, $K = \mathbb{Q}$. The ring of integers is often denoted as $\mathcal{O}_K$, which is a set that contains all algebraic integers in K. In quadratic fields, algebraic integers are also known as *quadratic integers* which are roots of quadratic polynomials with coefficients in $\mathbb{Z}$. The minimal polynomial denoted as $f(X)$ of $\mathcal{O}_K$ can be expressed as:

$$f(X) = \begin{cases} X^2 - D, & \text{if } D \not\equiv 1 \pmod 4 \\ X^2 - X + \frac{1-D}{4}, & \text{if } D \equiv 1 \pmod 4, \end{cases} \quad (1)$$

or alternatively,

$$f(X) = X^2 + BX + C, \quad (2)$$

where $B = 0$ and $C = -D$ when $D \not\equiv 1 \pmod 4$, and $B = -1$ and $C = \frac{1-D}{4}$ when $D \equiv 1 \pmod 4$. The proof of $f(X)$ can be found in [14]. Let q and $\hat{q}$ denote the two roots of $f(X)$ respectively. With the notations above, it can be easily calculated that

$$q = -\frac{1}{2}B + \frac{1}{2}\sqrt{B^2 - 4C}, \text{ and} \tag{3}$$

$$\hat{q} = -\frac{1}{2}B - \frac{1}{2}\sqrt{B^2 - 4C} \tag{4}$$

Here $\{1, q\}$ and $\{1, \hat{q}\}$ are called the *integral bases* of $\mathbb{Q}(\sqrt{D})$ [14], i.e., every element in $\mathbb{Q}(\sqrt{D})$ can be written as $m_1 + m_2 q$ corresponding to the former basis or as $m_1 + m_2\hat{q}$ corresponding to the latter with $m_1, m_2 \in \mathbb{Q}$. Accordingly, every element in its ring of integers can be formed by $m = m_1 + m_2 q$ or $\hat{m} = m_1 + m_2\hat{q}$ with $m_1, m_2 \in \mathbb{Z}$. Here $m_1 + m_2 q$ and $m_1 + m_2\hat{q}$ are called *algebraic conjugates* of each other, which can be viewed as a generalization of the complex conjugation. From (3) and (4), it can be verified that with $B^2 - 4C < 0$ ($D < 0$), the two conjugations are identical to each other.

With the knowledge of the integral basis, the ring of integers $\mathcal{O}_K$ can be denoted as $\mathbb{Z}[q]$, and $m = m_1 + m_2 q$ is called a quadratic integer of $\mathbb{Z}[q]$ for any m_1 and m_2 in $\mathbb{Z}$, which generalizes rational integers in $\mathbb{Z}$ to quadratic fields. Note that $q \neq \hat{q}$ since D is square-free, whereas $\mathbb{Z}[q]$ and $\mathbb{Z}[\hat{q}]$ represent the same ring of integers as $\hat{q} = -B - q$. Henceforth, we will use $\mathbb{Z}[q]$ as the notation of the ring of integers of $\mathbb{Q}(\sqrt{D})$.

When $D = -1$, for example, $f(X) = X^2 + 1$ whose roots are $q = i$ and $\hat{q} = -i$. The ring of integers of $\mathbb{Q}(i)$ denoted by $\mathcal{O}_K = \mathbb{Z}[i]$ is also known as the ring of *Gaussian integers*. In this case, $\{1, i\}$ is an integral basis of $\mathbb{Z}[i]$, since $-1 \equiv 3 \pmod 4$. Therefore, every element in $\mathbb{Z}[i]$ can be uniquely expressed as $m_1 + m_2 i$ with $m_1, m_2 \in \mathbb{Z}$. The algebraic conjugation of m is $\hat{m} = m_1 + m_2\hat{q} = m_1 - m_2 i$ which is also the complex conjugation of m. Another example that will be used in this paper for illustrative purposes is the ring of *Eisenstein integers* with $D = -3$. In this case, $\mathcal{O}_K = \mathbb{Z}[\omega]$ with $\{1, \omega\}$ as its integral basis where $\omega = e^{i\pi/3} = \frac{1}{2} + i\frac{\sqrt{3}}{2}$ since $D \equiv 1 \pmod 4$. An arbitrary element in $\mathbb{Z}[\omega]$ can be expressed as $n = n_1 + n_2\omega$ with $\hat{n} = n_1 + n_2\hat{\omega}$ being its algebraic conjugation where $\hat{\omega} = \frac{1}{2} - i\frac{\sqrt{3}}{2}$.

B. Construction of Algebraic Lattices

Definition 1: Given F linearly independent column vectors $\mathbf{g}_1, \mathbf{g}_2, \ldots, \mathbf{g}_F \in \mathbb{R}^F$, an F-dimensional lattice Λ is defined as the set of integer combinations of the basis vectors, *i.e.*,

$$\Lambda = \left\{ \sum_{k=1}^{F} x_k \mathbf{g}_k : x_k \in \mathbb{Z} \right\}.$$

Accordingly, the generator matrix of the lattice Λ is obtained by

$$\mathbf{G} = [\mathbf{g}_1 | \mathbf{g}_2 | \cdots | \mathbf{g}_F].$$

The Voronoi cell of Λ is defined by

$$\mathcal{V}(\Lambda) = \{\mathbf{y} \in \mathbb{R}^F : \|\mathbf{y}\| \leq \|\mathbf{y} - \lambda\|, \forall \lambda \in \Lambda\}, \tag{5}$$

where ties are broken in a systematic manner.

There are various ways to construct lattices, for instance, from codes and groups. In this paper, lattices and their ideals are obtained from rings of quadratic integers $\mathbb{Z}[q]$ via the canonical embedding.

In general, the canonical embedding builds a bridge between lattices and rings of algebraic integers as it establishes a bijective mapping between the elements in an algebraic number field of degree F and the vectors of the F-dimensional Euclidean space. In other words, the canonical embedding σ sends an algebraic integer m to a lattice point $\mathbf{m} = \sigma(m)$ in Euclidean space where $\mathbf{m}$ is an F-by-1 vector. The canonical embedding of any algebraic number field of degree F is given in [28, Definition 5.15].

Herein we consider quadratic fields where $F = 2$. Then the embeddings of $\mathbb{Q}(\sqrt{D})$ are simply given by

$$\sigma_1(\sqrt{D}) = \sqrt{D}, \quad \text{and} \quad \sigma_2(\sqrt{D}) = -\sqrt{D}.$$

The canonical embedding σ is a geometrical representation of $\mathbb{Q}(\sqrt{D})$ that maps $m \in \mathbb{Q}(\sqrt{D})$ to a vector of 2D Euclidean space, i.e., $\sigma(m) = (\sigma_1(m), \sigma_2(m))^T \in \mathbb{R}^2$. For example, the embeddings of an arbitrary element $m = m_1 + \sqrt{2}m_2 \in \mathbb{Q}(\sqrt{2})$ are given by $\sigma_1(m) = m_1 + \sqrt{2}m_2$ and $\sigma_2(m) = m_1 - \sqrt{2}m_2$. Therefore, an algebraic lattice can be constructed by embeddings as follows:

Given $\{1, q\}$ as an integral basis of $\mathbb{Q}(\sqrt{D})$, a 2D *algebraic lattice* $\Lambda = \Lambda(\mathcal{O}_K) = \sigma(\mathcal{O}_K)$ is a lattice whose generator matrix is explicitly given by

$$\mathbf{G} = \begin{pmatrix} 1 & \sigma_1(q) \\ 1 & \sigma_2(q) \end{pmatrix} \text{ for } D > 0, \tag{6}$$

whereas if $D < 0$, $\mathbb{Q}(\sqrt{D})$ is also known as an imaginary quadratic field where the canonical embedding is further simplified and can be formulated by $\sigma(m) = (\mathrm{Re}(m), \mathrm{Im}(m))^T$. Hence the corresponding generator matrix is computed by stacking the real and imaginary parts of 1 and q:

$$\mathbf{G} = \begin{pmatrix} 1 & \mathrm{Re}(q) \\ 0 & \mathrm{Im}(q) \end{pmatrix} \text{ for } D < 0. \tag{7}$$

Note that $\mathbf{G}$ is a non-singular matrix whose absolute determinant equals to the fundamental volume of its corresponding lattice, i.e., $V(\Lambda) = |\det(\mathbf{G})|$ [28, Theorem 5.8].

For example, in the case of $D = -3$ (Eisenstein integers), since the integral basis is $\{1, \omega\}$, the generator matrix of the corresponding algebraic lattice is given by

$$\mathbf{G}_E = \begin{pmatrix} 1 & \mathrm{Re}(\omega) \\ 0 & \mathrm{Im}(\omega) \end{pmatrix} = \begin{pmatrix} 1 & \frac{1}{2} \\ 0 & \frac{\sqrt{3}}{2} \end{pmatrix}. \tag{8}$$

The lattice constructed from $\mathbf{G}_E$ is shown in Fig. 1, which is also known as the hexagonal lattice A_2 with the densest sphere packing in dimension two. The fundamental volume of A_2 is $V(A_2) = \sqrt{3}/2$ with a minimum distance 1.

Analogously, the ring of Gaussian integers gives rise to

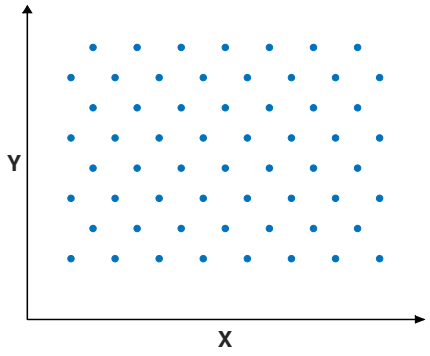


Figure 1. An illustration of A_2 lattice.

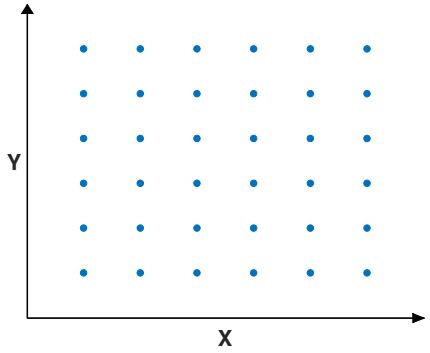


Figure 2. An illustration of $\mathbb{Z}^2$ lattice.

the integer lattice $\mathbb{Z}^2$ whose generator matrix is

$$\mathbf{G}_G = \begin{pmatrix} 1 & \mathrm{Re}(i) \\ 0 & \mathrm{Im}(i) \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{9}$$

Fig. 2 depicts the configuration of $\mathbb{Z}^2$.

In general, given a number field of degree F, its ring of integers $\mathcal{O}_K$ can always construct the algebraic lattice that is expressed by means of the generator matrix. This construction provides a general and straightforward way of finding pairwise coprime matrices from pairwise coprime algebraic integers, which significantly simplifies the method of matrix factorization from Smith form [9], [29] and extends integer matrices in Smith form to any matrices that correspond to coprime elements in $\mathcal{O}_K$.

III. Prime Ideals in Quadratic Fields and Construction of Ideal Lattices

In the previous section, the construction of 2D algebraic lattices from quadratic fields was briefly reviewed. Similar to 1-D arrays [7] where two coprime rational integers in $\mathbb{Z}$ were applied to determine sensor positions, in 2D array design, the quadratic integers in $\mathbb{Z}[q]$ shall be coprime as well, to which Chinese Remainder Theorem applies. Therefore, this section studies prime quadratic integers along with its corresponding prime ideals, from which the algebraic lattices will be constructed. The computation of prime ideals and the issue of coprimality pertaining algebraic conjugates will be addressed. Examples are provided in Gaussian and Eisenstein integers, which will be exploited to design CRT arrays in the following sections.

A. Prime Elements in Quadratic Fields

To distinguish from prime numbers in $\mathbb{Z}$ (e.g., $\pm 2, \pm 3, \pm 5, \pm 7 \cdots$), a non-zero element m in $\mathbb{Z}[q]$ is a *prime element* if and only if it is not a unit of $\mathbb{Z}[q]$ and whenever m divides a product in $\mathbb{Z}[q]$, it also divides one of the factors. Herein, the unit is defined as a quadratic integer $u \in \mathbb{Z}[q]$ with $\mathrm{N}(u) = \pm 1$. In the case of Gaussian integers, there are four units: $\pm 1, \pm i$, and in $\mathbb{Z}[\omega]$, the six units are $\pm 1, (\pm 1 \pm \sqrt{3})/2$.

For example, 7 is a prime number in $\mathbb{Z}$ but not a prime element in $\mathbb{Z}[\omega]$ since it is reducible, i.e., $7 = (1+2\omega)(3-2\omega)$. Analogous to the norm of a complex number, with the notations above, the norm of a quadratic integer $m = m_1 + m_2 q$ in $\mathbb{Z}[q]$ is defined as the product of m and its algebraic conjugate $\hat{m}$, i.e., $\mathrm{N}(m) = m\hat{m}$. As q and $\hat{q}$ are roots of Equation (2), $q + \hat{q} = -B$ and $q\hat{q} = C$. Thus $\mathrm{N}(m)$ can be derived as follows:

$$\begin{aligned} \mathrm{N}(m) &= m\hat{m} = (m_1 + m_2 q)(m_1 + m_2 \hat{q}) \\ &= m_1^2 + m_1 m_2 (q + \hat{q}) + m_2^2 q\hat{q} = m_1^2 - B m_1 m_2 + C m_2^2. \end{aligned} \tag{10}$$

Since $m_1, m_2, B, C \in \mathbb{Z}$, the norm of a quadratic integer is always in $\mathbb{Z}$. In general, for all $m \in \mathbb{Z}[q]$, it can be verified from [30, Theorem 1.8] that if $\mathrm{N}(m)$ is a prime number in $\mathbb{Z}$, then m is a prime element. In the cases of Gaussian and Eisenstein primes, the sufficient and necessary conditions of prime elements can be derived [31].

A *Gaussian prime* is a prime element in the ring of Gaussian integers of the form $m_1 + m_2 i$ that satisfies one of the following:

- Both m_1 and m_2 are nonzero and $\mathrm{N}(m) = m_1^2 + m_2^2$ is a prime number.
- $m_1 = 0$ and $m_2 \neq 0$ (or $m_1 \neq 0$ and $m_2 = 0$), m_2 is a prime number and $|m_2| \equiv 3 \pmod 4$ (or m_1 is a prime number and $|m_1| \equiv 3 \pmod 4$).

In $\mathbb{Z}[\omega]$, an Eisenstein integer of the form $n = n_1 + n_2\omega$ is a *Eisenstein prime* if either:

- $n_1 + n_2\omega$ equals to the product of a unit and a prime number of the form $3a - 1$, $a \in \mathbb{Z}$, or
- $\mathrm{N}(n) = n_1^2 + n_1 n_2 + n_2^2$ is a prime number.

For example, $2+i$ is a Gaussian prime because $1^2+2^2 = 5$ is a prime number. Likewise, $2+\sqrt{3}i = 1+2\omega$ is a Eisenstein prime since $1^2 + 2 + 2^2 = 7$ is a prime number.

B. Prime Factorization into Ideals

An *ideal* $\mathcal{I}$ in a quadratic field is a subset of $\mathbb{Z}[q]$ such that whenever $x \in \mathcal{I}$ and $m \in \mathbb{Z}[q]$, mx belongs to $\mathcal{I}$. If the ideal is generated by a single element in $\mathbb{Z}[q]$, this ideal is called a *principal ideal*. For instance, $5\mathbb{Z}$ of $\mathbb{Z}$ is a principal ideal whose elements are $\pm 5, \pm 10 \pm 15 \cdots$. For simplicity,

we can write $5\mathbb{Z} = \langle\, 5 \,\rangle$. Similar to the prime elements in $\mathbb{Z}[q]$ mentioned in Section III-A, a *prime ideal* is an ideal such that $mn \in \mathcal{I}$ implies $m \in \mathcal{I}$ or $n \in \mathcal{I}$. In a *principal ideal domain* (PID) where every ideal is principal, prime ideals are simply generated by prime elements. All quadratic fields with class number one are PIDs. It has been proved that the PIDs in imaginary quadratic fields are $\mathbb{Q}(\sqrt{D})$, for $D = -1, -2, -3, -7, -11, -19, -43, -67, -163$, while the full list of PIDs in real quadratic fields is not known yet. Examples include $D = 2, 3, 5, 6, 7, 11, 13, 14, 17, 19 \cdots$ [32]. For simplicity, we only consider PIDs henceforth. For example, $\langle\, 2 + \sqrt{3}i \,\rangle$ is a prime ideal of the ring of integers of $\mathbb{Q}(\sqrt{-3})$, namely $\mathbb{Z}[\omega]$, since $\mathbb{Q}(\sqrt{-3})$ is a PID and $2 + \sqrt{3}i$ is a prime element (Section III-A). The elements in $\langle\, 2 + \sqrt{3}i \,\rangle$ are in the set $\langle\, 2 + \sqrt{3}i \,\rangle = \langle\, 2 + \sqrt{3}i \,\rangle\mathbb{Z}[\omega] = \{(2 + \sqrt{3}i)m : m \in \mathbb{Z}[\omega]\}$.

Similar to the fundamental theorem of arithmetic to rational integers [16, Theorem 5.3], every non-zero element in a unique factorization domain (UFD) can be written as a product of prime elements. More generally, a nonzero ideal $\langle\, p \,\rangle$ of $\mathcal{O}_K$ where $K = \mathbb{Q}(\sqrt{D})$ can be uniquely factored as

$$\langle\, p \,\rangle = \prod_{k=1} \mathfrak{p}_k^{\alpha_k} \tag{11}$$

where $\mathfrak{p}_k$'s are distinct prime ideals. Particularly, if p is a rational prime greater than 2, then [14]

$$\langle\, p \,\rangle = p\mathcal{O}_K = \begin{cases} \mathfrak{p}_1\mathfrak{p}_2, & \text{if } \left(\frac{D}{p}\right) = 1; \\ \mathfrak{p}, & \text{if } \left(\frac{D}{p}\right) = -1; \\ \mathfrak{p}^2, & \text{if } p|D. \end{cases} \tag{12}$$

where $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are distinct prime ideals, and $\left(\frac{a}{p}\right)$ is the Legendre symbol defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if for some } x \in \mathbb{Z}\text{: } a \equiv x^2 \pmod{p}, \\ -1 & \text{otherwise.} \end{cases}$$

In the first case where p *splits*, $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are distinct prime ideals of norm p, thus they are coprime by nature. Particularly in PIDs, the primality of these two ideals can be tested using the criteria given in Section III-A. Based on $\mathfrak{p}_1$ and $\mathfrak{p}_2$, two coprime ideal lattices can be constructed whereby two subarrays can be allocated on respectively.

C. Coprime Ideal lattices and their matrix representations

In general, an *ideal lattice* $\Lambda_1 = \sigma(\mathcal{I})$ is constructed by canonical embedding from an ideal $\mathcal{I} \subseteq \mathcal{O}_K$, which is a sublattice of the algebraic lattice Λ constructed from $\mathcal{O}_K$. For example, $7A_2$ is an ideal lattice constructed from the ideal $\langle\, 7 \,\rangle \subset \mathbb{Z}[\omega]$, thus it is a sublattice of A_2 constructed from $\mathbb{Z}[\omega]$.

In $\mathbb{Z}[q]$, an integral basis of the principal ideal $\langle\, m \,\rangle$ generated by the quadratic integer $m = m_1 + m_2 q$ can be calculated as

$$\begin{aligned} m\{1, q\} &= \{m_1 + m_2 q, (m_1 + m_2 q)q\} \\ &= \{m_1 + m_2 q, -Cm_2 + q(m_1 - Bm_2)\}. \end{aligned}$$

The canonical embedding of a principal ideal maps the elements in the ideal to lattice points, which are similar to that of $\mathcal{O}_K$ defined in (6) and (7) for $D > 0$ and $D < 0$ respectively. Therefore, an ideal lattice denoted as $\sigma(\mathfrak{p})$ that is generated by a principal ideal $\mathfrak{p} = \langle\, m \,\rangle$ has a generator matrix given by

$$\mathbf{G}_m = \mathbf{G}\mathbf{B}_m, \text{ where} \tag{13}$$

$$\mathbf{B}_m = \begin{pmatrix} m_1 & -Cm_2 \\ m_2 & m_1 - Bm_2 \end{pmatrix}. \tag{14}$$

Here $\mathbf{G}$ is the generator matrix of $\mathcal{O}_K$ that expressed in (6) or (7) for real or imaginary quadratic field respectively. $\mathbf{B}_m$ is called the *matrix representation* of $m \in \mathbb{Z}[q]$ and $|\det(\mathbf{B}_m)| = \mathrm{N}(m)$ [28, Theorem 5.11]. Note that $\mathbf{B}_m$ is always an integer matrix by definition, i.e., all entries in $\mathbf{B}_m$ are rational integers. The following two lemmas discuss the properties of $\mathbf{B}_m$ from the perspectives of eigenvectors/eigenvalues and commutativity respectively.

Lemma 1: $(1,\ q)$ and $(1,\ \hat{q})$ are left row eigenvectors of $\mathbf{B}_m$ with eigenvalues m and $\hat{m}$ respectively.

Proof: The row vector $(1,\ q)$ is a left eigenvector of $\mathbf{B}_m$ if $(1,\ q)\mathbf{B}_m = m(1,\ q)$ [33, Definition 4.2]. Substituting (14) to the left hand side of the equation results in

$$\begin{aligned} &(1,\ q)\begin{pmatrix} m_1 & -Cm_2 \\ m_2 & m_1 - Bm_2 \end{pmatrix} \\ &= \big(m_1 + m_2 q,\ m_1 q + m_2(-Bq - C)\big) \end{aligned}$$

As q is the root of $f(X) = 0$ where $f(X)$ is given in (2), it satisfies $q^2 + Bq + C = 0$. Then the second element in the row vector becomes $m_1 q + m_2 q^2 = (m_1 + m_2 q)q = mq$. Likewise, substituting $\hat{q}^2 = -B\hat{q} - C$ and $\hat{m} = m_1 + m_2\hat{q}$ to $(1,\ \hat{q})\mathbf{B}_m$ yields $(1,\ \hat{q})\mathbf{B}_m = \hat{m}(1,\ \hat{q})$. ■

Lemma 2: Any two matrix representations of quadratic integers are commutative.

Proof: By the eigendecomposition discussed in Lemma 1, any two matrix representations $\mathbf{B}_m$ and $\mathbf{B}_n$ of two quadratic integers m and n respectively can be factorized as

$$\mathbf{B}_m = \mathbf{Q}^{-1}\mathbf{P}_m\mathbf{Q} \text{ and } \mathbf{B}_n = \mathbf{Q}^{-1}\mathbf{P}_n\mathbf{Q} \tag{15}$$

where

$$\mathbf{Q} = \begin{pmatrix} 1 & q \\ 1 & \hat{q} \end{pmatrix}, \mathbf{P}_m = \begin{pmatrix} m & 0 \\ 0 & \hat{m} \end{pmatrix} \text{ and } \mathbf{P}_n = \begin{pmatrix} n & 0 \\ 0 & \hat{n} \end{pmatrix} \tag{16}$$

Therefore, by Lemma 1 we can write

$$\begin{aligned} &\mathbf{B}_m\mathbf{B}_n = \mathbf{Q}^{-1}\mathbf{P}_m\mathbf{Q}\mathbf{Q}^{-1}\mathbf{P}_n\mathbf{Q} = \mathbf{Q}^{-1}\mathbf{P}_m\mathbf{P}_n\mathbf{Q} \\ &= \mathbf{Q}^{-1}\mathbf{P}_n\mathbf{P}_m\mathbf{Q} = (\mathbf{Q}^{-1}\mathbf{P}_n\mathbf{Q})(\mathbf{Q}^{-1}\mathbf{P}_m\mathbf{Q}) = \mathbf{B}_n\mathbf{B}_m. \end{aligned}$$

■

In other words, the commutativity of algebraic integers implies the commutativity of the corresponding matrices. Next, we will relate the coprimality of quadratic integers with the coprimality of their corresponding matrix representations and provide an alternative way of generating coprime lattices from algebraic conjugate pairs.

D. Connection with coprime algebraic integers

In general, the left coprimality of integers matrices is defined by Bezout's identity [16]–[18]:

Definition 2: Two integer matrices $\mathbf{B}_m$ and $\mathbf{B}_n$ are left coprime if and only if there exist integer matrices $\mathbf{C}$ and $\mathbf{D}$ such that

$$\mathbf{B}_m\mathbf{C} + \mathbf{B}_n\mathbf{D} = \mathbf{I}. \tag{17}$$

Likewise, $\mathbf{B}_m$ and $\mathbf{B}_n$ are right coprime if and only if there exist $\mathbf{C}'$ and $\mathbf{D}'$ such that $\mathbf{C}'\mathbf{B}_m + \mathbf{D}'\mathbf{B}_n = \mathbf{I}$.

Theorem 1: In PIDs, two algebraic integers are coprime if and only if their corresponding matrix representations obtained from canonical embeddings are left coprime.

Proof: See Appendix A ■

Corollary 1: Two integers matrices generated from embeddings are right coprime if and only if they are left coprime.

Proof: See Appendix B ■

From Theorem 1 and Proposition 1, the coprimality of two quadratic integers indicates the right and left coprimality of their corresponding matrix representations obtained from embeddings and vice versa. Henceforth, we say two lattices are *coprime lattices* if their matrix representations are (left and right) coprime. Exploiting this theorem, we will provide conditions on the coprimality of adjugate matrix pairs next.

E. Adjugate Matrix Pairs

Since the notion of greatest common divisor (GCD) can be generalized to an arbitrary commutative ring, it can be defined in the rings of integers of quadratic fields as well [34], [35]. Herein, the concept of GCD is generalized to quadratic integers in PIDs, i.e., if $d = \text{GCD}(m, n)$ is a GCD of m and n, then all the common divisors of m and n divide d [34, Definition 6.1.3]. Similarly, the Bezout's identity can also be generalized as if two integers $m, n \in \mathbb{Z}[q]$ are not both equal to 0 then there exist $\alpha, \beta \in \mathbb{Z}[q]$ such that

$$\text{GCD}(m, n) = \alpha m + \beta n.$$

Given $\text{GCD}(m, n) = u$ where u is the unit in $\mathbb{Z}[q]$ and $\text{N}(u) = 1$, m and n are defined as *coprime quadratic integers* [34, Definition 6.1.4]. In other words, two quadratic integers m and n are coprime if and only if there exist α' and β' such that $m\alpha' + n\beta' = u$. Because u is a unit, u^{-1} always exists. Then Bezout's identity becomes $m\alpha + n\beta = 1$ where $\alpha = \alpha' u^{-1}$ and $\beta = \beta' u^{-1}$. Recall that the following facts of GCD hold for $a, b, c \in \mathbb{Z}[q]$:

1) $\text{GCD}(a, b) = \text{GCD}(a + \alpha b, b)$, $\forall \alpha \in \mathbb{Z}[q]$;
2) $\text{GCD}(a, b) = 1$ if and only if $\text{GCD}(a^\alpha, b^\beta) = 1$, $\forall \alpha, \beta \in \mathbb{Z}^+$.
3) $\text{GCD}(a, bc) = 1$ if and only if $\text{GCD}(a, b) = 1$ and $\text{GCD}(a, c) = 1$.

These facts can be proved straightforward and will be employed in the following proofs of coprimality.

As mentioned in Section II-A, the algebraic conjugate of m denoted by $\hat{m}$ is also in $\mathbb{Z}[q]$ and can be written as $m_1 + m_2\hat{q}$. The matrix generated by $\hat{m}$ is the same as the adjugate of $\mathbf{B}_m$, which is the transpose of the cofactor matrix of $\mathbf{B}_m$, i.e., $adj(\mathbf{B}_m)_{kj} = (-1)^{k+j}\mathbf{M}_{jk}$ where $\mathbf{M}_{jk}$ is the determinant of the matrix that results from deleting row k and column j of $\mathbf{B}_m$. Therefore, in the dimension of two, the adjugate of $\mathbf{B}_m$ is

$$\mathbf{B}_{\hat{m}} = \begin{pmatrix} m_1 - Bm_2 & Cm_2 \\ -m_2 & m_1 \end{pmatrix}. \tag{18}$$

Theorem 2: Using the notations above, two adjugate 2-by-2 matrices $\mathbf{B}_m$ and $\mathbf{B}_{\hat{m}}$ are coprime if and only if

(a) $\text{GCD}(m_1, m_2) = 1$ and $\text{GCD}(2m_1 + m_2,\ 4C - 1) = 1$, for $B = -1$,
(b) $\text{GCD}(m_1, m_2) = 1$ and $\text{GCD}(m_1,\ C) = 1$, for $B = 0$ and C is even,
(c) $\text{GCD}(m_1 + m_2, m_1 - m_2) = 1$ and $\text{GCD}(m_1,\ C) = 1$ for $B = 0$ and C is odd.

Proof: See Appendix C ■

It is worth to notice that according to Theorem 1, Theorem 2 also provides the coprime conditions of two algebraic conjugates $m = m_1 + m_2 q$ and $\hat{m} = m_1 + m_2\hat{q}$ where q and $\hat{q}$ are given in (3) and (4) respectively. For illustration purposes, two examples of algebraic conjugate integers are given, providing two classes of coprime matrices.

Corollary 2: A Gaussian integer m and its conjugate are relatively prime if and only if $\text{GCD}(m_1 + m_2, m_1 - m_2) = 1$.

Proof: The minimum polynomial of the ring of Gaussian integers is $X^2 + 1 = 0$ with the basis $\{1, i\}$. By Theorem 2, $B = 0$ and $C = 1$ match the assumptions of case (c), thus the coprimality condition becomes $\text{GCD}(m_1 + m_2, m_1 - m_2) = 1$ and $\text{GCD}(m_1, 1) = 1$. Note that $\text{GCD}(m_1, 1) = 1$ holds for all $m_1 \in \mathbb{Z}$. ■

Corollary 3: An Eisenstein integer and its conjugate are relatively prime if and only if $\text{GCD}(m_1, m_2) = 1$ and $\text{GCD}(m_1 - m_2, 3) = 1$.

Proof: Likewise, in the case of $\mathbb{Z}[\omega]$, the coefficients become $C = 1$ and $B = -1$, which can be addressed to case (a) in Theorem 2. The coprime conditions are $\text{GCD}(m_1, m_2) = 1$ and $\text{GCD}(2m_1 + m_2, 3) = 1$. By Fact (1), $\text{GCD}(m_1, m_2) = 1$ is equivalent to $\text{GCD}(2m_1 + m_2, m_1) = 1$, which can be combined with the second condition by Fact (3), i.e., $\text{GCD}(2m_1 + m_2, 3m_1) = 1$. Applying Fact (1) again results in $\text{GCD}(3m_1 - (2m_1 + m_2), 3m_1) = \text{GCD}(m_1 - m_2, 3) = 1$, which holds if and only if both $\text{GCD}(m_1, m_2) = 1$ and $\text{GCD}(m_1 - m_2, 3) = 1$ hold. ■

Remark: By Theorem 2, the class of coprime matrix pairs is enriched to any matrices obtained from quadratic integers. By exploiting the bijective mappings between algebraic integers and integer matrices, [17, Theorem 2] can be viewed as the coprimality of two algebraic conjugates and proved by the generalized GCD, i.e.,

$$\begin{aligned} &\text{GCD}(m_1 + m_2 q,\ m_1 + m_2\hat{q}) \\ &= \text{GCD}\big((m_1 + m_2 q)(m_1 + m_2\hat{q}),\ 2m_1 + m_2(q + \hat{q})\big) \\ &= \text{GCD}(\text{N}(m), 2m_1 - Bm_2). \end{aligned}$$

According to the coprimality relation between quadratic integers and matrices stated in Theorem 1, some useful classes of coprime matrices such as skew-circulant adjugates

derived in [18] can be viewed as a case of Corollary 2 with canonical embedding, i.e., the following two integer matrices

$$\mathbf{B}_m = \begin{pmatrix} m_1 & -m_2 \\ m_2 & m_1 \end{pmatrix} \quad \text{and} \quad \mathbf{B}_{\hat{m}} = \begin{pmatrix} m_1 & m_2 \\ -m_2 & m_1 \end{pmatrix}$$

are coprime if and only if GCD$(m_1 + m_2,\, m_1 - m_2) = 1$. Similarly, an alternative way of describing Corollary 3 would be as follows:

Two integer matrices

$$\mathbf{B}_m = \begin{pmatrix} m_1 & -m_2 \\ m_2 & m_1 + m_2 \end{pmatrix} \quad \text{and}$$

$$\mathbf{B}_{\hat{m}} = \begin{pmatrix} m_1 + m_2 & m_2 \\ -m_2 & m_1 \end{pmatrix}$$

are coprime if and only if GCD$(m_1,\, m_2) = 1$ and GCD$(m_1 - m_2,\, 3) = 1$, i.e., m_1 and m_2 are relatively prime with their difference being not divisible by 3.

IV. Design of CRT-based Sparse Arrays

We have proved that the coprimality of quadratic integers in PIDs is a necessary and sufficient condition of the coprimality of the corresponding matrices obtained from canonical embeddings. In this section, we will briefly review the generalized CRT based on [14, Appendix 1], and then propose a design method for coprime arrays based on CRT over rings of quadratic integers where the sensors are deployed by the use of coprime lattices generated by coprime ideals. For illustrative purposes, CRT is employed over the ring of Gaussian integers and the ring of Eisenstein integers respectively as examples.

To begin with, we extend the modulo operation to ideals, and define the sum and the product of ideals as follows:

Definition 3: Let $\mathcal{I}$ be an ideal of a ring R. Given $x, y \in R$, x is congruent to y modulo $\mathcal{I}$, i.e., $x \equiv y \mod \mathcal{I}$ if and only if

$$x - y \in \mathcal{I}. \tag{19}$$

Definition 4: Let $\mathcal{I}$ and $\mathcal{J}$ be two ideals of the ring R. The sum of $\mathcal{I}$ and $\mathcal{J}$ is the ideal

$$\mathcal{I} + \mathcal{J} = \{x + y, x \in \mathcal{I}, y \in \mathcal{J}\},$$

and their product is the ideal

$$\mathcal{I}\mathcal{J} = \{\sum x_k y_j, x_k \in \mathcal{I}, y_j \in \mathcal{J}\}.$$

The quotient ring is defined as the set that contains all the cosets of the ideal $\mathcal{I}$, i.e., $R/\mathcal{I} = \{r + \mathcal{I}, r \in R\}$. Let ideals $\mathcal{I}$ and $\mathcal{J}$ be relatively prime in a commutative ring R, then $\mathcal{I} + \mathcal{J} = R$. For example, given $\mathcal{I} = \langle 3 \rangle$ and $\mathcal{J} = \langle 5 \rangle$ as two coprime ideals of $\mathbb{Z}$, $\mathcal{I} + \mathcal{J} = \langle 3 \rangle + \langle 5 \rangle = \langle 3 \cdot 2 + 5 \cdot (-1) \rangle = \langle 1 \rangle = \mathbb{Z}$, $\mathcal{I}\mathcal{J} = \langle 15 \rangle$, and $R/\mathcal{I} = \mathbb{Z}/3\mathbb{Z} = \{0, 1, 2\}$ which is an equivalence class with $[x] = [y]$ if and only if $x - y \in \langle 3 \rangle$.

The Chinese Remaindering Theorem [14] asserts that there is a ring isomorphism

$$R/\mathcal{I}\mathcal{J} \simeq R/\mathcal{I} \times R/\mathcal{J}. \tag{20}$$

This implies that for all $a_k \in R/\mathcal{I}$ and $b_j \in R/\mathcal{J}$ there exists $z \in R/\mathcal{I}\mathcal{J}$ such that

$$\begin{aligned} z &\equiv a_k \pmod{\mathcal{I}} \text{ and} \\ z &\equiv b_j \pmod{\mathcal{J}}, \end{aligned} \tag{21}$$

which can also be proved as follows: from coprimality that $\mathcal{I} + \mathcal{J} = R$, there exist $x_k \in \mathcal{I}$ and $y_j \in \mathcal{J}$ such that $x_k + y_j = 1$. For all $a_k \in R/\mathcal{I}$ and $b_j \in R/\mathcal{J}$, it can be readily verified that every pair (a_k, b_j) forms the solution

$$z \equiv x_k b_j + y_j a_k \pmod{\mathcal{I}\mathcal{J}}. \tag{22}$$

We may check that

$$\begin{aligned} z &\equiv y_j a_k \equiv x_k a_k + y_j a_k = (x_k + y_j) a_k \equiv a_k \pmod{\mathcal{I}} \\ z &\equiv x_k b_j \equiv x_k b_j + y_j b_j = (x_k + y_j) b_j \equiv b_j \pmod{\mathcal{J}}. \end{aligned}$$

The pair (x_k, y_j) serves as a "CRT basis" which can be chosen as the basis of prime ideals in $\mathbb{Z}[q]$. With this basis, the mapping from $R/\mathcal{I} \otimes R/\mathcal{J}$ to $R/\mathcal{I}\mathcal{J}$ is bijective, i.e., all solutions of z are identical given the different pairs (a_k, b_j), which leads to the definition of CRT arrays and its cross-difference and sum coarrays:

Definition 5 (CRT arrays): Given two coprime ideals $\mathcal{I}$ and $\mathcal{J}$ in ring R, a CRT-based array is defined as:

$$\mathcal{Z} = \sigma(\mathcal{I})/\sigma(\mathcal{I}\mathcal{J}) \cup \sigma(\mathcal{J})/\sigma(\mathcal{I}\mathcal{J}), \tag{23}$$

where $\sigma(\mathcal{I})$ denotes the canonical embedding of $\mathcal{I}$ and same with $\mathcal{J}$.

Definition 6 (Cross-difference coarrays of CRT arrays): The cross-difference coarray $\mathcal{D}$ generated by an CRT array is given by:

$$\mathcal{D} = \{\mathbf{z}_1 - \mathbf{z}_2 \mid \mathbf{z}_1 \in \sigma(\mathcal{I})/\sigma(\mathcal{I}\mathcal{J}), \mathbf{z}_2 \in \sigma(\mathcal{J})/\sigma(\mathcal{I}\mathcal{J})\}.$$

Definition 7 (Sum coarray of CRT arrays): The sum coarray $\mathcal{S}$ generated by an CRT array can be expressed as:

$$\mathcal{S} = \{\mathbf{z}_1 + \mathbf{z}_2 \mid \mathbf{z}_1 \in \sigma(\mathcal{I})/\sigma(\mathcal{I}\mathcal{J}), \mathbf{z}_2 \in \sigma(\mathcal{J})/\sigma(\mathcal{I}\mathcal{J})\}.$$

Note that because of the symmetry of the ideal lattices, $\mathcal{D}$ is identical to $\mathcal{S}$. From the point of view that regards lattices as sets of points, $\sigma(\mathcal{I})/\sigma(\mathcal{I}\mathcal{J})$ corresponds to $\mathcal{I}/(\mathcal{I}\mathcal{J})$ in number fields.

According to [14], the ring isomorphism (20) holds over any commutative ring, therefore over all PIDs where the ideals can be obtained from the prime decomposition (12). Given $\mathcal{I} = \mathfrak{p}_1 = \langle m \rangle$ and $\mathcal{J} = \mathfrak{p}_2 = \langle n \rangle$ where $m, n \in \mathbb{Z}[q]$, the canonical embedding $\sigma(\mathfrak{p}_1)$ of $\mathfrak{p}_1$ is given in (13) and similar with $\sigma(\mathfrak{p}_2)$. The product of these two ideals forms a principal ideal as well, i.e., $\mathcal{I}\mathcal{J} = \langle mn \rangle = \langle p \rangle$. With the notations above, expressions for the number of sensors and the achievable DOF can be derived as follows:

Proposition 1: If $\mathcal{I}$ and $\mathcal{J}$ that are used to allocate sensors are decomposed from $\langle p \rangle$, the total number of physical sensors is $2p - 1$ and its maximum DOF is p^2.

Proof: By assumption $\mathcal{I}\mathcal{J} = \langle p \rangle = pR$, the number of elements in $\mathcal{I}/pR$ is p which is the same as $\mathcal{J}/pR$ [28, Definition 3.12]. Since the only identical element that they share is $\mathbf{0}$, the total number of nonidentical elements in $(\mathcal{I}/pR) \cup (\mathcal{J}/pR)$ is $2p - 1$.

Define the maximum DOF as the maximum number of degrees of freedom that the array can achieve, i.e., the total

number of identical elements in the coarray. According to the ring isomorphism of the generalized CRT given in (20), all the difference/sum vectors generated by coprime lattices are nonidentical, thus the total number of elements in $(\mathcal{I}+\mathcal{J})/pR$ can be written as:

$$|\mathcal{I}/pR| \cdot |\mathcal{J}/pR| = p^2, \tag{24}$$

where $|\cdot|$ is the cardinality of a set. Note that as canonical embedding $\sigma(\cdot)$ is bijective, the number of lattice points in $\sigma(\mathcal{J})/\sigma(\mathcal{I}\mathcal{J})$ is the same as the number of elements in $\mathcal{J}/\mathcal{I}\mathcal{J}$ ■

The rest of this section will demonstrate the proposed design method by Chinese Remaindering over PIDs in quadratic fields, namely over $\mathbb{Z}[i]$ and $\mathbb{Z}[\omega]$.

A. Chinese Remaindering over $\mathbb{Z}[i]$

In the ring of Gaussian integers, we look for the p such that $D=-1$ is a quadratic residue:

$$x^2 \equiv -1 \pmod{p}$$

for some $x \in \mathbb{Z}$. The first few solutions are $2^2 \equiv -1 \pmod 5$, $5^2 \equiv -1 \pmod{13}$, and so forth. By performing the prime decomposition (12), these rational primes can be decomposed into prime ideals as $\langle 5\rangle = \langle 2+i\rangle\langle 2-i\rangle$, and $\langle 13\rangle = \langle 3+2i\rangle\langle 3-2i\rangle$. Here all the quadratic integers are Gaussian primes as stated in the criteria given in Section III-A. Alternatively, it can be checked that all pairs are relatively prime according to Corollary 2. Let us take the example of $p=5$ to demonstrate the design procedure. $p=5$ yields two prime ideals $\mathfrak{p}_1 = \langle 2+i\rangle$ and $\mathfrak{p}_2 = \langle 2-i\rangle$, whose corresponding matrices are coprime as well by Theorem 1. As $\{1,i\}$ is the integral basis of $\mathbb{Z}[i]$, an integral basis of $\langle 2+i\rangle$ can be calculated as

$$(2+i)\{1,i\} = \{2+i, -1+2i\}.$$

Since the minimum polynomial over $\mathbb{Z}[i]$ is X^2+1 ($B=0$ and $C=1$), by canonical embedding given as (13) and (14), the generator matrix of $\langle 2+i\rangle$ is

$$\mathbf{G}_{(2+i)} = \begin{pmatrix} 2 & -1 \\ 1 & 2 \end{pmatrix}. \tag{25}$$

Notice that because $\mathbf{G}=\mathbf{I}$, the generator matrix of $\langle 2+i\rangle$ is identical to its matrix representation, i.e., $\mathbf{G}_{(2+i)} = \mathbf{B}_{(2+i)}$. Analogously, an integral basis of $\langle 2-i\rangle$ is given by

$$(2-i)\{1,i\} = \{2-i, 1+2i\},$$

whose generator matrix is

$$\mathbf{G}_{(2-i)} = \begin{pmatrix} 2 & 1 \\ -1 & 2 \end{pmatrix}. \tag{26}$$

The determinant of $\mathbf{G}_{(2+i)}$ is equivalent to the norm of $\langle 2+i\rangle$ and same with $\mathbf{G}_{(2-i)}$ and $\langle 2-i\rangle$ [28]. By the definition of the norm (10), it can be proved straightforward that if $\langle p\rangle = \langle 2+i\rangle\langle 2-i\rangle$, $\mathrm{N}(\langle 2+i\rangle)\mathrm{N}(\langle 2-i\rangle) = \mathrm{N}(p)$ and since p is a prime number, $\mathrm{N}(p)=p^2$ has and only has three divisors, namely 1, p, and p^2. According to the decomposition shown in (12), both $\langle 2+i\rangle$ and $\langle 2-i\rangle$ are not units. This implies $|\det(\mathbf{G}_{(2+i)})| = |\det(\mathbf{G}_{(2-i)})| = \mathrm{N}(\langle 2+i\rangle) = \mathrm{N}(\langle 2-i\rangle) = p = 5$.

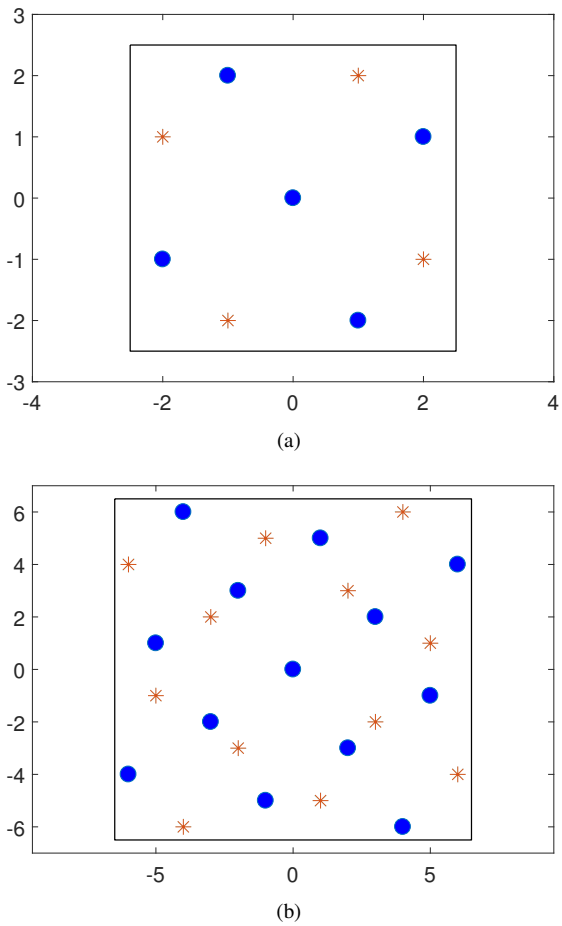


Figure 3. $\mathbb{Z}^2$ arrays in the Voronoi cells (black polygons) constructed from decomposition over Gaussian integers of $p=5$ (a) and $p=13$ (b) with the first subarray ($\mathbf{G}_{(2+i)}\mathbf{g_1}$) in red stars and the second subarray ($\mathbf{G}_{(2-i)}\mathbf{g_2}$) in blue dots.

Using the matrix representation, the cross-difference coarray consisting of vectors can be defined by

$$\mathcal{D}_G = \{\mathbf{d}_g : \mathbf{d}_g = \mathbf{G}_{(2-i)}\mathbf{g}_1 - \mathbf{G}_{(2+i)}\mathbf{g}_2\},$$

where $\mathbf{g}_1 \in \mathbb{Z}^2/\sigma\big(\langle 2+i\rangle\big)$ and $\mathbf{g}_2 \in \mathbb{Z}^2/\sigma\big(\langle 2-i\rangle\big)$. $\mathbf{G}_{(2+i)}$ and $\mathbf{G}_{(2-i)}$ are given by (25) and (26) respectively and they are coprime because $2+i$ and $2-i$ are coprime integers (Theorem 1). According to the ring isomorphism of the generalized CRT, with $R=\mathbb{Z}$, $\mathcal{I}=\langle 2+i\rangle$ and $\mathcal{J}=\langle 2-i\rangle$, it can be readily calculated that $\mathcal{I}\mathcal{J} = \langle 5\rangle = 5\mathbb{Z}$ and thus $\mathbf{d}_g \in \mathbb{Z}^2/5\mathbb{Z}^2$, yielding an array of $5^2=25$ degrees of freedom according to Proposition 1. The locations of the elements of the first subarray are given by

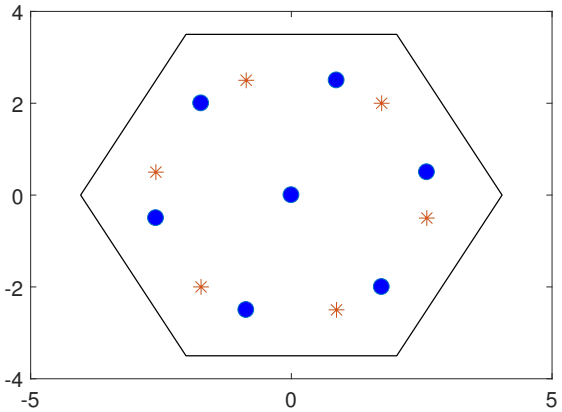
$$\mathbf{G}_{(2-i)}\mathbf{g}_1 \in \sigma\big(\langle 2-i\rangle\big)/5\mathbb{Z}^2,$$

while those of the second subarray are given by

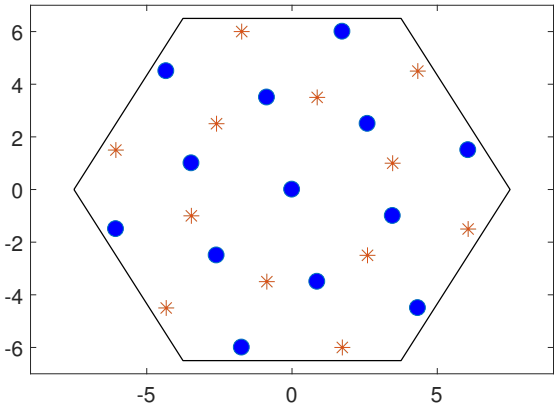
$$\mathbf{G}_{(2+i)}\mathbf{g}_2 \in \sigma\big(\langle 2+i\rangle\big)/5\mathbb{Z}^2.$$

Therefore, $\mathcal{Z} = \sigma\big(\langle 2-i\rangle\big)/5\mathbb{Z}^2 \cup \sigma\big(\langle 2+i\rangle\big)/5\mathbb{Z}^2$ and only 9 elements are actually used in the sparse array by Proposition 1.

Another example that comprises more sensors is $p=13$,



(a)



(b)

Figure 4. A_2 arrays in the Voronoi cells (black polygons) constructed from decomposition of $p = 7$ (a) and $p = 13$ (b) over Eisenstein integers.

where two coprime ideals $\langle 3 + 2i \rangle$ and $\langle 3 - 2i \rangle$ can be obtained from (12). The generator matrices of the corresponding ideal lattices are given by

$$\mathbf{G}_{(3+2i)} = \begin{pmatrix} 3 & -2 \\ 2 & 3 \end{pmatrix}, \text{ and } \mathbf{G}_{(3-2i)} = \begin{pmatrix} 3 & 2 \\ -2 & 3 \end{pmatrix}.$$

This coprime array produces $13^2 = 169$ DOFs from $13 \times 2 - 1 = 25$ physical sensors according to Proposition 1.

Since $\mathbb{Z}[i]$ is isomorphic to polynomial ring $\mathbb{Z}[x]/(x^2+1)$ that gives rise to skew-circulant matrices, the sensor arrays obtained from skew-circulant matrices in [9] can be viewed as CRT arrays over $\mathbb{Z}[i]$. Symmetric Voronoi regions $\mathcal{V}(p\mathbb{Z}^2)$ defined in (5) are used to modulo these sensors corresponding to algebraic integers in $\mathbb{Z}[i]$, as depicted in Fig. 3(a) and Fig. 3(b) for $p = 5$ and $p = 13$ respectively.

B. Chinese Remaindering over $\mathbb{Z}[\omega]$

To derive the prime ideals in the ring of Eisenstein integers, we shall aim for p such that $D = -3$ is a quadratic residue:

$$x^2 \equiv -3 \pmod{p},$$

for some $x \in \mathbb{Z}$. For example, solutions can be $2^2 \equiv -3 \pmod 7$, $6^2 \equiv -3 \pmod{13}$, and so forth. By performing ideal decomposition (12), these rational primes can be decomposed into prime ideals as: $\langle 7 \rangle = \langle 2+\sqrt{3}i \rangle \langle 2-\sqrt{3}i \rangle$ and $\langle 13 \rangle = \langle 1+2\sqrt{3}i \rangle \langle 1-2\sqrt{3}i \rangle$. With $p = 7$, the two prime ideals decomposed from $\langle 7 \rangle$ are $\mathfrak{p}_1 = \langle 2 + \sqrt{3}i \rangle$ and $\mathfrak{p}_2 = \langle 2 - \sqrt{3}i \rangle$, where $2 + \sqrt{3}i$ and $2 - \sqrt{3}i$ are prime elements by the criteria given in Section III-A. Because $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are algebraic conjugate of each other ($2 + \sqrt{3}i = 1 + 2\omega$ and $2 - \sqrt{3}i = 1 + 2\hat{\omega}$), it can also be checked that these two conjugate Eisenstein integers are coprime according to Corollary 3 with $m_1 = 1$ and $m_2 = 2$. Similar to Gaussian integers, $\langle 2 + \sqrt{3}i \rangle$ in $\mathbb{Z}[\omega]$ has an integral basis represented by

$$(2 + \sqrt{3}i)\{1, \omega\} = \left\{2 + \sqrt{3}i, \frac{-1 + 3\sqrt{3}i}{2}\right\}$$

whose corresponding generator matrix is

$$\begin{aligned} \mathbf{G}_{(2+\sqrt{3}i)} &= \begin{pmatrix} 2 & -\frac{1}{2} \\ \sqrt{3} & \frac{3\sqrt{3}}{2} \end{pmatrix} \\ &= \begin{pmatrix} 1 & \frac{1}{2} \\ 0 & \frac{\sqrt{3}}{2} \end{pmatrix} \underbrace{\begin{pmatrix} 1 & -2 \\ 2 & 3 \end{pmatrix}}_{\mathbf{B}_{(2+\sqrt{3}i)}}, \end{aligned}$$

and the integral basis of $\langle 2 - \sqrt{3}i \rangle$ is given by

$$(2 - \sqrt{3}i)\{1, \omega\} = \left\{2 - \sqrt{3}i, \frac{5 + \sqrt{3}i}{2}\right\}$$

with the generator matrix:

$$\mathbf{G}_{(2-\sqrt{3}i)} = \begin{pmatrix} 1 & \frac{1}{2} \\ 0 & \frac{\sqrt{3}}{2} \end{pmatrix} \underbrace{\begin{pmatrix} 3 & 2 \\ -2 & 1 \end{pmatrix}}_{\mathbf{B}_{(2-\sqrt{3}i)}}.$$

Here the matrices $\mathbf{B}_{(2+\sqrt{3}i)}$ and $\mathbf{B}_{(2-\sqrt{3}i)}$ are the matrix representations of ideals $\langle 2 + \sqrt{3}i \rangle$ and $\langle 2 - \sqrt{3}i \rangle$ respectively and they are coprime according to Theorem 1. Similar to the Gaussian case, it can be verified that $|\det(\mathbf{B}_{(2+\sqrt{3}i)})| = |\det(\mathbf{B}_{(2-\sqrt{3}i)})| = \mathrm{N}(\langle 2 + \sqrt{3}i \rangle) = \mathrm{N}(\langle 2 - \sqrt{3}i \rangle) = p = 7$. With the notations above, the locations of the elements of the first subarray are given by $\mathbf{G}_{(2-\sqrt{3}i)}\mathbf{e}_1 \in \sigma\big(\langle 2-\sqrt{3}i \rangle\big)/7A_2$, while those positions of the second subarray are $\mathbf{G}_{(2+\sqrt{3}i)}\mathbf{e}_2 \in \sigma\big(\langle 2+\sqrt{3}i \rangle\big)/7A_2$, where $\mathbf{e}_1 \in A_2/\sigma\big(\langle 2+\sqrt{3}i \rangle\big)$, and $\mathbf{e}_2 \in A_2/\sigma\big(\langle 2-\sqrt{3}i \rangle\big)$. The elements in the cross-difference coarray are defined in the same form as the $\mathbb{Z}^2$ array, i.e., $\mathbf{d}_e = \mathbf{G}_{(2-\sqrt{3}i)}\mathbf{e}_1 - \mathbf{G}_{(2+\sqrt{3}i)}\mathbf{e}_2$. By substituting $R = A_2$, $\mathcal{I} = \langle 2 + \sqrt{3}i \rangle$ and $\mathcal{J} = \langle 2 - \sqrt{3}i \rangle$ to (20), the generalized CRT guarantees $\mathbf{d}_e \in A_2/7A_2$, yielding an array of 49 degrees of freedom with 13 sensors according to Proposition 1.

Similarly, with a larger array aperture such as $p = 13$, the two prime ideals decomposed from $\langle 13 \rangle$ are $\langle 1+2\sqrt{3}i \rangle = \langle -1+4\omega \rangle$ and $\langle 1-2\sqrt{3}i \rangle = \langle -1+4\hat{\omega} \rangle$, which are coprime according to Corollary 3 with $m_1 = -1$ and $m_2 = 4$. The generator matrices of the corresponding ideal lattices are

Table I
HOLE-FREE SYMMETRIC CRT ARRAY DESIGN

Require: A PID $\mathbb{Q}(\sqrt{D})$.
Steps:

1: Calculate a rational integer $p \in \mathbb{Z}$ such that Legendre symbol $\left(\frac{D}{p}\right) = 1$.
2: Compute the integral basis $\{1, q\}$ of $\mathbb{Z}[q]$ as $q = -\frac{1}{2}B + \frac{1}{2}\sqrt{B^2 - 4C}$ where $B = 0$ and $C = -D$ if $D \not\equiv 1 \pmod 4$, and $B = -1$ and $C = \frac{1-D}{4}$ if $D \equiv 1 \pmod 4$.
3: Decompose $\langle\, p \,\rangle$ into two coprime ideals $\mathfrak{p}_1 = \langle\, m_1 + m_2 q \,\rangle$ and $\mathfrak{p}_2 = \langle\, n_1 + n_2 q \,\rangle$ of $\mathbb{Q}(\sqrt{D})$.
4: Compute generator matrices as

$$\mathbf{G}_1 = \mathbf{G}\begin{pmatrix} m_1 & -Cm_2 \\ m_2 & m_1 - Bm_2 \end{pmatrix} \quad \text{and} \quad \mathbf{G}_2 = \mathbf{G}\begin{pmatrix} n_1 & -Cn_2 \\ n_2 & n_1 - Bn_2 \end{pmatrix},$$

where $\mathbf{G}$ is defined in (6) for $D > 0$ and (7) for $D < 0$.
5: The sensors are allocated on a 2D space where the positions are given by $\mathbf{G}_1\mathbf{x}_2$ and $\mathbf{G}_2\mathbf{x}_1$ with $\mathbf{x}_1 \in \sigma(\mathbb{Z}[q])/2\sigma(\mathfrak{p}_1)$ and $\mathbf{x}_2 \in \sigma(\mathbb{Z}[q])/\sigma(\mathfrak{p}_2)$.

given by

$$\mathbf{G}_{(1+2\sqrt{3}i)} = \begin{pmatrix} 1 & -\frac{5}{2} \\ 2\sqrt{3} & \frac{3\sqrt{3}}{2} \end{pmatrix} \text{ and}$$
$$\mathbf{G}_{(1-2\sqrt{3}i)} = \begin{pmatrix} 1 & \frac{7}{2} \\ -2\sqrt{3} & -\frac{\sqrt{3}}{2} \end{pmatrix}.$$

Here the set of the difference coarray is $A_2/13A_2$ Thus this array provides 169 DOF with 25 sensors. The subarrays are allocated on the following two ideal lattices:

$$\sigma\big(\langle\, 1 - 2\sqrt{3}i \,\rangle\big)/13A_2, \text{ and } \sigma\big(\langle\, 1 + 2\sqrt{3}i \,\rangle\big)/13A_2.$$

Similar to the Gaussian cases, Voronoi regions $\mathcal{V}(pA_2)$ are employed to allocate sensors, yielding more compact arrays. The examples of A_2 array configurations are shown in Fig. 4(a) and Fig. 4(b) for $p = 7$ and $p = 13$ respectively. To highlight the shape of hexagonal Voronoi cell for illustrative purposes, all A_2 based arrays are rotated 90 degrees counterclockwise henceforth.

When all antennas act like receivers, the array configuration given in Definition 5 can be redefined equivalently as a set that consists of sensor locations given by vectors, i.e.,

$$\begin{aligned}\mathcal{Z} =& \{\mathbf{z} = \mathbf{G}_2\mathbf{x}_1 \mid \mathbf{x}_1 \in \sigma(\mathbb{Z}[q])/\sigma(\mathfrak{p}_1)\} \\ &\cup \{\mathbf{z} = \mathbf{G}_1\mathbf{x}_2 \mid \mathbf{x}_2 \in \sigma(\mathbb{Z}[q])/\sigma(\mathfrak{p}_2)\},\end{aligned}$$

where $\mathbf{G}_1$ and $\mathbf{G}_2$ defined as (13) are generator matrices of $\mathfrak{p}_1$ and $\mathfrak{p}_2$ respectively.

V. HOLE-FREE SYMMETRIC CRT-BASED ARRAYS

In general, the elements in the coarrays may not be contiguous, i.e., $\mathcal{D}$ (or equivalently $\mathcal{S}$) may contain holes, which cause ambiguities when subspace-based algorithms are applied. In this section, we provide conditions for hole-free and contiguous cross-difference and sum coarrays by modifying the CRT arrays (Definition 5) under certain restrictions on quotient rings. The definition of hole-free symmetric CRT (HSCRT) arrays is given as follows:

Definition 8: [Hole-free Symmetric CRT arrays, HSCRT] Assume the prime decomposition $\langle\, p \,\rangle = \mathfrak{p}_1\mathfrak{p}_2$ in $\mathbb{Z}[q]$, with $\mathbf{G}_1$ and $\mathbf{G}_2$ being the generator matrices of $\mathfrak{p}_1$ and $\mathfrak{p}_2$ respectively. A hole-free Symmetric CRT array is an extension of CRT array where $\mathbf{x}_1 \in \sigma(\mathbb{Z}[q]) \,/\, 2\sigma(\mathfrak{p}_1)$ and $\mathbf{x}_2 \in \sigma(\mathbb{Z}[q]) \,/\, \sigma(\mathfrak{p}_2)$ and the two subarrays are $\mathbf{G}_1\mathbf{x}_2$ and $\mathbf{G}_1\mathbf{x}_2$ respectively.

Note that the two subarrays can be rewritten by means of Voronoi cells (Definition 1) as $\sigma(\mathfrak{p}_1) \cap \mathcal{V}(\sigma(\mathfrak{p}_1\mathfrak{p}_2)) = \sigma(\mathfrak{p}_1) \cap \mathcal{V}(p\Lambda)$ and $\sigma(\mathfrak{p}_2) \cap \mathcal{V}(2p\Lambda)$ where $\Lambda = \sigma(\mathbb{Z}[q])$ is the algebraic lattice that corresponds to $\mathbb{Z}[q]$ of a quadratic field. The following proposition exploits the concept of Voronoi cells to guarantee the 'hole-free' property of HSCRT:

Proposition 2 (Generating All Lattice Points in $\Lambda \cap \mathcal{V}(p\Lambda)$): HSCRT can generate at least all lattice points in $\Lambda \cap \mathcal{V}(p\Lambda)$ by using the cross-difference coarray.

Proof: For simplicity, let us denote the two ideal lattices by $\Lambda_1 = \sigma(\mathfrak{p}_1)$ and $\Lambda_2 = \sigma(\mathfrak{p}_2)$ respectively. The ideal is to find a new range for $\mathbf{x}_1$ such that the difference vectors can overspread $\Lambda \cap \mathcal{V}(p\Lambda)$ which corresponds to $\Lambda/p\Lambda$ from quotient group point of view. According to CRT, for all $\mathbf{d} \in \Lambda \cap \mathcal{V}(p\Lambda)$, there exist $\mathbf{x}_1' \in \Lambda \cap \mathcal{V}(\Lambda_1)$ and $\mathbf{x}_2 \in \Lambda \cap \mathcal{V}(\Lambda_2)$ such that

$$\begin{aligned}\mathbf{d} &\equiv \mathbf{G}_2\mathbf{x}_1' - \mathbf{G}_1\mathbf{x}_2 \pmod{p\Lambda} \\ &= \mathbf{G}_2\mathbf{x}_1' - \mathbf{G}_1\mathbf{x}_2 - \mathbf{y}, \quad \mathbf{y} \in p\Lambda \cap \mathcal{V}(2p\Lambda) \\ &= \mathbf{G}_2\mathbf{x}_1 - \mathbf{G}_1\mathbf{x}_2, \quad \mathbf{x}_1 = \mathbf{x}_1' - \mathbf{G}_2^{-1}\mathbf{y}.\end{aligned}$$

Considering $\langle\, p \,\rangle = \mathfrak{p}_1\mathfrak{p}_2$ and their corresponding matrices $\mathbf{G}_1$ and $\mathbf{G}_2$, $\mathbf{G}_2^{-1}\mathbf{y}$ is in $\Lambda_1 \cap \mathcal{V}(2\Lambda_1)$. Note that Λ_1 is a sublattice of Λ and $\mathbf{x}_1' - \mathbf{G}_2^{-1}\mathbf{y}$ is identical to $\mathbf{x}_1' + \mathbf{G}_2^{-1}\mathbf{y}$ because of the symmetry of Λ_1. The proof is completed by noting that $\mathbf{x}_1 \in \Lambda \cap \mathcal{V}(2\Lambda_1)$. In short, by selecting $\mathbf{x}_1 \in \Lambda \cap \mathcal{V}(2\Lambda_1)$ and $\mathbf{x}_2 \in \Lambda \cap \mathcal{V}(\Lambda_2)$ results in $\mathbf{d} = \Lambda \cap \mathcal{V}(p\Lambda)$. ■

Generally, the contiguous coarray can be defined as elements within a convex polygon, whereas in this paper, we only consider convex regular polygons such as square and hexagon. One remarkable advantage of HSCRT arrays is that because of the symmetry of the algebraic lattices, their cross-difference coarrays are identical to the corresponding sum coarrays. As a result, Proposition 2 also applies to the sum coarrays, implying that both passive and active

sensing algorithms that require contiguous coarrays can employ HSCRT arrays. The design procedure of HSCRT is summarized in Table I. Next, we study the properties of HSCRT and formulate the contiguous coarrays of hole-free $\mathbb{Z}^2$ and hole-free A_2, which are in the class of HSCRT.

A. Properties of HSCRT Arrays

1) Number of Physical Sensors: According to Proposition 1, the number of sensors in $\Lambda_1/p\Lambda$ and in $\Lambda_2/p\Lambda$ both equal to p. After doubling the range of $\mathbf{x}_1$ to $\Lambda \cap \mathcal{V}(2\Lambda_1)$ and removing the duplicated sensors at the origin, the total sensor number in $2\Lambda_1$ becomes $4(p-1)$. Thus the number of physical sensors of HSCRT is

$$4(p-1)+p = 5p-4.$$

2) Perimeters and Areas of Physical Arrays: Given a prime p, the perimeters of hole-free $\mathbb{Z}^2$ denoted as C_G and of hole-free A_2 denoted as C_E can be calculated as

$$C_G = 8pd, \qquad C_E = 6pd(\sin\frac{\pi}{3})^{-1} \approx 6.928pd,$$

where d is the minimum inter-element spacing and the areas acquired by the two array configurations are

$$A_G = 4p^2d^2, A_E = 3p^2d^2(\sin\frac{\pi}{3})^{-1} \approx 3.464p^2d^2.$$

Therefore the perimeter and the area of A_2 array are about 86% of those $\mathbb{Z}^2$ array, which implies that hole-free A_2 is more compact regarding the geometry.

3) Number of Virtual Sensors in Contiguous Coarrays: According to Proposition 2, the cross-difference/sum coarray of HSCRT can generate all lattice points in $\Lambda \cap \mathcal{V}(p\Lambda)$, which corresponds to $\Lambda/p\Lambda$ from the quotient group of view. Since Λ is a lattice with generator matrix $\mathbf{G}$, $p\Lambda$ is also a lattice whose generator matrix is $\mathbf{G}\mathbf{B}_p$ where $\mathbf{B}_p = p\mathbf{I}$. The cardinality of $\Lambda \cap \mathcal{V}(p\Lambda)$ equals to the cardinality of $\Lambda/p\Lambda$ [28, Definition 3.12.]:

$$|\Lambda/p\Lambda| = |\det(\mathbf{B}_p)| = p^2,$$

i.e., the number of sensors in $\Lambda \cap \mathcal{V}(p\Lambda)$ is p^2.

B. Examples of contiguous coarrays of HSCRT

1) Hole-free $\mathbb{Z}^2$: A hole-free $\mathbb{Z}^2$ array is an HSCRT over the ring of Gaussian integers $\mathbb{Z}[i]$, i.e., $\mathfrak{p}_1, \mathfrak{p}_2 \in \mathbb{Z}[i]$ and $\Lambda = \mathbb{Z}^2$. The consecutive set of hole-free $\mathbb{Z}^2$ is a uniform rectangular array (URA) which can be expressed as $\mathcal{D}_{C,G} = \mathbb{Z}^2 \cap \mathcal{V}(p\mathbb{Z}^2)$, or equivalently

$$\mathcal{D}_{C,G} = \{\mathbf{d} = (x_k, y_j) \mid \mathbf{d} \in \mathcal{D},\ -l_G \le x_k \le l_G,$$
$$-l_G \le y_j \le l_G, k, j = 1, 2, \cdots l_G\},$$

where $l_G = \frac{1}{2}p$ according to Proposition 2. It can be verified that the cardinality of $\mathcal{D}_{C,G}$ is p^2. An example of hole-free $\mathbb{Z}^2$ array is depicted in Fig. 5(a) corresponding to Fig. 3(b) and the effect of filling the holes is illustrated in Fig. 5(b). From this point of view, [9, Theorem 2] can be interpreted as a particular case of $\mathbb{Z}^2$.

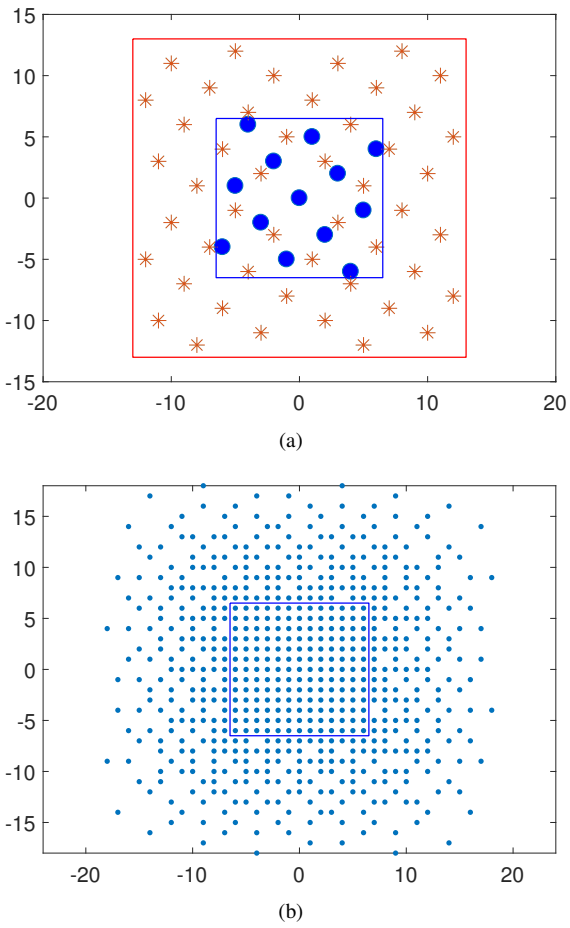


Figure 5. Given the decomposition of $p = 13$, hole-free $\mathbb{Z}^2$ array (a) and its contiguous cross-difference/sum coarray is within $13\mathbb{Z}^2$ (b). The first subarray $\mathbf{G}_2\mathbf{x}_1$ is in red stars and the second subarray $\mathbf{G}_1\mathbf{x}_2$ is in blue dots. Voronoi cells of $13\mathbb{Z}^2$ and $26\mathbb{Z}^2$ are also shown.

2) Hole-free A_2: Analogously, hole-free A_2 is defined as a type of HSCRT over the ring of Eisenstein integers $\mathbb{Z}[\omega]$, whose contiguous part of the coarray is also hexagonal with basis given by (8). Let l_r denote the inscribed radius of the contiguous hexagonal cell $\mathcal{V}(pA_2)$. Using Proposition 2 and the geometry property of hexagonal lattices, it can be easily verified that $l_r = \frac{1}{2}p$. The contiguous part of the cross-difference/sum coarray of hole-free A_2 can be described as $A_2 \cap \mathcal{V}(pA_2)$, or equivalently

$$\mathcal{D}_{C,E} = \{\mathbf{d} = (x_k, y_j) \mid \mathbf{d} \in \mathcal{D},\ -l_r \le y_j \le l_r,$$
$$-2l_r \le \pm\sqrt{3}x_k + y_j \le 2l_r\}$$

where there are p^2 elements in $\mathcal{D}_{C,E}$. Fig. 6(a) depicts an example of hole-free A_2 with $p = 13$ over Eisenstein integers whose cross-difference/sum coarray is shown in Fig. 6(b).

VI. Conclusion

In this paper, it has been demonstrated that the problem of designing planar coprime arrays can be solved through Chinese remaindering over quadratic fields. Inspired by the bijective mappings between the rings of integers and lattices,

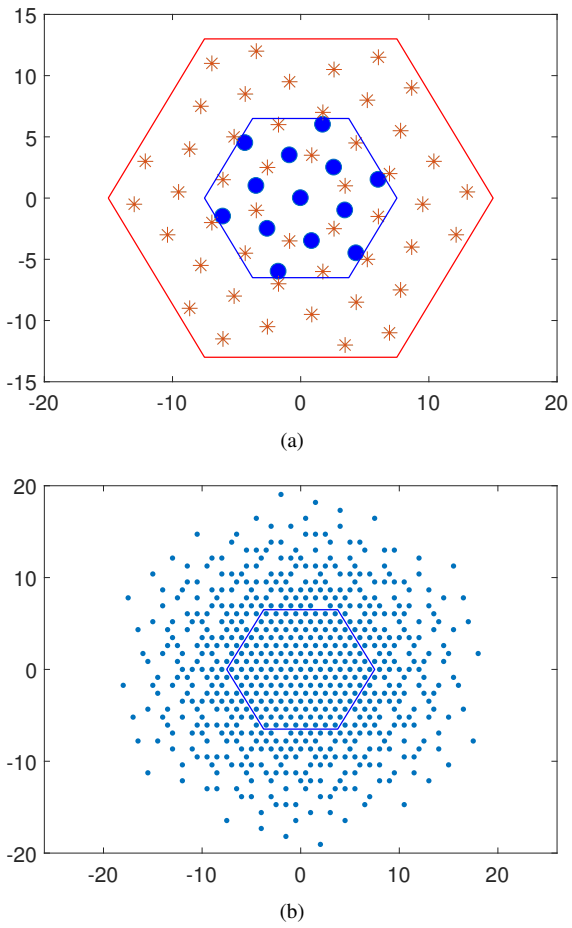


Figure 6. Given the decomposition of $p = 13$, hole-free A_2 array (a) with contiguous cross-difference/sum coarray within $13A_2$ (b). Voronoi cells of $13A_2$ and $26A_2$ are also shown.

a new class of array configurations based on coprime lattices constructed from quadratic integers in PIDs is proposed, which provides enhanced DOF and sparse array geometries, and thus alleviates the mutual coupling effect. By exploiting the properties of PID, a lattice can be represented by a generator matrix calculated by its corresponding quadratic integer, which significantly simplifies the notations of the sensor locations and generalizes the discussions of coprimality issues. The correlation between coprime quadratic integers and matrices have been investigated in great detail, whereby the coprimality of skew-circulant adjugate pairs can be interpreted as special cases of adjugate matrices in Theorem 2. A modified configuration of CRT array is also introduced for an enlarged contiguous coarray. Examples over $\mathbb{Z}[i]$ and $\mathbb{Z}[\omega]$ are provided for illustrative purposes while in general all quadratic coprime integers can be chosen for CRT array design since the generalized CRT only requires the coprimality of ideals.

In the accompanying paper, a new approach of obtaining coprime matrices will be demonstrated, after which the multi-sublattice CRT arrays will be introduced, where the subarrays are built from three or more pairwise coprime quadratic integers. The feasibility of the proposed arrays will be employed for both passive and active sensing, which puts forward the algorithms of angle estimations to sparser and more compact hexagonal arrays.

Appendix A
Proof of Theorem 1

By the assumption on the coprimality of m and n, there must exist α and β such that $m\alpha+n\beta = 1$ with $m, n, \alpha, \beta \in \mathbb{Z}[q]$. Without loss of generality, let $\{1, q\}$ be an integral basis of $\mathbb{Z}[q]$ where $q^2+Bq+C = 0$ according to (2). Taking the algebraic conjugation of both sides of $m\alpha + n\beta = 1$ yields $\hat{m}\hat{\alpha} + \hat{n}\hat{\beta} = 1$ where $\hat{m}$ is the algebraic conjugate of m and same with other elements. $\hat{q}$ is the other root of $f(X) = 0$ expressed (4). By expending all quadratic integers using the basis, it can be easily proved that $m\alpha + n\beta = 1$ if and only if $\hat{m}\hat{\alpha} + \hat{n}\hat{\beta} = 1$. Let us write these two equations by the matrix form:

$$\begin{pmatrix} m & 0 \\ 0 & \hat{m} \end{pmatrix}\begin{pmatrix} \alpha & 0 \\ 0 & \hat{\alpha} \end{pmatrix} + \begin{pmatrix} n & 0 \\ 0 & \hat{n} \end{pmatrix}\begin{pmatrix} \beta & 0 \\ 0 & \hat{\beta} \end{pmatrix} = \mathbf{I}. \tag{27}$$

Define $\mathbf{P}_\alpha$ and $\mathbf{P}_\beta$ as eigenvalue matrices as $\mathbf{P}_m$ given in (16). Then (27) can be rewritten as $\mathbf{P}_m\mathbf{P}_\alpha + \mathbf{P}_n\mathbf{P}_\beta = \mathbf{I}$. According to Lemma 1, $\mathbf{Q}$ consists the eigenvectors of matrix representations and is expressed in (16), then left and right multiplying $\mathbf{Q}^{-1}$ and $\mathbf{Q}$ respectively yields

$$\mathbf{B}_m\mathbf{B}_\alpha + \mathbf{B}_n\mathbf{B}_\beta = \mathbf{I}, \tag{28}$$

i.e., $\mathbf{B}_m$ and $\mathbf{B}_n$ are left coprime.

Next, we prove the sufficiency of the theorem. If $\mathbf{B}_m$ and $\mathbf{B}_n$ are assumed to be coprime, there exist $\mathbf{B}'_\alpha$ and $\mathbf{B}'_\beta$ where

$$\mathbf{B}'_\alpha = \begin{pmatrix} \alpha'_1 & \alpha'_2 \\ \alpha'_3 & \alpha'_4 \end{pmatrix} \text{ and } \mathbf{B}'_\beta = \begin{pmatrix} \beta'_1 & \beta'_2 \\ \beta'_3 & \beta'_4 \end{pmatrix}$$

such that $\mathbf{B}_m\mathbf{B}'_\alpha + \mathbf{B}_n\mathbf{B}'_\beta = \mathbf{I}$, which results the following:

$$m_1\alpha'_1 - Cm_2\alpha'_3 + n_1\beta'_1 - Cn_2\beta'_3 = 1, \text{ and} \tag{29}$$

$$m_1\alpha'_3 + m_2\alpha'_1 + n_1\beta'_3 + n_2\beta'_1 - Bm_2\alpha'_3 - Bn_2\beta'_3 = 0. \tag{30}$$

Let $\alpha' = \alpha'_1 + \alpha'_3 q$ and $\beta' = \beta'_1 + \beta'_3 q$ be two quadratic integers in $\mathbb{Z}[q]$. Then replacing q^2 with $-Bq - C$ yields

$$\begin{aligned} m\alpha' + n\beta' &= (m_1\alpha'_1 - Cm_2\alpha'_3 + n_1\beta'_1 - Cn_2\beta'_3) \\ &+ (m_1\alpha'_3 + m_2\alpha'_1 + n_1\beta'_3 + n_2\beta'_1 - Bm_2\alpha'_3 - Bn_2\beta'_3)q \end{aligned} \tag{31}$$

Substituting (29) and (30) to (31), it can be verified that $m\alpha' + n\beta' = 1$.

Appendix B
Proof of Corollary 1

Assume $\mathbf{B}_m$ and $\mathbf{B}_n$ are left coprime. From Theorem 1, this assumption is equivalent to that their corresponding quadratic integers m and n in $\mathbb{Z}[q]$ are coprime, i.e., there exist α and β such that $m\alpha + n\beta = 1$, which is equivalent to (28). By Lemma 2, (28) is equivalent to

$$\mathbf{B}_\alpha\mathbf{B}_m + \mathbf{B}_\beta\mathbf{B}_n = \mathbf{I},$$

i.e., $\mathbf{B}_m$ and $\mathbf{B}_n$ are right coprime.

APPENDIX C
PROOF OF THEOREM 2

Since the canonical embedding is bijective, the inverse mapping realizes the corresponding algebraic integers of $\mathbf{B}_m$ and $\mathbf{B}_{\hat{m}}$ by $m = m_1 + m_2 q$ and $\hat{m} = (m_1 - Bm_2) - m_2 q = m_1 + m_2 \hat{q}$ respectively. According to Theorem 1, Theorem 2 is equivalent to the coprime conditions of two algebraic conjugates in $\mathbb{Z}[q]$. Suppose two conjugate quadratic integers m and $\hat{m}$ are coprime, i.e., $\text{GCD}(m_1 + m_2 q,\, m_1 + m_2 \hat{q}) = 1$. Then $\text{GCD}(m_1 + m_2 q,\, m_2(q - \hat{q})) = 1$ by applying Fact (1). This is equivalent to the following two conditions according to Fact (3):

$$\text{GCD}(m_1 + m_2 q,\, m_2) = 1, \text{ and} \tag{32}$$

$$\text{GCD}(m_1 + m_2 q,\, \hat{q} - q) = 1. \tag{33}$$

By Fact (1), (32) can be simplified to

$$\text{GCD}(m_1,\, m_2) = 1, \tag{34}$$

which needs to be held for all cases from (a) to (c). According to (3) and (4), $\hat{q}$ can be replaced by $\hat{q} = -B - q$, then (33) can be rewritten as $\text{GCD}(m_1 + m_2 q,\, 1 - 2q) = 1$ or $\text{GCD}(m_1 + m_2 q,\, 2q) = 1$ corresponding to $B = -1$ or $B = 0$ respectively depending on the minimum polynomial of the quadratic field $\mathbb{Q}(\sqrt{D})$ given in (1).

(a) In the first case ($B = -1$), $\text{GCD}((2m_1 + m_2)q, 1 - 2q) = 1$ is obtained by subtracting $m_1(1 - 2q)$ to the first entry, which is equivalent to

$$\text{GCD}(2m_1 + m_2,\, 1 - 2q) = 1,$$

since $\text{GCD}(q, 1 - 2q) = \text{GCD}(1, q) = 1$ (1 and q must be coprime as $\{1, q\}$ is an integral basis). Substituting $B = -1$ to $f(X)$, (2) becomes $q^2 - q + C = 0$. Thus (a) is obtained by enforcing a square on the second entry, i.e., $(1 - 2q)^2 = 1 - 4C$. Recall (34) shall hold.

(b) With $B = 0$ (the GCD of $m_1 + m_2 q$ and $2q$ is 1), enforcing a square on $m_1 + m_2 q$ and applying Fact (1) result in $\text{GCD}(m_1^2 + m_2^2 q^2, 2q) = 1$, which is equivalent to $\text{GCD}(m_1^2 + m_2^2 q^2, q) = 1$ and $\text{GCD}(m_1^2 + m_2^2 q^2, 2) = 1$ by Fact (3). Note that $q^2 = C$ given $B = 0$ (3). Thus by Fact (1)-(3), the former can be simplified to

$$\text{GCD}(m_1^2, q) = \text{GCD}(m_1, C) = 1, \tag{35}$$

and the latter becomes $\text{GCD}(m_1^2 + m_2^2 C, 2) = 1$, which can be simplified depending on the parity of C as follows:

If C is an even number, 2 divides Cm_2^2 and thus it can be eliminated, resulting in $\text{GCD}(m_1^2,\, 2) = 1$, which is equivalent to

$$\text{GCD}(m_1,\, 2) = 1 \tag{36}$$

by Fact (2), i.e., m_1 is odd, which coincides with (35) with even C. Recall (34) shall hold.

(c) Likewise, when C is odd, C can be viewed as a sum of a even number C' and the unit, i.e., $\text{GCD}(m_1^2 + (2C' + 1)m_2^2,\, 2) = 1$. Therefore $C' m_2^2$ can be eliminated as the previous case, after which Fact (1) and Fact (3) can be applied, i.e.,

$$\text{GCD}((m_1 + m_2)^2,\, 2) = \text{GCD}(m_1 + m_2,\, 2) = 1. \tag{37}$$

Recall (34) and (35) shall hold. By repeatedly applying Fact (1) and Fact (3), (34) and (37) can be incorporated together since (34) can be rewritten as $\text{GCD}(m_1 + m_2,\, m_2) = 1$ and $\text{GCD}(m_1 + m_2,\, 2m_2) = \text{GCD}(m_1 + m_2,\, m_1 + m_2 - 2m_2)$.

REFERENCES

[1] C. Li, L. Gan, and C. Ling, "Coprime sensing by chinese remaindering over rings," in *Sampling Theory and Applications (SampTA), 2017 International Conference on*, pp. 561–565, IEEE, 2017.

[2] R. Schmidt, "Multiple emitter location and signal parameter estimation," *IEEE Transactions on Antennas and Propagation*, vol. 34, pp. 276–280, Mar 1986.

[3] R. Roy and T. Kailath, "ESPRIT-estimation of signal parameters via rotational invariance techniques," *IEEE Transactions on Acoustics, Speech, and Signal Processing*, vol. 37, no. 7, pp. 984–995, 1989.

[4] C.-Y. Chen and P. P. Vaidyanathan, "Minimum redundancy MIMO radars," in *2008 IEEE International Symposium on Circuits and Systems*, pp. 45–48, May 2008.

[5] P. Pal and P. Vaidyanathan, "Nested arrays: A novel approach to array processing with enhanced degrees of freedom," *IEEE Transactions on Signal Processing*, vol. 58, no. 8, pp. 4167–4181, 2010.

[6] C. L. Liu and P. P. Vaidyanathan, "Super nested arrays: Linear sparse arrays with reduced mutual coupling–Part I: Fundamentals," *IEEE Transactions on Signal Processing*, vol. 64, pp. 3997–4012, Aug 2016.

[7] P. P. Vaidyanathan and P. Pal, "Sparse sensing with co-prime samplers and arrays," *IEEE Transactions on Signal Processing*, vol. 59, no. 2, pp. 573–586, 2011.

[8] S. Qin, Y. D. Zhang, and M. G. Amin, "Generalized coprime array configurations for direction-of-arrival estimation," *IEEE Transactions on Signal Processing*, vol. 63, pp. 1377–1390, March 2015.

[9] P. Vaidyanathan and P. Pal, "Theory of sparse coprime sensing in multiple dimensions," *IEEE Transactions on Signal Processing*, vol. 59, no. 8, pp. 3592–3608, 2011.

[10] P. Pal and P. Vaidyanathan, "Nested arrays in two dimensions, part I: geometrical considerations," *IEEE Transactions on Signal Processing*, vol. 60, no. 9, pp. 4694–4705, 2012.

[11] J. Shi, G. Hu, X. Zhang, F. Sun, and H. Zhou, "Sparsity-based two-dimensional DOA estimation for coprime array: From sum–difference coarray viewpoint," *IEEE Transactions on Signal Processing*, vol. 65, no. 21, pp. 5591–5604, 2017.

[12] C.-L. Liu and P. P. Vaidyanathan, "Hourglass arrays and other novel 2-D sparse arrays with reduced mutual coupling," *IEEE Transactions on Signal Processing*, vol. 65, no. 13, pp. 3369–3383, 2017.

[13] R. A. Haubrich, "Array design," *Bulletin of the Seismological Society of America*, vol. 58, no. 3, p. 977, 1968.

[14] D. A. Marcus, *Number Fields*, vol. 8. Springer, 1977.

[15] M. Vidyasagar, "Control system synthesis: a factorization approach, part ii," *Synthesis lectures on control and mechatronics*, vol. 2, no. 1, pp. 1–227, 2011.

[16] L. Hua, *Introduction to number theory*. Commercial Press, 1967.

[17] P. Vaidyanathan and P. Pal, "A general approach to coprime pairs of matrices, based on minors," *IEEE Transactions on Signal Processing*, vol. 59, no. 8, pp. 3536–3548, 2011.

[18] P. Pal and P. Vaidyanathan, "Coprimality of certain families of integer matrices," *IEEE Transactions on Signal Processing*, vol. 59, no. 4, pp. 1481–1490, 2011.

[19] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices, and Groups*. New York: Springer-Verlag, 3 ed., 1998.

[20] Z. Tian and H. L. V. Trees, "DOA estimation with hexagonal arrays," in *Acoustics, Speech and Signal Processing, 1998. Proceedings of the 1998 IEEE International Conference on*, vol. 4, pp. 2053–2056 vol.4, May 1998.

[21] H. Van Trees, *Optimum Array Processing: Part IV of Detection, Estimation, and Modulation Theory*. Wiley Interscience, 2004.

[22] A. Guessoum and R. Mersereau, "Fast algorithms for the multidimensional discrete fourier transform," *IEEE transactions on acoustics, speech, and signal processing*, vol. 34, no. 4, pp. 937–943, 1986.

[23] C. Dahl, I. Rolfes, and M. Vogt, "Comparison of virtual arrays for MIMO radar applications based on hexagonal configurations," in *Microwave Conference (EuMC), 2015 European*, pp. 1439–1442, IEEE, 2015.

[24] C. Dahl, I. Rolfes, and M. Vogt, "MIMO radar concepts based on antenna arrays with fractal boundaries," in *Radar Conference (EuRAD), 2016 European*, pp. 41–44, IEEE, 2016.

[25] Q. Wu, Y. D. Zhang, M. G. Amin, and B. Himed, "High-resolution passive sar imaging exploiting structured bayesian compressive sensing," *IEEE Journal of Selected Topics in Signal Processing*, vol. 9, no. 8, pp. 1484–1497, 2015.

[26] R. T. Hoctor and S. A. Kassam, "The unifying role of the coarray in aperture synthesis for coherent and incoherent imaging," *Proceedings of the IEEE*, vol. 78, no. 4, pp. 735–752, 1990.

[27] S. Qin, Y. D. Zhang, and M. G. Amin, "DOA estimation of mixed coherent and uncorrelated targets exploiting coprime MIMO radar," *Digital Signal Processing*, vol. 61, pp. 26–34, 2017.

[28] F. Oggier, E. Viterbo, *et al.*, "Algebraic number theory and code design for rayleigh fading channels," *Foundations and Trends® in Communications and Information Theory*, vol. 1, no. 3, pp. 333–415, 2004.

[29] Y.-P. Lin, S.-M. Phoong, and P. Vaidyanathan, "New results on multidimensional chinese remainder theorem," *IEEE Signal Processing Letters*, vol. 1, no. 11, pp. 176–178, 1994.

[30] R. A. Mollin, *Algebraic number theory*. Chapman and Hall/CRC, 2011.

[31] H. Pollard and H. G. Diamond, *The theory of algebraic numbers*. Courier Corporation, 1998.

[32] J. Neukirch, "Algebraic number theory, volume 322 of grundlehren der mathematischen wissenschaften [fundamental principles of mathematical sciences]," 1999.

[33] W. W. Hager, *Applied numerical linear algebra*. Prentice Hall, 1988.

[34] M. R. Adhikari and A. Adhikari, *Groups, rings and modules with applications*. Universities Press, 2003.

[35] K. Conrad, "The Gaussian integers," *Pre-Print, paper edition*, 2008.